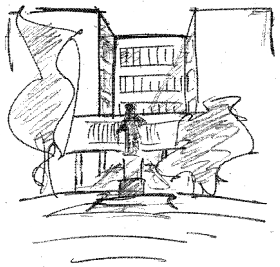
[P271]
Информациони системи

8

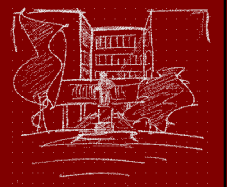


Саша Малков

Универзитет у Београду
Математички факултет

2023/2024

[P271]
Информациони системи



Саша Малков

Тема 12

Безбедност

Најважнија питања

- Основни појмови
  - О чему се овде ради?
- Предмет угрожавања
  - Шта може да буде доведено у питање?
- Начини угрожавања
  - Какве се опасности постоје по информациони систем?
- Начини одбране
  - Како се организује одбрана?

Безбедност информација

- Општа дефиниција безбедности
  - "Безбедност је степен ослобођености од опасности«
- Безбедност информација је степен у коме је онемогућено угрожавање информација
  - "...заштита информација и ИС од неауторизованог приступа, употребе, објављивања, мењања, уништавања, као и од спречавања расположивости."
  - "Једини стварно безбедан систем је систем који је искључен, стављен у блок бетона, запечаћен у оловом обложеној соби са наоружаним стражарима... па чак и тада нисам баш уверен... "
    - (A.Hickey)

Важни појмови

- Опасност
  - сваки догађај који потенцијално угрожава безбедност
- Слабост
  - сваки елемент система, или његова карактеристика, који излаже систем опасностима
- Ризик
  - вероватноћа да се догоди нешто лоше (да се опасност оствари)
- Утицај
  - предмет, обим и/или дубина могућих последица неке опасности

Предмет угрожавања

- Да би смо могли да се старамо о безбедности морамо да знамо шта је све предмет угрожавања безбедности
- ***Предметом угрожавања*** безбедности називамо елементе информационих система који могу да буду доведени у питање услед угрожавања безбедности

Предмет угрожавања

- Основни предмети угрожавања:
  - Поверљивост информација (*Confidentiality*)
  - Интегритет информација (*Integrity*)
  - Расположивост информација (*Availability*)
- Називају се "Безбедносна тројка" - *CIA*
  - често намерно окренуто, као *CAI*
- Често обрнута нотација, из угла *поступака*: *DAD*
  - одавање (*disclosure*)
  - мењање (*alteration*)
  - ометање (*denial*)

Предмет угрожавања (2)

- **Поверљивост информација (*Confidentiality*)**
  - Способност да се сопствени подаци заштите од неовлашћеног приступа
    - Концепт сличан приватности (али не и исти)
    - Представља неопходан саставни део приватности
  - Угрожава се **одавањем информација** (***disclosure***)
- Интегритет информација (*Integrity*)
- Расположивост информација (*Availability*)

Предмет угрожавања (3)

- Поверљивост информација (*Confidentiality*)
- **Интегритет информација (*Integrity*)**
  - Способност да се спречи неовлашћено или непожељно мењање података
  - Угрожава се **мењањем информација** (***alteration***)
- Расположивост информација (*Availability*)

Предмет угрожавања (4)

- Поверљивост информација (*Confidentiality*)
- Интегритет информација (*Integrity*)
- **Расположивост информација (*Availability*)**
  - Способност да се приступа подацима када су потребни
  - Угрожава се **ометањем информација** (***denial***)

Други предмети угрожавања

- Препознају се и други предмети угрожавања:
  - **Поседовање или управљање**
    - способност пуног управљања подацима
    - обухвата поседовање физичких носилаца информација
  - **Аутентичност**
    - способност да се утврди оригиналност информација
    - обично различити видови ел. потписа
  - **Употреба**
    - степен употребљивости податка
      - зависи од облика, количине и сл.
    - једина не-бинарна угроженост

Карактеристике опасности

- Да бисмо сагледали могуће опасности, морамо да упознамо њихове карактеристике
- Неке од најважнијих карактеристика опасности су:
  - предмет угрожавања
  - узрок
  - начин испољавања
  - утицај
  - ризик

Предмет опасности

- Свака опасност се односи на један или више предмета угрожавања
- Већ смо видели основне предмете угрожавања

Узроци опасности

- ***Спољашње опасности***
  - опасности чији су носиоци субјекти ван организације
- ***Унутрашње опасности***
  - опасности чији су носиоци субјекти запослени у организацији
- ***Незгоде***
  - опасности које настају без експлицитне људске активности
  - кварови, елементарне непогоде,...

