Информационна сигурност

(избираема дисциплина)

Лектор: доц. д-р Николай Касъклиев

Контакти: **kasakliev@uni-plovdiv.bg**

Information security, computer security, information assurance, cyber security и IT security

- Това не са синоними в тесния смисъл и ясна граница не е дефинирана
- Имат много общи аспекти и промяна на термините във времето
- Но всяко понятие засяга и нещо специфично-вж. https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/ или https://onlinedegrees.sandiego.edu/information-assurance-vs-cybersecurity/
- Информационна сигурност – засяга както цифровата, така и аналоговата информация, инф. системи, контролиран достъп (друг термин използван в много научни публикации и по-често в САЩ за физически инф. активи преди да се наложи ИС е **Information Assurance**)
- Компютърна сигурност – акцентира върху технологичния аспект- хардуер, софтуер, начини за съхраняване, обработка, предаване на информацията в цифров вид (синонимни термини **Cyber security и IT security**)
- Срещат се и дефиниции (от по-общ към по специфичен термин) information assurance-> Information security-> cyber security

Различия между понятията - пример

- Information Assurance според NIST (федерална агенция в U.S. Department of Commerce) :

"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

- Information Security според NIST:

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Information Security Policy (ISP)

- Политиката за информационна сигурност е набор от правила, които да следват хората при използване на ИТ активи.
- Компаниите могат да създават политики за сигурност на информацията, за да гарантират, че служителите и другите потребители следват протоколите и процедурите за сигурност.
- Политиките за сигурност имат за цел да гарантират, че само оторизирани потребители имат достъп до чувствителни хардуер, системи и информация.
- Създаването на ефективна политика за сигурност и предприемането на стъпки за гарантиране на съответствие е важна стъпка към предотвратяване и смекчаване на заплахите за сигурността.
- За да е политиката наистина ефективна трябва да се актуализира по-често въз основа на: промени в компанията, новите заплахи, изводи направени от предишни атаки и промени в системите и инструментите за сигурност.

Пример - Employee Internet Usage Policy

Employee Internet Policy, Company Internet Policy or Computer Usage Policy.

Policy brief & purpose

Our employee internet usage policy outlines our guidelines for using our company's internet connection, network and equipment. We want to avoid inappropriate or illegal internet use that creates risks for our company's legality and reputation.

Scope

This employee internet usage policy applies to all our employees, contractors, volunteers and partners who access our network and computers.
Employee internet usage policy elements

What is appropriate employee internet usage?

Our employees are advised to use our company's internet connection for the following reasons:
- To complete their job duties.
- To seek out information that they can use to improve their work.
- To access their social media accounts, while conforming to our social media policy.

We don't want to restrict our employees' access to websites of their choice, but we expect our employees to exercise good judgement and remain productive at work while using the internet. Any use of our network and connection must follow our confidentiality and data protection policy.

Employees should:

- Keep their passwords secret at all times.
- Log into their corporate accounts only from safe devices.
- Use strong passwords to log into work-related websites and services.

Пример - Employee Internet Usage Policy

What is inappropriate employee internet usage?

Our employees mustn't use our network to:

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

We also advise our employees to be careful when downloading and opening/executing files and software. If they're unsure if a file is safe, they should ask [their supervisor/ IT manager/ etc.]

Our company may install anti-virus and disk encryption software on our company computers. Employees may not deactivate or configure settings and firewalls without managerial approval.

We won't assume any responsibility if employee devices are infected by malicious software, or if their personal data are compromised as a result of inappropriate employee use.

Company-issued equipment

We expect our employees to respect and protect our company's equipment. "Company equipment" in this computer usage policy for employees includes company-issued phones, laptops, tablets and any other electronic equipment, and belongs to our company.

We advise our employees to lock their devices in their desks when they're not using them. Our employees are responsible for their equipment whenever they take it out of their offices.

Пример - Employee Internet Usage Policy

Email

Our employees can use their corporate email accounts for both work-related and personal purposes as long as they don't violate this policy's rules. Employees shouldn't use their corporate email to:

- Register to illegal, unsafe, disreputable or suspect websites and services.
- Send obscene, offensive or discriminatory messages and content.
- Send unauthorized advertisements or solicitation emails.
- Sign up for a competitor's services unless authorized.

Our company has the right to monitor corporate emails. We also have the right to monitor websites employees visit on our computers.

Disciplinary Action

Employees who don't conform to this employee internet usage policy will face disciplinary action. Serious violations will be cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

Защо е важно да се превърне в приоритет?

- В 21 век всичко в нашия бит опира до информацията и нейната правилна обработка, съхранение и разпространение.
- В личен план всеки от нас ежедневно се налага да предоставя или консумира информация от различен характер и за различни нужди. Например интернет търговия, е-банкиране, електронни комуникации, социални мрежи и др.
- В професионален – аналогично. Например подготовка и изпращане на оферти, обработка на поръчки, управление на склад/магазин, счетоводство, превод на парични средства и др.
- Във всички случаи, ако не изцяло, то поне частично използваме различни помощни средства, като компютри, мобилни устройства, различни софтуерни решения или електронни канали за комуникация.

. . .

