Тема 4

Основни принципи, модели и организация

Увод

- Всяка организация, която въвежда система (програма) за сигурност използва някакъв **модел** при реализацията и.
- Например, ако се разчита предимно на т.нар. защитни стени или прокси сървър, то говорим за модел за сигурност на **периметъра**.
- В друг случай, ако се разчита на няколко различни механизми за защита, говорим за модел на **слоеве**.
- При дизайна на инфраструктурата на програмата за сигурност се разчита на това да се **определи**, какво е безопасно и какво не, наред с това кой модел да се избере.
- Програмата за сигурност **отчита** и големината на организацията, степента на дигитализация, нормативната уредба, човешкия и финансовия ресурс и мн. др.

Ключови концепции

- Съществува наложен концептуален модел по отношение на сигурността и това е т.нар. **CIA тройка — Confidentiality, Integrity и Availability**.
- Считат се за 3-те основополагащи **стълба(атрибута, характеристики, цели, аспекта)** на ИС.
- Този, добре установен концептуален модел, макар и повече ориентиран към данните, често е полезен за подпомагане на хората да мислят за сигурност по отношение на най-важни аспекти на защита на информацията.
- Модела не е съвършен и днес се засягат и **други аспекти** на сигурността освен тези три.

CIA тройка

- Базова концепция, която помага на професионалистите по информационна сигурност да мислят как най-добре да защитят информационните активи.
- Ядро, върху което се гради информационната сигурност – достатъчно просто за изучаване, разбиране и имплементиране.
- На схемата трите термина/характеристики се застъпват, тъй като при имплементиране на тази концепция принципи, политики, инструменти, насоки, документи и др. могат да засягат повече от един от тях.

Конфиденциалност (Confidentiality)

- Представлява **предотвратяване** разкриването на информация на неоторизирани лица или системи.
- Или с други думи, всеки набор от данни да е достъпен само от точно определено лице или група лица или информационни системи.
- Компроментирането на конфиденциалността може да бъде в следствие, например на откраднат смартфон или лаптоп, разкрита парола или дори погрешно изпратен имейл. **Други примери?**
- За запазване на конфиденциалността се използват **методи** като:

➢ Класификациия на информацията;

➢ Съхранение в сигурни оторизирани физически обекти;

➢ Прилагане на основни политики за сигурност, напр. криптиране;

➢ Обучение на информационните държатели/отговорници и на крайните потребители.

- Липсата/провал на конфиденциалност се нарича и **нарушение** (**breach)** и по принцип не може да се поправи/отреагира.

Конфиденциалност (Confidentiality)

- Конфиденциалността, като повечето от характеристиките на информация, е взаимозависима от други характеристики и е най-тясно свързана с характеристиката известна като поверителност(privacy).
- Конфиденциалност – отнася се за данните. Споразумение да се запази лична информация в тайна.
- Поверителност – отнася се до човек. Възможност да се представяме пред другите селективно, уединение, ограничаване на публичността. Поверителността понякога се определя като опция за запазване на тайна, да останеш в тайна. **Privacy Policy**
- Важността на конфиденциалността на информацията е особено висока, когато това е **лична** информация за деца, служители, клиенти или пациенти.
- **Дискусия**…. Помислете и дайте и други примери.

Интегритет (Integrity)

- Интегритета е от особено значение за данните и се отнася до уверението, че данните са били **записани** коректно и не са били **променени** по неразрешен начин.
- Понякога се използват и понятията **цялостност, автентичност** или **достоверност**.
- Основната цел е да се блокира възможността за промяна на данните и евентуално, ако възникне проблем, да може тези данни да се **възстановят**.
- Помислете колко големи могат да бъдат вредите например за банка, ако някой може да проникне в системите и и промени баланса по депозит или, ако например може да се изтрият криминалните регистрации на хора в системите на МВР.

Интегритет (Integrity)

Мерки

- Мерките свързани с интегритета са предназначени да гарантират, че даден набор от данни **не може** да бъде променен (или изцяло изтрит), напр. при преноса, от неупълномощено лице или в следствие на хардуерен проблем.
- За да се гарантира интегритета може да се прилагат механизми като:
  - **Валидация** на данните;
  - **Криптиране**;
  - **Проверка за грешки** – вмъкнат бит, контролна сума -cyclic redundancy check - CRC;
  - **File permissions;**
  - **User access controls** – автентикация и оторизация;
  - **Version control (история за промени на данните).**
- Например: от практиката познаваме два метода за проверка на интегритета на информация съхранена във файл – чрез проверка на обема на файла и на т.нар. file hashing (CRC, MD5 и SHA-1 checksum).