Узроци опасности (2)

- Најчешће се највише пажње придаје спољашњим опасностима
- Али унутрашње опасности и незгоде праве далеко више штете
  - до њих чешће долази
  - ИС су за њих слабије припремљени

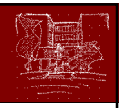
Начин испољавања опасности

- Начин испољавања опасности је одређен начином испољавања проблема које је опасност произвела
- Проблеме настале услед спољашњих и унутрашњих опасности делимо према начину испољавања на:
  - отворене проблеме
  - прикривене проблеме
- Поред тога, по специфичном начину испољавања се издвајају и
  - ненамерни проблеми

Начин испољавања опасности (2)

- Отворени проблеми
  - То су проблеми који се релативно лако уочавају
  - Обично се ради о угрожавању интегритета или расположивости
  - Често је уочљивост проблема управо циљ предузете активности
    - На пример, напади на веб локације и слично
  - Релативно ретко настају као последица унутрашњих напада
  - Отворени проблеми често служе као маска за неке друге врсте напада
    - Привуче се пажња неким отвореним проблемом, да би се одложило уочавање неког много озбиљнијег прикривеног проблема

Начин испољавања опасности (3)



- Прикривени проблеми
  - То су проблеми који се релативно тешко уочавају
  - Обично се ради о угрожавању поверљивости
  - Често међу најважније циљеве предузетих напада спада и што боље прикривање проблема

Начин испољавања опасности (4)

- Ненамерни проблеми
  - Имају веома различито испољавање
  - Настају као последица незгода или услед непажње унутрашњег корисника
    - Спољашњи корисници не могу непажњом да угрозе безбедност ИС
      - осим у случају озбиљне грешке у ИС, а за то опет нису они одговорни, а ако је свесно користе, онда то више није непажња него намера...
      - они могу да доведу у питање само личне информације
  - Некада се неодговорно прикривају из страха од последица

Утицај опасности

- Утицај опасности описује ширини и дубину дејства опасности на предмет угрожавања
- Опасности могу да буду
  - прецизно усмерене – ако је предмет опасности врло узак
    - угрожени су конкретни подаци или уређаји
    - не наноси се широка штета
    - обично су прикривене
  - широког дејства
    - угрожена је инфраструктура
    - обично су то отворене опасности
  - комбиноване
    - негде између
    - имају карактеристике и широких и усмерених опасности

Утицај опасности (2)

- Изражава се и као очекивана вредност штете
- Осим што обухвата непосредне губитке ту су и:
  - компензација последичних губитака
    - нпр. у случају губитка бројева кредитних картица
  - трошкови санирања штете
    - нпр. издавања нових картица
  - трошкови спољних тимова
    - за детекцију и процењивање штете
    - за санирање штете
  - трошкови унапређивања заштитних мера
    - и сертификације...
  - и друго...

Ризик опасности

- Ризик опасности је вероватноћа њеног наступања
- Процењује се у контексту општег и локалног стања система
  - на пример, ако је компанија дошла на лош глас, може да се очекује пораст спољашњих напада
  - или, ако се очекује редукција трошкова, онда може да се очекује пораст унутрашњих напада

Неке од честих опасности

- Грешке и пропусти
- Преваре и крађе
- Унутрашња саботажа
- Инфраструктурни и физички проблеми
- Злонамерни хакери
- Индустријска шпијунажа
- Злонамерни код
- Шпијунажа страних држава
- Претње личној приватности

Грешке и пропусти

- Скоро увек су резултат непажње унутрашњих корисника
- Настају
  - При уношењу података
    - неотпорност програма на неисправне улазне податке
    - недостатак робусности
  - При обради података
    - багови
    - неисправност програма
  - При инсталацији и конфигурисању софтвера
    - необученост администратора и корисника
  - При процедурама одржавања система (резервне копије, извоз, увоз,...)
    - необученост администратора и корисника