- Освен, че информацията има изключително висока цена и важност за нас, тя и нейната обработка подлежи и на регулации, независимо дали вътрешно фирмени, национални или международни.
- Неправилното управление на информацията може да доведе и до значителни загуби включващи пари, имидж, рестрикции и др.
- Например през 2019 г. :

1) Рекордната глоба(209 млн. евро) наложена на British Airways след изтичане на лични данни. През 2018 година хакери откраднаха лична и финансовата информация на повече от 500 000 клиенти от уебсайта и мобилното приложение на компанията.

2) НАП е глобена от КЗЛД за сумата от 5,1 млн. лева за изтичането в Интернет пространството на лични и други данни на около 5 млн. граждани.

3) 1 млн. лева глоба от КЗЛД за банка ДСК за допускане на кражба на хард диск с 23 270 кредитни досиета.

2021 г.

- Годината показа, че проблемите с компютърната сигурност са потенциално катастрофални за цели държави или многонационални компании.
- Януари се установява уязвимост на Microsoft Exchange Servers и до март има заразени около 250 000 в САЩ и няколко хиляди във Великобритания. Уязвимостта дава достъп до имейл комуникациите, самите сървъри и мрежите.
- Теч на данни на 533 милиона потребители на Facebook в началото на април включително и телефонни номера показа, че дори и след теча от 2019 г. компанията има проблем с опазването на личните данни.
- Хакерска група през май успява да получи достъп и да започне да управлява 8,900 km тръбопровод за пренос на горива в САЩ. За около седмица са нарушени доставките на петролни продукти, като се стига до дефицит и затваряне на бензиностанции и повишаване на цените. Платен е откуп от около 5 милиона долара за да се възстанови контрола.
- През май Toshiba Tec France Imaging Systems също е подложена на атака и се налага да спре системи и мрежи в Япония и Европа.
- И в двата случая не се съобщава за изтичане на данни.
- Септември 2021 г. е открита уязвимост при клауд услугата на Майкрософт Azure известна като OMIGOD.

2022 г.

- Съобщава се за множество кибер атаки свързани с руски източници след началото на войната в Украйна.
- Атаките, най-вече от тип phishing, засягащи криптовалути са се увеличили с 200% спрямо 2021г. Не намаляват и случаите на копаене на криптовалута на заразени устройства.
- Продължаващата работа онлайн повишава и атаките чрез PDF документи, които се приемат за стандартни за бизнес цели и съдържащи линкове, които да водят до фалшив сайт или до заразен файл.
- Месец август Apple съобщи за сериозни слабости във връзка със сигурността на някои модели нейни айфони, айпади и компютри, които биха могли да позволят на хакери да поемат контрола върху тези устройства – на 17 и 18 август са публикувани актуализации.
- Ноември - глоба от 391,5 млн. долара ще трябва да плати Google заради незаконно проследяване на местоположението на потребители.
- Ноември - руската хакерска група "KILLNET„ провежда DDoS атака върху редица сайтове на български институции.

2023 г.

- Twitter – януари – теч на данни(имейл адреси) на 200млн. потребители
- UK – осъществен е достъп до сървъри на Electoral Commission , които съдържат имейли, системи за контрол и копия на електорални регистри за периода 2014 и 2022 г., съдържат се персонална информация (имена, имейл и дом. адреси, телефонни номера).
- Уязвимост в услугата GoAnywhere дава достъп до файлове. Едни от засегнатите са Hatch Bank, the City of Toronto, Rubrik и Hitachi Energy. Съобщава се за атака с криптовирус.
- AT&T съобщава за теч на лични данни за около 9 млн. потребители.
- През годината са атакувани множество системи на университети, болници, банки, мобилни оператори и др.
- Откраднати са паспортни данни от система на Индонезийското мин. На правосъдието и човешките права. Засегнати са 34 млн. души.
- За България най-известен е случаят с изтечени около 12 млн. лева от водеща БГ компания с фишинг атака и подменен IBAN.
- TikTok е глобена с 345 милиона евро (370 милиона долара) за нарушаване на законите за конфиденциалност по отношение на обработката на лични данни на деца в ЕС.

Тема 1

Въведение

Съдържание

- Увод
- Цели на учебния курс
- Теми
- Литература
- Въведение в информационната сигурност

Увод

- Информационна сигурност се занимава със **защитата на информацията** (често се говори за данни) и **информационните системи** от неоторизиран достъп, използване, разкриване, промяна, прочитане, запис и унищожаване.
- Терминът е общ и може да бъде използван независимо от **формата**, която можа да имат данните (електронна или на хартия).
- Информационната сигурност (понякога наричана InfoSec) обхваща **инструментите и процесите**, които организациите използват за защита на информацията. Това включва установяване на правила, които предотвратяват достъпа на неоторизирани лица до бизнес или лична информация.
- Информационна сигурност засяга и практиките по **управление на рисковете**, свързани с използването, работата, съхранението и разпространението на информацията, както и системите и процесите използвани за тези цели.