Наличност (Availability)

- Наличността позволява оторизирани потребители - лица или компютърни системи да **достъпят** информация безпрепятствено или без обструкция(възражение) и да я получат в необходимия формат.
- За разлика от конфиденциалността и интегритета, които се свързват по-скоро с данните събирани и обработвани от информационните системи, наличността се свързва с **информационните услуги**.
- За осигуряване на непрекъснати информационни услуги се използват методи, като дублиране на сървърите на услуги и на данните (изграждане на т.нар. клъстери*, използване на RAID дискове и др.)
- Взимат се мерки при прекъсването на ток, техническите проблеми, свързани със софтуер и хардуер, както и подновяването или смяната на техника или софтуер да не прекъсват работните процеси свързани с обработка и съхранение на информацията.

***** група от няколко независими КС, които работят като един. Ако една от КС се повреди завките се пренасочват към другите и така информационната услуга не се прекъсва.

CIAT

- Напоследък много експерти говорят и за 4 стълб/принцип на ИС
- **T- traceability**
- Отнася се до възможността да се знае по всяко време кой е достъпвал данните, респективно кой ги е променял
- Този принцип е залегнал и в GDPR, където се изисква, когато чувствителни(лични) данни се достъпват това да се отрази и запази в съответен лог.

Други модели

- Parkerian hexad е съвкупност от шест елемента на сигурността на информацията, предложен от Дон Б. Паркър през 1998 г. Parkerian hexad добавя три допълнителни атрибути на трите класически атрибути за сигурност на тройката CIA.
- Атрибутите на Parkerian Hexad са следните:

- Поверителност/ конфиденциалност
- Притежание или контрол
- Интегритет
- Автентичност
- Наличност
- Полезност

Други модели

- Министерството на отбраната на САЩ допълва общоприетия модел с още два аспекта: Автентичност и защита от отхвърляне (се отнася до способността да се гарантира, че една от страните по договор или на комуникация не може да отрече автентичността на подписа си върху документ или изпращане на съобщение – прилага се цифрово подписване)
- Може би най-пълния модел е представен от Националния институт за стандарти и технологии (NIST) на САЩ в т.нар. специална публикация 800-27, ревизия А, която предлага общо 33 принципа за защита на технологичните системи.

NIST 800-27

Security Foundation

- Principle 1. Establish a sound security policy as the "foundation" for design.
- Principle 2. Treat security as an integral part of the overall system design.
- Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Principle 4. Ensure that developers are trained in how to develop secure software.

NIST 800-27

Risk Based

- Principle 5. Reduce risk to an acceptable level.
- Principle 6. Assume that external systems are insecure.
- Principle 7. Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
- Principle 8. Implement tailored system security measures to meet organizational security goals.
- Principle 9. Protect information while being processed, in transit, and in storage.
- Principle 10. Consider custom products to achieve adequate security.
- Principle 11. Protect against all likely classes of “attacks”.

NIST 800-27

Ease of Use

- Principle 12. Where possible, base security on open standards for portability and interoperability
- Principle 13. Use common language in developing security requirements.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
- Principle 15. Strive for operational ease of use.

NIST 800-27

Increase Resilience

- Principle 16. Implement layered security.
- Principle 17 . Design and operate an IT system to limit damage and to be resilient in response.
- Principle 18. Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
- Principle 19. Limit or contain vulnerabilities.
- Principle 20 . Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
- Principle 21. Use boundary mechanisms to separate computing systems and network infrastructures.
- Principle 22. Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
- Principle 23. Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.

NIST 800-27

Reduce Vulnerabilities

- Principle 24 . Strive for simplicity
- Principle 25. Minimize the system elements to be trusted.
- Principle 26. Implement least privilege.
- Principle 27. Do not implement unnecessary security mechanisms.
- Principle 28. Ensure proper security in the shutdown or disposal of a system.
- Principle 29. Identify and prevent common errors and vulnerabilities.

Design with Network in Mind

- Principle 30. Implement security through a combination of measures distributed physically and logically.
- Principle 31 . Formulate security measures to address multiple overlapping information domains.
- Principle 32. Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
- Principle 33. Use unique identities to ensure accountability.