Преваре и крађе

- Обично прикривене, подједнако унутрашње и спољашње
- Подврсте
  - Унутрашње преваре
    - већина превара спада у унутрашње проблеме
  - Преваре у јавном простору
    - на Интернету, поштом,...
  - Крађе података
  - Крађе хардвера

Унутрашња саботажа

- Обично отворене, подједнако унутрашње и спољашње
- Видови:
  - уништавање опреме
  - постављање логичких бомби
  - неисправан унос података
  - брисање података
  - мењање података
  - обарање система
  - узимање података за таоце
- Различити узроци
  - освета (за малтретирање, израбљивање, умор...)
  - "виши" циљеви (против "зле" организације)
  - досада и забава
- Процењује се да је
  - мање случајева саботаже него крађе
  - али саботаже су обично скупље

Инфраструктурни и физички проблеми

- Обично су у питању незгоде, али могу да буду и последице саботаже
- Подврсте проблема
  - Проблеми са напајањем (прекиди, удари, нестанак)
  - Прекид комуникације (Интернет)
  - Цурења воде или нестанак воде
  - Проблеми са канализацијом
  - Прекиди у транспортним услугама
  - Пожари, поплаве
  - Грађански немири, штрајкови

Злонамерни хакери

- По правилу спољашње опасности, најчешће отвореног типа
- Овде обично убрајамо све злонамерне неовлашћене упаде у рачунарски систем
  - могу бути спољашњи и унутрашњи
  - углавном се циљају значајни друштвени или економски циљеви
  - многи системи се нападају свакодневно
- Веома непредвидиви
  - и циљеви и намере често нису унапред предвидиви
    - самим тим и средства могу да буду непредвидива
  - напади хакера чине да се људи осећају несигурно, што је често и главни циљ напада
- Често им се придаје већи значај него што реално заслужују
  - фокусирање на ову врсту води занемаривању других врста опасности

Индустријска шпијунажа

- Најчешће прикривена и спољашња, али може да буде и унутрашња
- Чин прикупљања туђих података
  - ради остваривања сопствене користи
    - углавном корпоративне
  - ради наношења штете другоме
    - углавном корпоративне
- У сталном порасту

Злонамерни код

- Обично спољашње опасности
- У фази ширења прикривене, а у фази дејства отворене
- Фронталне, али могу да буду и усмерене на конкретне циљеве
- Вируси, црви, тројански коњи, логичке бомбе и друго
- Број вируса расте експоненцијално, а број инцидената спорије

Шпијунажа страних држава

- По свему слична индустријској шпијунажи али са другачијим циљевима
- Постоји одувек, само мења облике
- Најчешће прикривена и спољашња, али може да буде и унутрашња
- Чин прикупљања туђих података
  - ради остваривања сопствене користи
    - углавном државне, али и корпоративне
  - ради наношења штете другоме
    - углавном државне, али и корпоративне и личне
- У сталном порасту

Претње личној приватности

- Углавном спољашња, најчешће прикривена
- Има сличности са шпијунажом
- Чин прикупљања туђих личних података
  - ради остваривања сопствене користи
    - личне
    - корпоративне
  - ради наношења штете другоме
    - личне
- Постаје све већи проблем
  - пораст употребе рачунарства у облаку
  - огромне количине личних података у различитим рачунарским системима
    - корпоративним и државним
  - запослени у тим системима често имају неограничен приступ личним подацима
    - неовлашћено прегледање
    - крађа
    - продаја информација трећим лицима

Заступљеност опасности

- *Computer Systems Security and Privacy Advisory Board, 1991 Annual Report*
- Преглед губитака:
  - 65% грешке и пропусти
  - 13% непоштени запослени
  - 6% разочарани запослени
  - 8% инфраструктурни проблеми (струја, комуникација, вода, канализација, превоз, пожар, поплава, грађански немири, штрајкови)
  - 5% вода, невезано за поплаве и пожаре
  - 3% спољашњи утицаји, укључујући вирусе, шпијунажу, дисиденте и злонамерне садржаје разних врста, као и бивши запослени, након више од 6 недеља одсуствовања