Цели и оценяване

- Курсът има за основна цел да **запознае** обучаващите се с основите на информационната сигурност.
- Разглеждат се различните **аспекти** на сигурността.
- Курсистите се запознават с **добри практики, средства и политики** при формиране на **програма за сигурност** в една организация или в личен план.
- Оценяване: текуща оценка – присъствено.
- *Алтернатива за оценяване. При невъзможност за получаване на текуща оценка се изготвя курсов проект в едноседмичен срок от датата на последната лекция, като например курсистите могат да проучат текущото състояние по отношение на сигурността на информацията в една фирма/организация и да предложат мерки за повишаване на новото на информационна сигурност.*
- *Или, в курсовия проект да изследват задълбочено конкретна тема, като се акцентира на практическото приложение на разглежданите принципи, дейности, средства и др.*

Разглеждани теми

- Въведение
- Основни понятия и терминология
- Анализ на риска
- Стандарти, регулации и нормативна уредба
- Сигурност на данните. Криптиране.
- Мрежова сигурност
- Автентикация и оторизация
- Сигурност на приложенията
- Мобилна сигурност
- …

Литература

- Цветан Семерджиев, Управление на информационната сигурност, Софттрейд
- Цветан Семерджиев , Сигурност и защита на информацията, Класика и Стил
- Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress; 1 edition (July 16, 2011)
- David Salomon, Foundations of Computer Security, Springer, ISBN-10: 1-84628-193-8
- John E. Canavan, Fundamentals of Network Security, ISBN 1-58053-176-8
- Tony Campbell, Practical Information Security Management: A Complete Guide to Planning and Implementation, ISBN-10: 9781484216842
- Michael Nieles; Kelley Dempsey; Victoria Yan Pillitteri, An Introduction to Information Security, NIST Special Publication 800-12 Revision 1, June 2017, на адрес: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Въведение

- Информацията е една от **най-ценните „стоки“** в наши дни.
- Информацията е от изключителна важност за всеки човек независимо дали се касае за личния живот, свободното време или работата му.
- С бъдещото развитие на информационните технологии всеки от нас ще бъде представен с все повече информация във виртуалното пространство, като се увеличава обема на **личните данни, данни за кредитни и дебитни данни, медицински картони** и много други.
- В тази връзка в наши дни много ярко се откроява нуждата от добра защита на информацията във всеки един аспект.

Значение на защитата на информацията

- От гледна точка на бизнеса информацията е един много **ценен актив**. Да вземем например един производител на хардуер или мобилни устройства. В тази сфера конкуренцията е много голяма, ако друга конкурентна компания придобие информация за: нов патент за продукт, технически характеристики, начин на изработка, недостатъци или друга, то тя може да направи подобрения, или дори да изпревари първата и да отнеме от пазара.
- Или да се разкрият доставните цени на предлагани продукти за различните търговци.
- В личен план за всеки един от нас ситуацията е същата.
- Колкото повече информация се събира и обработва толкова **повече средства и усилия** са необходими за нейното опазване, за нейната цялост и за управлението ѝ.

Управление на информацията (Data Menagament/Governance)

- Всяка организация (а и всеки човек) **подрежда** информацията, с която разполага по определени критерии с цел по-лесната и защита, съхранение и обработка.
- Например, както човек често слага етикети, копира и събира в папки документи на хартия, така и информацията в електронен вид (под формата на файлове) може да се **управлява** по същия начин.
- Когато информацията е в електронен вид нейното управление се **контролира от специалисти и специализиран софтуер и хардуер**.
- Информацията в електронен вид може да се съхранява в бази от данни, на файлови сървъри, на бакъп устройства, използвайки облачни технологии и др.
- Специалисти (професии) - Office Management Specialist, Database Management, Record Center Specialist, Safety Coordinator, Data Entry Specialist…

Предимства от адекватното управление на информацията

- Установено и формализирано управление на критичните данни;
- По-добро качество на данните, спомагащо за по-ниски загуби от осигуряване на качестовото за сложни проекти;
- По-високо качество на мета-данните и на тяхната документация, допринасящи за по-бърз достъп, по-прецизни и подобрени резултати при търсене;
- Налагане на стриктни изисквания и стандарти без нужда от постоянна промяна;
- Удовлетворяване на всички нормативни/регулаторни изисквания и избягване на глоби/санкции;
- Осигурява се единна версия (един формат) на всички данни в организацията, висока съвместимост.

КЛАСИФИКАЦИЯ НА ИНФОРМАЦИЯТА

Да се направи една пълна класификация на информацията е изключително **трудна** задача, тук, за илюстрация, се дава само една опростена класификация по един признак.

- Общодостъпна;
- Персонална / Лична;
- Класифицирана;
- Фирмена.

Дискусия и примери по класификацията*

** Безпрецедентният теч на лични данни от НАП през лятото на 2019 г. е ярък пример за важността на правилната класификация на събираните и обработвани данни и необходимостта от защита на личната информация/данни на най-високо ниво.*

Еволюция на информационната сигурност

- В **миналото** (90-те) компютрите се използват индивидуално, или ако се свързват то това е само в академични, корпоративни или държавни компютърни мрежи.
- Защитата на информацията може да се осигури **по-лесно и с по-малко средства**.
- Информацията в **компютърните мрежи (вкл. държавните и корпоративните) е относително защитена**, тъй като те нямат връзка с външни мрежи.
- В **академична среда** информацията в повечето случаи е **общодостъпна** и не се налага да бъде защитавана.