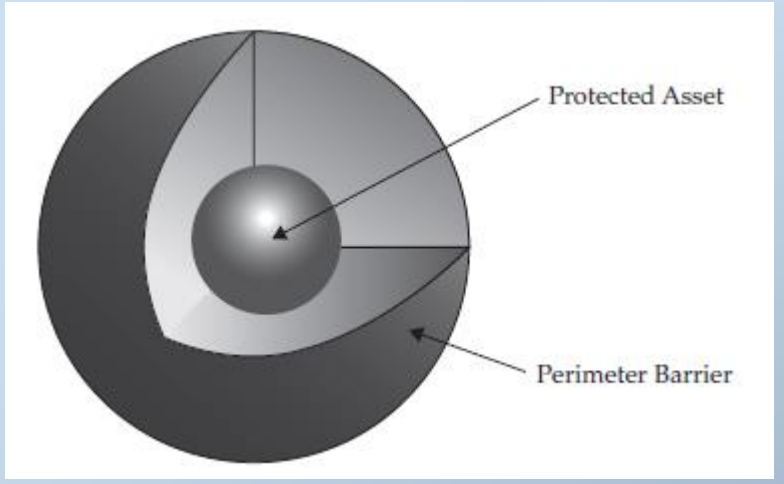
Модели на защита

Съществуват **два** основни практически подхода, за да се запази конфиденциалността, целостта, наличността, както и автентичността на електронни и физически активи, като например данните в една корпоративна мрежа:

1. Изграждане на защитен **периметър** около тези активи и последствие се даде доверие на всеки, който има достъп вътре в периметъра;
2. Използване на много различни видове и степени на контрол за сигурност или защита на много **нива.**

Модела Lollipop (лолипоп)

- Най-честата форма на защита, известена като периметрова защита (perimeter security), включва изграждането на виртуална (или физическа) **стена** около информационните активи.
- Защитата по периметър е с основна цел да държи атакуващите **отвън**.
- Лесно е да се **предскаже**.



Модела Lollipop (лолипоп)

- За илюстрация нека разгледаме следния пример. Имаме една къща, тя разполага със стени, врати и прозорци, за защита, каквото се намира вътре (в периметъра).
- Разбира се тази защита може да се пробие. Може да се влезне например през отворена врата или прозорец или да се използва някой отвътре, за да отвори.
- Когато се говори за мрежова сигурност този модел се реализира обикновено със **защитна стена**, която защитава ресурсите вътре в периметъра (локалната мрежа).

Модела Lollipop (лолипоп)

Недостатъци на модела

- Един от недостатъците на периметровата защита е, че след като един хакер пробие периметъра на отбраната, всички активи вътре в периметъра са напълно изложени на риск.
- Друг недостатък е липсата на различни нива на защита. Например: Ако се разчита само на корпоративната защитна стена, то компютрите ще бъдат заплашени от атаки вътре в локалната мрежа, толкова колкото и отвън.
- Защитата по този модел не е достатъчна, за да се осигури адекватна защита във всяка ситуация. Той не се занимава с **вътрешни заплахи** и не осигурява защита срещу нарушение на периметъра.