Напади

- ***Нāпадом*** се назива свака спољашња или унутрашња опасност која се остварује ради свесног и намерног угрожавања безбедности

Основне врсте напада

- Упад (*interception*)
- Онеспособљавање (*interruption*)
- Мењање информација (*modification*)
- Прављење информација (*fabrication*)

Врсте напада – Упад

- Упад је сваки чин неовлашћеног приступања информацијама
- Угрожава поверљивост
  - отвара широм врата другим врстама напада
- Основне мете су:
  - кориснички налози и лозинке
    - са акцентом на повлашћене врсте корисника
  - комуникација
- Неке од техника су:
  - Пецање (енгл. *fishing*)
  - Социјални инжењеринг
  - Провоциране корисничке грешке
  - Пресретање комуникације
  - Уметање упита

Врсте напада - Онеспособљавање

- Онеспособљавање је напад који има за последицу неки вид пуне или делимичне нерасположивости система или његовог дела
- Угрожава расположивост
  - посредно и интегритет
- Основне мете су:
  - кључни уређаји рачунарског система
  - кључне комуникације рачунарског система
- Неке од техника су:
  - Онеспособљавање употребе система *(DOS)*
  - Физичко онеспособљавање
  - Подметање злонамерног кода

Врсте напада – Мењање информација

- Напад којим се мењају постојећи подаци
- Угрожава првенствено интегритет података
  - посредно може да угрози и расположивост
  - углавном је потребно да се прво оствари упад
- Основни циљеви су:
  - мењање ради остваривања другог циља (добит,...)
  - мењање ради прикривања
  - мењање ради уништавања
- Неке од техника су:
  - претходни упад
  - уметање упита

Врсте напада – Прављење информација

- Напад којим се производе нови подаци у систему
  - може да се посматра као подврста мењања,
  - често лакше направити нове податке него мењати постојеће
- Угрожава интегритет
  - прављење велике количине информација може да непосредно угрози расположивост
- Основна мета су:
  - важне базе података
  - важне комуникације
- Неке од техника
  - упад у систем
  - пресретање комуникације

Заштита информационог система

- Информациони и рачунарски системи морају да се штите од опасности
- Заштита од опасности
  - заштита од напада и
  - заштита од незгода
- Заштита од последица опасности
  - резервне копије података
  - резервни подсистеми
    - резервни уређаји
    - резервне комуникације

Спровођење заштите

- Заштита се изводи планско
  - Сагледавају се могуће опасности и ризици
  - Имплементирају се одговарајући заштитни механизми
  - Дефинишу се протоколи реаговања на опасности

Отежавајући фактори

- Брзина и некритичност рачунара
- Несразмерност сложености прављења и превазилажења заштите
- Сложеност оперативних система
- Комуникациони протоколи се тешко мењају

Отежавајући фактори (2)

- Брзина и некритичност рачунара
  - Рачунари раде веома брзо
  - Могу да опслужују велики број корисника
  - Нису у стању да критички посматрају добијене задатке
  - Услед тога су предмет (жртве) рачунарског криминала
- Несразмерност сложености прављења и превазилажења заштите
  - Лакше је пробити рачунарску заштиту него је направити
  - За упад је довољно пронаћи једну слабост система заштите
  - Безбедносни радник мора да пронађе (и отклони) све слабости
- ...

Отежавајући фактори (2)

- ...
- Сложеност оперативних система
  - Савремени ОС имају много задужења
  - Веома су сложени и тешко се сагледавају сви могући проблеми
  - Штавише, додатне аплика
- Комуникациони протоколи се тешко мењају
  - Имају много корисника
  - Уочене слабости се морају крпити у имплементацијама а не у стандарду

Слојеви заштите ИС

- Заштита ИС се организује по слојевима, наводени су од најужег до најширег:
  - Подаци
  - Апликација
  - Сервер (чвор)
  - Интерна мрежа
  - Граница мреже
  - Спољашња мрежа

Слојеви заштите ИС (2)

- **Подаци**
  - криптовање
  - контрола приступа
  - резервне копије
  - проверавање упада
  - анализа слабости
- Апликација
- Сервер (чвор)
- Интерна мрежа
- Граница мреже
- Спољашња мрежа

Слојеви заштите ИС (3)