Еволюция на информационната сигурност

- В **наши дни** ситуацията е коренно различна.
- С развитието на Интернет на практика отделните компютри в академични, държавни и корпоративни мрежи са **достъпни отвън**.
- Налага се да се изграждат т.нар. **Virtual Private Network** или **Интранет мрежи**.
- Осигуряването на сигурността на информацията става все **по-трудно и скъпо**.
- Налага се тенденция на засилено използване на **Облачни технологии**, за да се подобри сигурността, макар че и тук се крият **опасности**.

Облачните технологии и някои въпроси за сигурността?

- Местоположение на данните – в повечето случаи клиентите на облачните услуги не знаят **къде** физически са съхранени техните данни. Въпросът тук е: под коя юрисдикция се намират, например в някоя страна може да е забранено да се събира и съхранява определена информация или файлове (напр. филми, музика).
- Достъп – трябва да се има предвид все пак, че освен администраторите на клиента и **администраторите на доставчика ще имат достъп** до данните. Криптиране?
- При пробив – **кои са отговорните** да разследват, дали специалисти на клиента ще имат права за това.
- Трябва много ясно да е **дефинирано** докъде е **отговорността** на клиента и къде на доставчика не само за сигурността но и за целостта и коректността.

Инвестиции в повишаване на сигурността?

- Категорично - **Да**.
- Макар и да не може да се **измери** по категоричен начин печалбата или ползите.
- Да си представим, че от дадена компания се откраднe информация за иновативен продукт, загубите за компанията могат да бъдат огромни.
- Инвестицията за повишаване на сигурността на информацията може да се разглежда като **застраховка**.

Ползи за бизнеса

- Днес почти всички компании (включително и у нас) разчитат на **Интернет**, за да увеличат продажбите, да подобрят работата с доставчици или с бизнес партньорите си.
- Например, производителите искат да достигнат лесно до всеки потенциален купувач, като за целта използват системи за **електронна търговия** (ЕТ), където обикновено има и разплащане и се събират лични данни.
- Ако дадена компания използва система за ЕТ, която е много добре защитена, то тя ще реализира значително по-големи продажби и като цяло ще има по-добър имидж на пазара.
- **Защо**?

Намаляване на разходите

- Високото ниво на информационна сигурност може да **намали разходите**, например от глоби, дела за вреди, по-малко персонал, нов хардуер или нови информационни системи и мн. др.
- Друг пример, ако бъде **загубена** информация, да кажем изтрита, възстановяването може да бъде много скъпо или в някои случаи невъзможно и да се наложи **въвеждане наново**.
- Пример: **изтрита или компрометирана** информация за оценките на студенти или ученици. Пример Кристиян Бойков през 2017 г. в интервю показа пробив в система на МОН и промяна на оценки на ученици.
- Или системата за ЕТ **откаже/спре** или **не работи коректно** поради атака, то клиентите няма да могат да пазаруват или ще се объркват поръчките им, което ще бъде много скъпо за компанията.
- Например за 2019 г. Alibaba на Деня на необвързаните 11 ноември реализират продажби за 25 млрд. долара за 8 часа, а продажби за 1 млрд. долара бяха отчетени още след първите 68 секунди – колко могат да бъдат загубите ако системите спрат за 30 мин или един час?

Същност

- Сигурността е **парадигма, философия, политика и начин на мислене**.
- Информационната сигурност касае защитата на информацията във **всичките и форми** (писмена, електронна, графична …).
- В ерата на Интернет неизменно трябва да се разглежда и т.нар. **мрежова сигурност** - защита на данните, хардуера и софтуера в мрежова среда.
- **Криптирането** вече е стандартна практика за защита – вижте смартфоните си – при Андроид след версия 5.1 е включено по подразбиране, но може и да се игнорира при първоначалното конфигуриране на устройствата.
- **Разработчиците** обръщат все по-голямо внимание на сигурността.

Аспекти на сигурността

Във всяка ситуация и на всяко ниво отличаваме три ключови аспекта на сигурността. Това са **защита, засичане и превенция**.

!!! Изборът на диаграма не е случаен, и показва …?

Аспекти на сигурността

- ***Защита*** – обикновено това е първото, което се откроява, когато говорим за сигурността.
- Нуждата от защита на информацията днес е равносилна на защитата на дома, ценностите и т.н.
- Защитата дори и в **домашни условия** се изразява в инсталиране на **защитни стени, антивирусни програми и пароли** за контролиран достъп.
- В **корпоративна среда** мерките за защита са значително завишени. Наред с изброените включват и достъп с **биометрични данни, криптиране и архивиране на данните** и много други.
- Дайте **примери** за такива мерки за организацията, в която учите, работите или имате информация.
- **Въпрос** – ако дадете тези примери на определени лица не нарушавате ли сигурността?

Аспекти на сигурността

- ***Откриване/Засичане*** – за да реагираме на заплаха за сигурността на информацията ние трябва да знаем, че такава съществува.
- Например, откриването може да стане от една страна с видеонаблюдение, сензори за движение и други технически средства - т.нар. физическа сигурност.
- От друга, това става, чрез поддръжка и преглед на т.нар. лог файлове, генериране на отчети за потребителска активност и използване на специализиран софтуер (често е част от платените версии на антивирусните програми).
- **Тестването (penetration testing)** е основен способ за откриване, когато говорим за информационни системи.