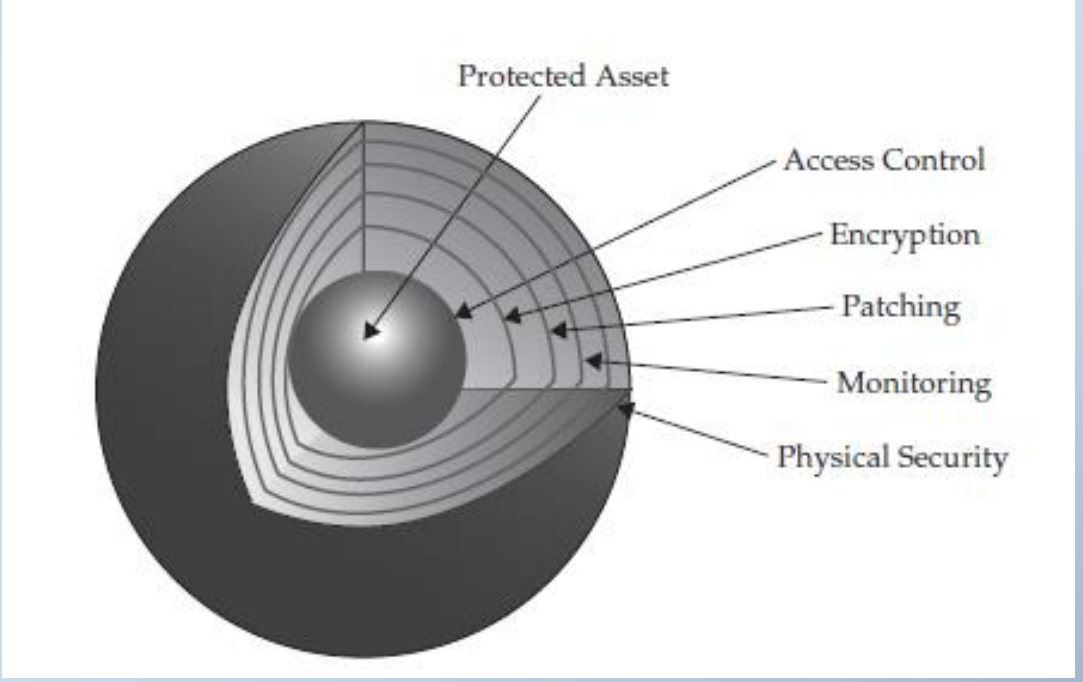
Модел на слоеве (Onion Model)

- Както видяхме модела на периметрова защита има значителни недостатъци.
- По-добрия подход е да построим защитата си на отделни **слоеве**.
- Той допълва защитата в периметър с добавяне на „**защита в дълбочина**“.
- Ако продължим примера с къщата, този модел предполага, че освен стени, врати и прозорци ценностите ще бъдат защитени с други мерки, например бижутата да бъдат заключени в сейф.
- Използването на много слоеве на защита може значително да **затрудни** или да **не допусне атака**. Тъй като пробивът в един слой може да се установи своевременно и да се предприемат бързи ответни мерки.

Модел на слоеве (Onion Model)

Например за ИС се постига чрез:

- Сегментирането на мрежа (на базата на достъп и нужда)
- Определяне на зони на доверие
- Защита на различни нива:
  - Мрежа
  - Система - софтуер за лична защитна стена, контрол на достъпа на системата и т.н.
  - Приложение - Multi-факторна автентикация, нива на разрешения и т.н.



Зони на доверие (Zones of trust)

- Друг добър подход за защита е формиране на **зони на доверие**.
- Информационната инфраструктура на една организация в повечето случаи е много **сложна**.
- Една част от информационните услуги може да се доставя от вътрешни ресурси, друга да са от външни, облачни и т.н.
- В една такава сложна архитектура може да се обособят **зони** с различна степен на риск или доверие. Логично външни информационни услуги имат по-висок риск и обратно информационните услуги вътре в организацията са по-малко рискови.
- Подходът е очевиден - при комуникация със системи (мрежи) с ниско ниво на доверие трябва да се прилагат всички мерки за защита, докато при тези с високо ниво да се прилагат само част.

Организация

- Информационната сигурност днес не е само инсталирането на хардуер и софтуер за защита.
- Докато в близкото минало в една организация няколкото човека от IT отдела бяха в силите си да се справят с опасностите днес те не са достатъчни.
- Днес информационната сигурност трябва да се **осъзнае**, взима под внимание и да получава подкрепа на най-високите нива на организацията.
- С други думи, тя трябва да бъде приведена в съответствие с бизнес целите на организация за поддържане или подобряване на благосъстоянието.

Роли и отговорности

- Сега се изисква подход за управление на риска за сигурността, който отговаря на организацията като цяло.
- За големи организации трябва да бъдат формирани работни позиции на всички нива от висшето ръководство до ниво отдел.
- За по-малки организации позициите са няколко на брой, но натоварени с повече отговорности.
- В малки организации обикновено има няколко **администратора** - отговорни за системи, мрежи, софтуер за сигурност и хардуер, инсталиране и настройки и **мениджър и/или директор по сигурността -** отговорни за комуникация с външни органи, изготвяне на политики, насоки, контрол и др.