- Подаци
- **Апликација**
  - системи за обједињену проверу аутентичности
  - филтрирање садржаја
  - провера исправности података
  - праћење и прављење дневника активности
  - провера упада
  - анализа слабости
- Сервер (чвор)
- Интерна мрежа
- Граница мреже
- Спољашња мрежа

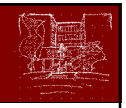
Слојеви заштите ИС (4)

- Подаци
- Апликација
- **Сервер (чвор)**
  - провера аутентичности
  - заштита од вируса
  - заштитни зид
  - систем за препознавање упада (ИДС)
  - систем за превенцију упада (ИПС)
  - криптовање лозинки
  - праћење и прављење дневника активности
  - провера упада
  - анализа слабости
- Интерна мрежа
- Граница мреже
- Спољашња мрежа

Слојеви заштите ИС (5)

- Подаци
- Апликација
- Сервер (чвор)
- **Интерна мрежа**
  - систем за препознавање упада (ИДС)
  - систем за превенцију упада (ИПС)
  - праћење и прављење дневника активности
  - провера упада
  - анализа слабости
- Граница мреже
- Спољашња мрежа

Слојеви заштите ИС (6)

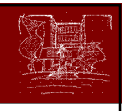


- Подаци
- Апликација
- Сервер (чвор)
- Интерна мрежа
- **Граница мреже**
  - заштитни зид
  - прокси
  - надзор пакета
  - праћење и прављење дневника активности
  - провера упада
  - анализа слабости
- Спољашња мрежа

Слојеви заштите ИС (7)

- Подаци
- Апликација
- Сервер (чвор)
- Интерна мрежа
- Граница мреже
- **Спољашња мрежа**
  - изоловање мреже (ДМЗ)
  - виртуално приватно умрежавање (ВПН)
  - праћење и прављење дневника активности
  - провера упада
  - анализа слабости

10 општих безбедносних правила (*MS Technet04*)



1. Ако вас неко убеди да на свом рачунару извршите његов програм, то више није ваш рачунар
2. Ако неко може да мења ОС на вашем рачунару, то више није ваш рачунар
3. Ако неко има неограничен физички приступ вашем рачунару, то више није ваш рачунар
4. Ако неко сме да поставља програме на вашу веб локацију, то више није ваша веб локација
5. Слабе лозинке побеђују јаку безбедност
6. Рачунар је безбедан само онолико колико је његов власник (корисник) поуздан
7. Криптовани подаци су само онолико безбедни колико и кључ за декриптовање
8. Неажурна антивирусна заштита је само мало боља него непостојећа
9. Потпуна анонимност није практична ни у животу ни на вебу
10. Технологија није лек за све проблеме

Технике превенције

- Међу најважније технике превенције спадају
  - идентификација
  - аутентикација
  - ауторизација
  - праћење (надзирање) активности
  - криптографска заштита
  - физички фактори
  - социјални фактори

Идентификација, аутентикација и ауторизација

- **Идентификација** је провера идентитета
- **Аутентикација** је провера аутентичности идентитета
- **Ауторизација** је провера права специфичног субјекта
  - назива се и **контрола приступа**
- Идентификација и ауторизација обично иду заједно
  - користе се при омогућавању приступа неком систему
  - обављају се у пару, ради "поузданог" утврђивања идентитета корисника
- Ауторизација је други ниво провере
  - претпоставља да је аутентикација успешно извршена

Идентификација

- Идентификација је претпостављање идентитета субјекта
- Уобичајено се одвија на основу
  - имена особе
  - корисничког имена
  - иконице корисника
  - броја рачуна
  - ИД картице
  - отиска прста
  - ДНК
- Сама за себе обично представља веома слаб концепт
  - углавном није или не мора да буде јединствена
  - може да се лажира
    - нпр. када се неко представи, како ћемо знати да није слагао?