Аспекти на сигурността

- ***Превенция/Възпиране*** – това е много ефективен метод за намаляване на честотата на атаките, а от там и на загубите.
- Често организациите въвеждат **политики** на превенция, като например се прави разяснителна кампания за потенциалните заплахи и техния източник (например правила за ползване на корпоративната електрона поща).
- Друга мярка е **мониторинг** на сайтовете, които се посещават, файловете, които циркулират във вътрешната мрежа и други.

Дискусия : Други мерки …

Изкуствен интелект(AI) и IS

- AI е способността на машина да показва способности, подобни на човешките, като разсъждение, учене, планиране или креативност.
- AI е наука и инженерство за създаване на интелигентни машини, особено интелигентни компютърни програми или системи от всякакъв вид.
- С AI са свързани технологии като невронни мрежи, големи данни, машинно обучение, извличане на данни, компютърно зрение, алгоритми и модели.
- AI става все по-достъпен за всякакви потребители и с това са свързани е множество опасения от използването му за нарушаване на информационната сигурност.

Изкуствен интелект(AI) и IS основни проблемни насоки

Technology based Social engineering

Социалното инженерство (SE) се счита за един от най-честите проблеми, пред които е изправена информационната сигурност днес, тъй като атаките могат да бъдат открити, но не и спрени. SE атаки имат множество форми базирани на различни технологии : phishing, vishing, baiting или pretexting, които могат да се използват съвместно с (да бъдат подпомогнати) от AI.

Artificial Intelligent Chatbots Usage

Chatbot са мощни и достъпни инструменти, задвижвани от AI, които могат да се използват за генериране както на стихотворение, така и на злонамерен код. Киберпрестъпността има много аспекти и потенциални проблеми и използването на чатботовете може да се развие в дейности като нарушаване на интелектуална собственост, кражба на самоличност, нарушаване на нечия поверителност, кражба на данни, разработване на зловреден софтуер, фишинг, вишинг, спам и дезинформация.

Изкуствен интелект(AI) и IS основни проблемни насоки

Political information security issues

Въздействието на AI върху политиката може да бъде сериозно или дори може да предизвика политически катаклизми. AI може потенциално да се използва за създаване на невероятно убедителни deep fake видеоклипове, аудиозаписи и писмено съдържание, което има потенциала да разпространява неточна информация, да изфабрикува фалшиви новини и да манипулира обществените настроения.

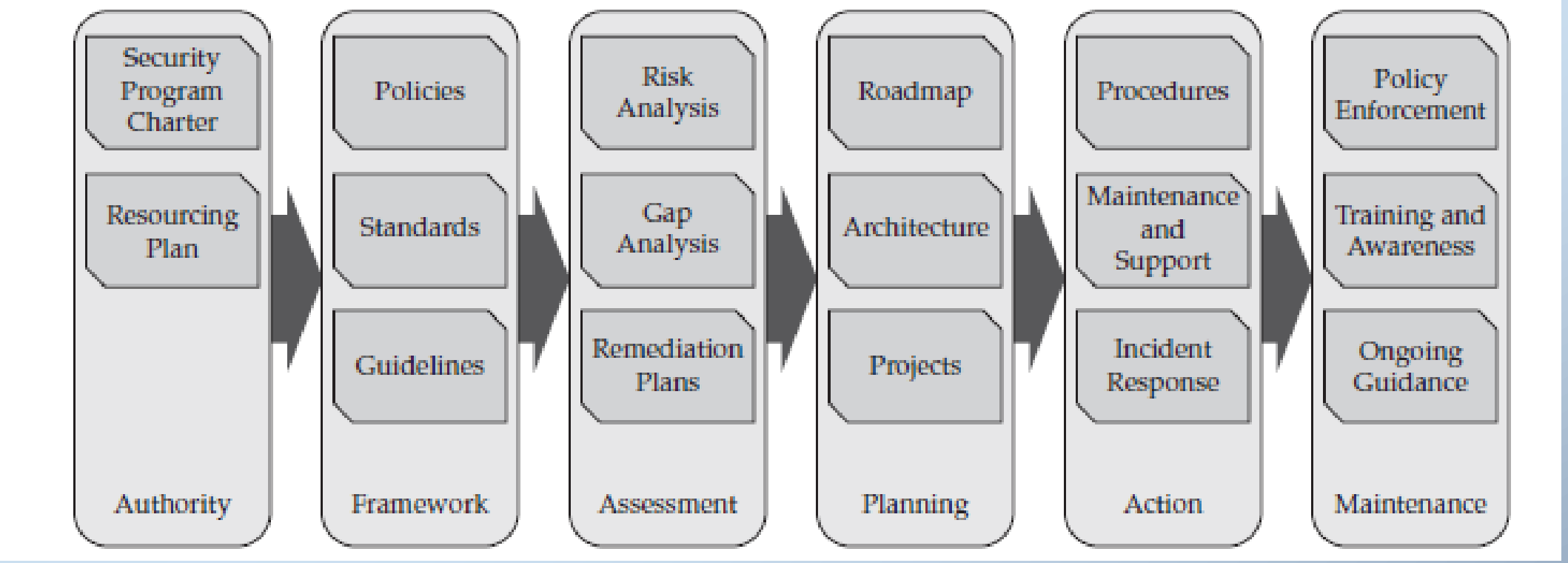
Disruption of the Information Infrastructure