Длъжности по сигурността

- Тук ще представим един набор от препоръчителни длъжности по сигурността за средни и големи организации.
- За организациите с малък мащаб вече подчертахме, че ще трябва да бъдат обособени длъжности с по-широки отговорности.
- За средни и големи по размер организации се препоръчва да обособени следните длъжности:

1. Chief Information Security Officer;
2. Security Director;
3. Security Manager;
4. Security Architect;
5. Security Engineer;
6. Security Administrator;
7. Други.

Пример за отговорностите на главен ръководител по сигурността(в софтуерна компания)

- Оформяне на основната група от експерти по сигурността
- Централизира общи функции за сигурност, за да работят заедно
- Разработване на сигурни практики за писане на програмен код, за да се избегнат често срещаните уязвимости
- Провеждане на регресивни тестове, за да се гарантира, че новите версии на софтуера не обезсилват предишни проверки за сигурност
- Подаване за оценка на независими организации за оценки на сигурността, като например Европейската програма за тестване (Common Criteria Testing) спонсорирана от Националния институт по Стандартизация (NIST)

Пример за отговорностите на директор по сигурността

- Координира стратегическите цели, свързани със сигурността.
- Ръководи структурите за управление на сигурността, които защитават активите на организацията, интелектуалната собственост и компютърни системи, както и физическата безопасност на служители.
- Идентифицира цели за защита и целите, които съответстват с корпоративни стратегически планове.
- Ръководи разработването и прилагането на глобалната политика за сигурност (правила), стандарти (минимални изисквания), насоки (препоръки), и процедури (стъпка-по-стъпка инструкции), за да се осигури постоянно поддържане на високо ниво на сигурността.
- Поддържа взаимоотношения с местните и държавните институции.
- …

Пример за отговорностите на мениджър по сигурността

- Мениджърът по сигурността има ежедневни отговорности за всички дейности, свързани със сигурността и настъпили инциденти.
- Всички оперативни позиции по сигурността докладват на тази длъжност.
- Мениджърът по сигурността е отговорен за управлението и разпределението на политиките за сигурност и поддръжка, координиране и съгласуване при инцидент със сигурността.
- Мениджърът по сигурността също възлага и определя собствеността на данните и информационните системи.
- Мениджърът по сигурност също се уверява, че всички нива на управление, както и административен и технически персонал участват по време на планиране, разработване и прилагането на политики и процедури за сигурност.

Пример за отговорностите на архитект по сигурността

- Идентифицира заплахи и уязвимости.
- Идентифицира рисковете за информационните ресурси, чрез анализ на риска.
- Идентифицира критични и чувствителни информационни ресурси.
- Работи с «притежателя» на данните за оценка и класифициране на информацията.
- Работи с техническото ръководство, за да оцени ефективността на мерките за сигурност.
- Подпомага мениджъра по сигурността в оценката на разходите и ефективността на мерките за сигурност.

Пример за отговорностите на инженер по сигурността

- Инсталация и конфигурация на мрежи и мрежови устройства, като например уеб защитни стени, мрежови защитни стени, ключове и рутери.
- Конфигурация за сигурност на Unix, Linux или Windows сървъри.
- Конфигурация за сигурност на приложения и бази данни.
- Инсталация, конфигурация и дизайн на инструменти за сигурност, включително и развитие и кодиране.
- Разследване на инциденти със сигурността.
- Поддръжка и мониторинг на мрежата.

Пример за отговорностите на администратор по сигурността

- Осъществява физически и процедурни гаранции за информационните ресурси в рамките на организацията
- Администрира достъпа до информационните ресурси и следи за навременното откриване, отчитане и анализ на опитите за неоторизиран достъп до информационни ресурси
- Осигурява съдействие на лицата, отговорни за сигурността на информацията
- Участва при придобиване на хардуер / софтуер за сигурност
- Съдейства при идентифициране на уязвимостите и други дейности, като събиране на данни и анализ на лог файловете
- Разработва и поддържа правила за контрол на достъпа
- Поддържа списъци с потребители, пароли, ключове за криптиране и автентификация и други

Заключение

- Въвеждането на добра програма/система за информационна сигурност е от изключителна важност в дни на непрекъснати атаки дори и към водещи компании от IT и финансовия сектор.
- Мерките за осигуряване на сигурност трябва да се базират на адекватен модел на защита.
- В организациите трябва да се формират звена/отдели с необходимите длъжности за осигуряване на високо ниво на защита на информационните ресурси.

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.
- Ако работите или имате информация за организация, посочете какви длъжности имащи отношение със сигурността има в нея.