Основна провера идентитета

- Провера идентитета (верификација идентитета) је корак након идентификације, али пре аутентикације
  - нпр, када се од особе тражи да покаже лични документ као потврду идентитета, то још увек није поуздана потврда - документ може да буде фалсификован
- Провера може да иде и даље, уз одређену проверу поузданости
  - нпр, може да се изврши поређење документа са базом података, али чак ни то није довољно
- У многим случајевима потврда идентитета потпуно изостаје
  - нпр. ел. пошта - око 90% свих порука је спам

Фалсификовање идентитета

- Сваки метод идентификације може да буде предмет фалсификовања
  - неки теже, неки лакше
- Крађа идентитета почива на успешном фалсификовању идентитета
  - процене губитака су различите, на пример:
    - *www.esecurityplanet.com*
    - процена губитака за 2009. у САД је око 54 млрд $
    - процена губитака за 2016. је око 16 млрд $
- Углавном успева због одсуства аутентикације

Аутентикација

- Аутентикација је скуп метода за установљавање истинитости саопштеног идентитета
- Фактори аутентикације су елементи који учествују у провери
  - што је више фактора, то је провера поузданија
- Уобичајени фактори су оно што особа може да
  - запамти или
  - носи са собом

Фактори аутентикације (1)

- Меморијски фактори:
  - лозинка
  - ПИН
  - фразе за пропуштање
  - нека секвенца поступака
  - или било шта друго што особа може да запамти
- Физички фактори су:
  - ИД картица
  - токен

Фактори аутентикације (2)

- Биометријски фактори су:
  - висина, тежина, боја косе или очију
  - отисак прста
  - узорак ириса или ретине
  - карактеристичне мере лица
  - рукопис
- Логички фактори
  - нека правила реаговања на различите услове
- Географски фактори
  - локација корисника

Аутентикација са више фактора

- Ради повећавања поузданости, аутентикација често користи више фактора
- На пример, при подизању новца са аутомата:
  - физички фактор је картица
  - меморијски фактор је ПИН
  - физички фактор може да буде и мобилни телефон
- Други пример:
  - нека се користи ДНК
  - то је непрактично за сваку проверу
  - у зависности од нивоа приступа додају се мање поуздани, али и мање инвазивни фактори

Аутентикација и приватност

- Аутентикација са више фактора може да представља угрожавање приватности
- Ако неко тражи и имејл адресу и број телефона и можда још неки податак, онда зна о кориснику практично све што му је потребно за потпуно праћење

Узајамна аутентикација

- У уобичајеном процесу аутентикације само једна страна проверава идентитет друге
- **Узајамна аутентикација** је поступак у коме учесници у комуникацију узајамно врше аутентикацију
- Ако се не користи узајамна аутентикација, постоји могућност тзв. напада "човек између"
  - неки субјекат може да се постави између система и корисника
  - може да преузме аутентикацију корисника и изврши операције у име корисника
  - може да запамти аутентикацију корисника и касније је употреби
- Пример је HTTPS

Лозинке

- Лозинке су уобичајени фактор аутентикације
- Употреба лозинке уз корисничко име је најчешћи начин идентификације и аутентикације
- Поузданост почива на "јачини" лозинке
  - дужина
  - сложеност азбуке
- Слабост
  - јаке лозинке се теже памте
    - корисници често бирају слабије лозинке
  - често се користе програми који памте лозинке
    - они представљају додатну слабост у систему
  - често се користи иста лозинка на више места
    - упад у један систем се лако шири на друге системе

Број комбинација лозинки

Дужина лозинке / Азбука	2 знака	4 знака	6 знакова
Мала слова енг. абецеде	676	456 976	308 915 776
Мала и велика слова енг. а.	2704	7 311 616	19 770 609 664
Мала и велика слова и цифре	3844	14 776 336	56 800 235 584
Сви знаци *ASCII*	8836	78 074 896	689 869 781 056

Биометријски фактори

- Могу да се користе на два начина
  - за потврђивање идентитета
    - нпр. слика у личној карти
  - за установљавање идентитета
    - нпр. криминолошка употреба отисака прстију
- Неки се могу фалсификовати лакше, неки теже
- Искључива употреба биометријских фактора често спушта аутентикацију на ниво верификације идентитета

Хардверски токени

- Уобичајено на основу времена (уграђеног часовника) и ПИН-а издају специфичан израчунат број који се користи за додатну аутентикацију
- Једноставније верзије (без часовника) се своде на обичан физички фактор