Информационната инфраструктура на една организация може да бъде застрашена от вътрешни и външни заплахи, които могат да бъдат реализирани с помощта на AI технологии. Нормалните бизнес операции могат да бъдат нарушени, спрени или да се появят аномалии, които могат да доведат до бедствия в сигурността дори на критични информационни инфраструктури (CII) като телекомуникации, въздушен транспорт, финансов сектор, електрическа мрежа и много други услуги, важни за икономиката и ежедневна активност.

Приложение
(Програма за сигурност)

- Всяка една организация имплементира в дейността си различни **програми** за различните направления, в които тя оперира като цяло.
- Такъв пример е **социалната програма** на една организация. Част от такава програма са например организиране на различни събития, семинари, културни прояви, допълнителни дни отпуски, парични премии, детски кътове, обучения и др.
- По отношение на защитата на информацията това е **програмата за информационна сигурност**.
- Дори и малки организации днес оперират с **голямо** количество информация, затова такава програма е **жизнено необходима**.
- В същността си тя представлява **сбор от мерки, дейности, средства, документи и др**., които имат за цел да дадат солидна база и да подобрят нивото на ИС.
- Дизайнът, имплементирането и управлението и под една или друга форма се оценява и при **сертификация** (ISO 27001) на организацията.

Общ модел на програма за сигурност



Програма за сигурност

- ***Отговорност*** (authority)– определят се обхвата, целите, отговорността и как ще се организира програмата. В големите компании това са цели отдели.
- В тяхната компетенция е защитата на информацията, управлението на риска и контрола.
- Често те отговарят и за физическата сигурност/защита, реакция при пробив или т.нар. възстановяване (disaster-recovery).
- Изработват политики и регулации, планират всички ресурси.

Програма за сигурност

- ***Работна рамка (framework)*** – *политиките* за сигурност описват намеренията на изпълнителното ръководство по отношение на това, което трябва да се направи, за да се съобразят с бизнес изискванията.
- Политиката управлява всички аспекти, като технически реализации, така и процедури. Политиките за сигурност трябва да бъдат документирани и публикувани преди да започнат каквито и реализации.
- *Стандартите* са подходящо средство за реализация на такава програма. Стандартите са документирани, за да се осигури приемственост и последователност в изпълнението на програмата и управление на ресурсите. Тъй като стандартите се променят, те изискват периодично преразглеждане, за да отразят промените в софтуера и хардуера, за които се отнасят.

Програма за сигурност

- ***Оценка (Assessment)*** – Анализа (оценката) на риска относно информацията осигурява поглед върху настоящите рискове за организацията. Този анализ се използва, за да се даде **приоритет** на дейностите и разпределение на бюджета, така че по-големите рискове, да получат по-голям дял на внимание и ресурси.
- Анализа на риска продуцира добре определен **набор от рискове**, върху които организацията трябва да акцентира. Тези рискове могат да бъдат намалени или ограничени до приемливо ниво.
- Анализа на пропуските сравнява желаното състояние на програмата за сигурност с действителното състояние и очертава различията. Тези различия, или пропуски, образуват **множество от цели**, за да се подобри сигурността на организацията, за да се приведе в съответствие с един или повече стандарти, изисквания или стратегии.

Програма за сигурност

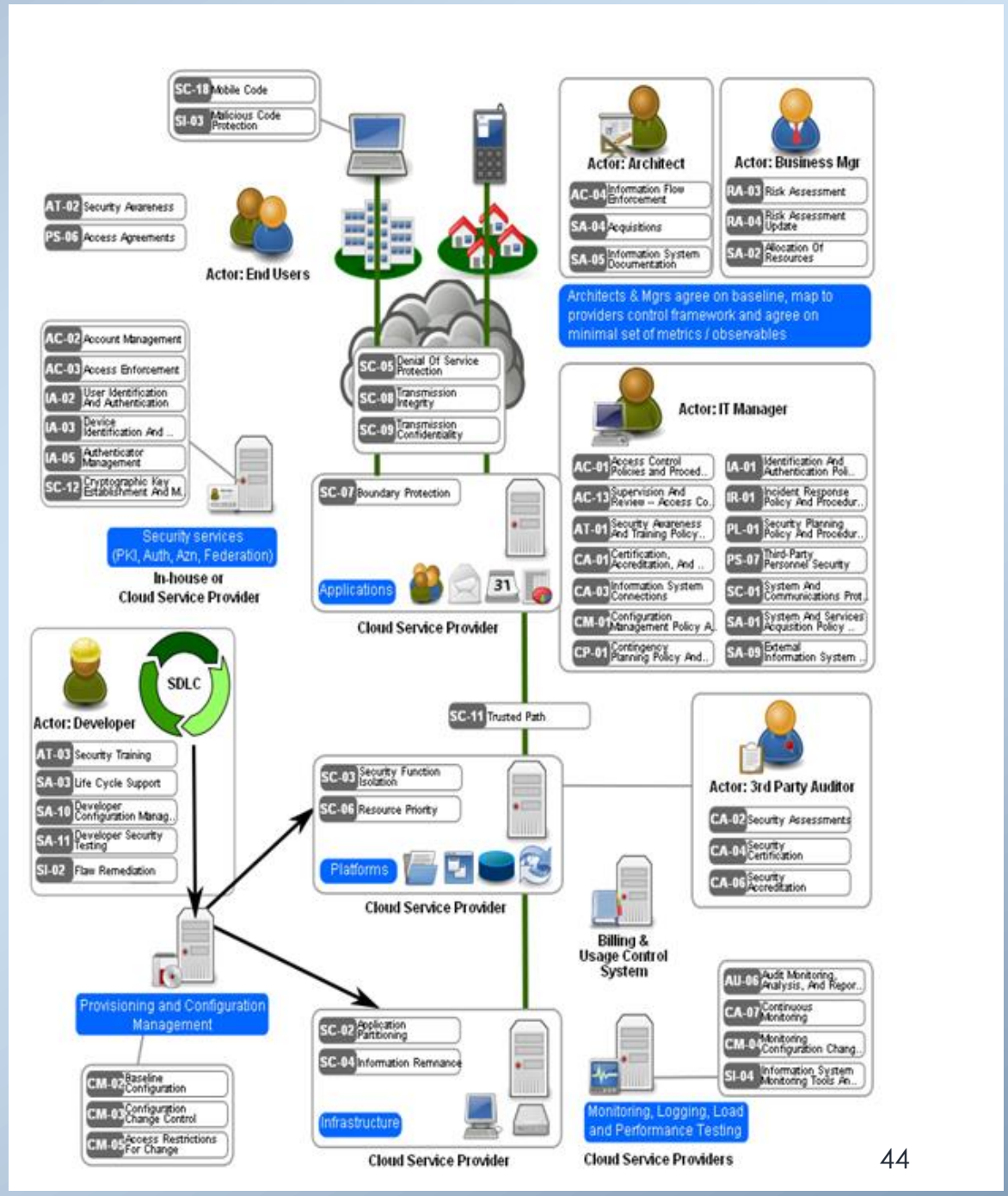
- ***Планиране (Planning)*** – *Пътната карта* е план за действие за това как да се прилагат планове за възстановяване на сигурността. Тя описва кога, къде и какво е планирано. Пътната карта е полезна за мениджъри по сигурността, които се нуждаят от информация, която да планира дейностите и да са посочени определени дати за имплементация и редът за действията.

- *Архитектура на сигурността*, е документ за това как се прилагат технологии за сигурност на относително високо ниво. Той се управлява от политиките за сигурност и идентифицира какво се прави и къде. Той не включва спецификациите на продукти или конкретни детайли за конфигуриране, но архитектурата показва как всичко се комбинира/напасва.

- За описание на архитектурата се използват т.нар. блок диаграма, която показва различните компоненти на архитектурата на сигурност на относително високо равнище, така че може да се види как компонентите работят заедно.

Cloud Computing Model

- Пример от Open Security Architecture (OSA).
- Разработени са безплатни работни рамки



Програма за сигурност

- ***Плана на проекта*** включва подробно дейностите на отделните членове на екипа по сигурността.
- Един добър план на проекта започва с етап на анализ, който обединява всички засегнатите страни, за да обсъдят и прегледат изискванията, обхвата и политиките.
- Анализът е последван от фаза на проектиране, в която архитектурата се разработва с подробности.
- След като дизайнът е бил изчистен, се провежда първоначалното изпитване, за да изчистят бъгове и проблеми.

Програма за сигурност

- ***Дейности*** – Процедурите описват как дадени процеси се извършват от хората на текуща база за осигуряване на желаните резултати от програмата за сигурност в повторяем, надежден начин.
- Техническото обслужване и поддръжка са част от поддържането на текущите операции на програма за сигурността и свързаните с нея технологии, като част от нормалния жизнен цикъл на планиране, актуализиране, преразглеждане и подобряване.
- Действията, които трябва да се предприемат при установяване на събитие заплашващо сигурността, са определени в план за реагиране при инциденти(incident response plan). Този план се отнася за това какво да се направи, когато се случват инциденти със сигурността, и помага да се съкрати времето за реакция и осигурява повторяеми, надеждни и ефективни действия за ограничаване на обхвата и щетите вследствие инцидент.