Ауторизација – Контрола приступа

- Контрола приступа је старање о томе
  - Ко сме да користи које податке и на који начин?
  - Ко сме да ради које послове?
- Класичан приступ је употреба листа за контролу приступа (енгл. *access control list – ACL*)
  - За сваки податак се направи листа у којој се за сваког корисника означи шта сме да ради са податком (ПЧМБ – прављење, читање, мењање, брисање)
- Савремени приступ је омогућавање система улога
  - *Улоге* су апстракција група корисника који имају нека права
  - Листе права приступа се дефинишу за улоге, а не за кориснике
  - Корисницима се додељују улоге (може и више улога)
- Неки системи комбинују систем улога и појединачних права

Праћење (надзирање) активности

- **Обрачунавање** (*accountability*) - свака обављена операција оставља траг који омогућава да се накнадно провери који субјекат ју је извршио
  - ради наплате или
  - ради провере злоупотребе
- **Проверавање** (*auditing*) – проверавање значајних информација о активности система
  - ради провере угрожавања безбедности
  - и из других разлога
- **Прављење дневника** (*logging*) - физичко записивање информација о операцијама у систему
  - техничка претпоставка за остваривање надзора

Проверавање (*Auditing*)

- Шта се проверава?
  - ток операција
  - грешке у поступцима
  - лозинке
  - промене у подацима
  - различите информације о раду система
- Разлози посматрања
  - ради провере угрожавања безбедности
  - ради сагледавања начина употребе
  - ради сагледавања ефикасности рада
  - ради остваривања обрачунавања
  - ради сагледавања поштовања лиценци
  - ради уочавања багова и кварова

Прављење дневника (*Logging*)

- Прављење дневника је основни начин прикупљања информација за надзор
- Дневници представљају трајне записе о активностима система
- Веома су поверљиви
  - обично садрже поверљиве информације из самог система
  - могу да садрже и лозинке
  - могу да садрже податке личне природе о корисницима
  - уобичајено им могу приступати искључиво администратори система
- Могу се конфигурисати
  - врста догађаја који се бележе
  - прецизност бележења
  - учесталост бележења стања система

Надгледање (*Monitoring*)

- **Надгледање** је будно праћење система
- Представља вид проверавања који се одвија "у реалном времену“
- Често укључује и механизме за аутоматизацију реаговања на неке ванредне случајеве

Процењивање (*Assesment*)

- На основу прикупљених информација се могу вршити различите процене о сагласности понашања система и његових корисника са неким скупом правила
  - процењивање законитости
  - процењивање ефикасности употребе
  - процењивање осетљивости или угрожености система
  - препознавање напада

Криптографија

- **Криптографија** је техника представљања информација на измењени начин (тзв. **криптовање**), тако да их може исправно тумачити само субјекат који познаје поступак враћања информација у оригинални облик (тзв. **декриптовање**)
- Криптографија је веома важно средство додатног обезбеђивања информација
  - омогућава заштиту података у одређеној мери чак и у случају да информације постану физички расположиве неовлашћеном лицу
  - степен заштите зависи од снаге криптографксе технике

Криптографија (2)

- Савремене криптографске технике почивају на Кирхофовом принципу:
  - при прављењу криптографског метода потребно је претпоставити да ће противник да упозна метод и стога сва снага метода мора да почива у кључу
- Више о томе у предмету Криптографија

Физичке опасности

- Физичке инфраструктурне опасности...
  - решење је физичка заштита података прављењем резервних копија
- Магнетно поље и електрицитет
  - неопрезно руковање магнетним пољем или електрицитетом у близини осетљивих уређаја може да буде узрок озбиљних кварова
- Крађа уређаја
  - крађом уређаја се долази у физички додир са информацијама на уређају

Физичке опасности (2)

- Провлачење
  - нападач стоји или се креће поред врата, као да је све нормално
  - када неко ауторизован откључа врата и прође кроз њих, он се провуче одмах иза њега
  - решење: двострука врата са међупростором за само једну особу
- Праћење корисника
  - ако корисник ради неки други посао паралелно са употребом рачунара, често се дешава да рачунар са отвореним налогом остане без физичког надзора
- Физичка крађа података
  - крађа медија са подацима, обично са резервним копијама

Физичке опасности (3)

- Копирање података
  - информације се могу копирати у папирном или дигиталном облику
  - решење: строго руковање физичким носиоцима информација
    - не смеју се остављати без надзора
    - морају се уништити након употребе
- Шпијунирање
  - визуално
  - аудио
  - електронско
  - физичко

Социјални фактори

- Разумевање личних и друштвених слабости
  - Вируси, као и хакери, могу да искористе неке слабости
  - Потребно је сагледати и разумети слабости да би се могла припремити одбрана
- Увођење одбрамбених механизама

Уобичајене слабости (1)

- Апатија корисника
  - иако су свесни могућности напада, корисници уобичајено имају став "то се неће догодити мени"
  - лежерно се дели софтвер (програми и подаци)
- Недовољна безбедносна контрола
  - многи рачунари, посебно лични, немају заштиту против вируса и других безбедностних опасности

Уобичајене слабости (2)

- Лоша употреба постојећих безбедносних алата
  - антивирусни програми морају бити ажурни
  - лежерно додељивање виших привилегија него што је неопходно
  - омогућавање слабих лозинки
- Слабости оперативног система
  - ширина и величина оперативних система и другог системског софтвера захтева велики број програмера
  - довољно је да један тим није дорастао послу и остаће неки сигурносни пропуст

Уобичајене слабости (3)

- Неовлашћена употреба
  - постоје људи којима је изазов упадање у туђе системе
  - када једном упадне у систем, изазов да начини штету је велики
- Мрежна анонимност
  - злонамерна особа на мрежи је анонимна, што отежава откривање и олакшава злонамерно поступање

Основна средства за превазилажење слабости (1)

- Тренинзи
  - безбедности службеници морају да буду у току са актуелним проблемима и решењима
- Безбедносна анализа при набавци софтвера
  - пре стављања у рад новог софтвера потребна је одговарајућа безбедносна анализа ради сагледавања и превазилажења евентуалних безбедносних ризика
- Надгледање
  - надгледање корисника
  - надгледање система
  - надгледање мреже

Основна средства за превазилажење слабости (2)

- План за случај опасности
  - при препознавању ванредног случаја се мора реаговати брзо
  - сваки секунд утрошен на размишљање потенцијално увећава штету
  - морају постојати дефинисане прецизне процедуре поступања у ванредним случајевима
- Ограничавање дељења
  - сви дељени ресурси морају бити строго управљани
    - подаци, програми, уређаји, мрежа
  - забрана спољашњих уређаја за пренос података
  - периодично чишћење и склањање података који су били дељени
    - претпоставка је да увек нешто мора да се дели, да би посао могао да се обавља

Основна средства за превазилажење слабости (3)

- Самоизолација у случају напада
  - у случају препознавања да је напад у току, обично је најочигледнија мера потпуни прекид комуникације интерне мреже са спољном мрежом
  - то је извесно темељно супротстављање нападу
  - међутим, ако је пословање тесно зависно од повезаности са спољашњом мрежом, то није добро решење
    - потребно је да план за случај опасности обухвати процедуру којом се искључује што је могуће више комуникације а да се одржи неопходан ниво функционалности система

Основна средства за превазилажење слабости (4)

- Проверавање (аудит)
  - проверавање омогућава уочавање неуобичајених активности и подизања нивоа пажње
- Резервне копије
  - неопходно је имати дефинисану прецизну процедуру прављења резервних копија и извођења поступка опоравка података (и програма)
- Темељна заштита од злонамерног софтвера
  - антивирус програми
  - антишпијунски програми
  - заштитни зид

Принципи управљања безбедношћу

1. Службеник би требало да зна само оно што је непосредно потребно за добро обављање посла за који је задужен
   - информације које нема, запослени не може одати, ни намерно ни ненамерно
2. Потребно је периодично ротирати службенике и радна места
   - службеник коме је досадно је ризичан службеник
3. Сваки осетљив посао мора да обави један службеник и затим да провери други службеник
   - тако се успорава посао, али се подиже безбедност

Литература за тему

- *Solomon*, ***An Introduction to Computer Security: The NIST Handbook***
  - *http://www.davidsalomon.name/*
- Обиље литературе...
  - примери књига:
    - *Jason Andress*, ***The Basics of Information Security***, *Syngress, 2011*
    - *David Solomon*, ***Elements of Computer Security***, *Springer, 2011*