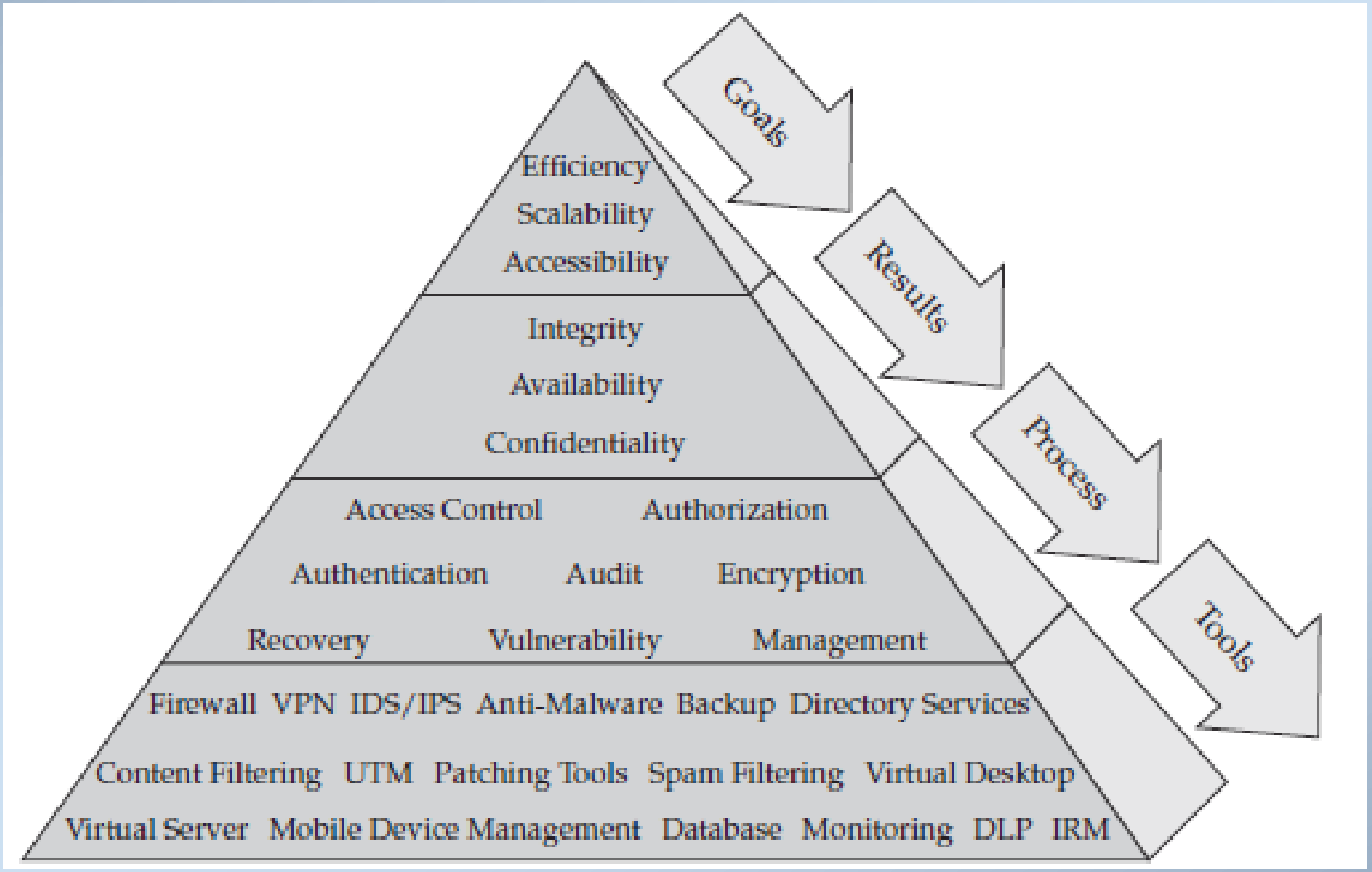
Програма за сигурност

- ***Поддръжка*** – Програми за повишаване на сигурността се използват за обучение на служители, бизнес партньори, както и други от заинтересованите страни за това, какво поведение се очаква от тях, какви действия трябва да предприемат при различни обстоятелства, за да се съобразят с политиките за сигурност, и какви последствия може има, ако те не спазват правилата.
- ***Указания и насоки*** за бизнес проектите и ежедневните операции е важна част от програмата за сигурност. В края на краищата, бизнес ситуациите се променят всеки ден и сигурността следва да се разглежда във всяка ситуация. Някой(експерт) трябва да бъде на разположение да съветва бизнеса по най-добрият начин как да се правят нещата по сигурен начин.

Стратегии и процеси по сигурността

- **Стратегия** за сигурност е съвкупността от архитектурни компоненти и политики, които образуват цялостен план за защита, откриване и реакция на заплахи за сигурността на информацията.
- Много от водещите разработчици на софтуер за сигурност предлагат продукти, които могат да се използват, като компонент от стратегиите, но това не е достатъчно.
- За да е стратегията най-ефективна трябва първо да се очертаят бизнес процесите в организацията.
- **Бизнес процес** представлява свързан набор от повтарящи се действия в точно определен ред, които преобразуват входящи ресурси в краен продукт в съответствие с предварително установени правила.
- Възможно е да се използват различни стратегии, тактики и средства за внедряване за различните бизнес процеси.

Цели, приоритети и процеси -> инструменти



Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Посочете какви разлики откривате, има ли важни пропуски или неточности.
- Опитайте се да дадете Ваша интерпретация.
- Обърнете внимание на това дали източниците Ви са достоверни.
- Практическо задание – напишете на един лист каква „чувствителна“ информация съхранявате на различни устройства(смартфон, флашка, лаптоп, PC), които използвате и евентуалните щети, които може да претърпите, ако я изгубите, ви я откраднат или изтриете погрешка.