Информациска безбедност

Предавање 1:

Вовед во информациска безбедност

Проф. д-р Весна Димитрова

Вовед

- Што е информациска безбедност?
- На што се однесува информацискатa безбедност?
- Зошто ни е потребна безбедност на информациите?
- Дали е скапа инвестиција да се направи безбеден систем?
- Кои технички решенија постојат за безбедноста на информациите?

Вовед

- Дали може да се направи пресметка за повратокот на инвестицијата која што се инвестира во безбедноста на информациите?
- Дали може да се предвидат најголемите ризици и штетите кои може да настанат при нивна реализација?
- Кои се опасности постојат за безбедноста на нашите информации?
- Дали постојат норми за безбедноста на информациите?

Вовед

- Колку софтверот што го користиме е безбеден?
- Дали интернетот е безбеден?
- Како да ги заштитиме нашите податоци на интернет?
- Дали нашата е-пошта е безбедна?
- Колку се безбедни апликациите кои секојдневно ги користиме?
- Кога еден систем е безбеден?

Вовед

- Норми за безбедност на информациите
  - ISO/IEC 27001:2005 - стандард за воведување на систем за управување со информатичката безбедност
  - ISO/IEC 27002:2007 - множество на препораки за имплементација на безбедносни контроли
  - ISO/IEC 27005:2008: - стандард за управување на ризиците при безбедност на информациите

Вовед

- Закон за заштита на личните податоци
  - - се регулира заштитата на собирање, чување, користење и размена, како и објавување на личните податоци на поединците.
- Закон за електронски потпис
  - - се уредува користењето на електронски потпис во правничкото работење.
- Закон за електронски комуникации
  - - се регулира заштитата на доверливоста на комуникациите.
- Акт за слобода на пристап до информации
  - - се уредуваат правата за пристап до информациите од јавен интерес со кои располагаат органите на јавната власт.

Основни поими

- Цели:
- Дефинирање за информациска безбедност (воведување на поимите: доверливост, интегритет и достапност)
- Наведување на општи одлуки за дизајн кои треба да допринесат за креирање безбедносни системи

Дефиниции

- Безбедност – се однесува на заштита на средствата.
  - Имплицира дека треба да се знаат средствата и нивната вредност.
- **Превенција** - преземање мерки за превенција од оштетување на средствата
- **Откривање** - преземање мерки кои овозможуваат откривање на оштетување на средството, начинот на оштетување и кој го предизвикал
- **Реакција** - преземање мерки кои овозможуваат обнова на средствата или поправка на штетите

Компјутерска безбедност

- Како може да се компромитираат информациските средства?
- Има три аспекти:
- **Доверливост** – спречување неовластено откривање на информации
- **Интегритет** – спречување неовластено изменување на информации
- **Достапност** – спречување неовластено задржување на информации или ресурси

Компјутерска безбедност

- **Доверливост** – спречување неовластено откривање на информации
- Доверливост (приватност, тајност)
  - Неовластените корисници не треба да **дознаат** деликатни информации
- Приватност – заштита на лични податоци
- Тајност – заштита на податоци кои се сопственост на некоја организација

Компјутерска безбедност

- **Интегритет** – спречување неовластено изменување на информации
- Интегритет
  - Осигурување дека се е онака како што треба да биде
- Интегритет
  - Ниту на еден корисник на систем, дури и ако е овластен, не може да му се дозволи да менува податоци така што средствата на организациите ќе бидат загубени или оштетени
- Податочен интегритет
  - Состојба која постои кога компјутеризираните податоци се исти со оние во изворните документи и не се изложени на случајни или злонамерни измени или уништување

Податоци наспроти информации

- Податоците
  - претставуваат информации
- Информација
  - е толкување на податоците

Компјутерска безбедност

- **Достапност** – спречување неовластено задржување на информации или ресурси
- Достапност
  - Пристапност на услугите на производот кога истите се потребни и тоа без застој
- Достапност
  - Пристапност и можност за користење по барање на овластен субјект
- Необезбедување услуга
  - Спречување неовластен пристап до ресурси или предизвикување застој кај временско-зависните операции

Компјутерска безбедност

- **Одговорност** – корисниците треба да бидат одговорни за нивните активности
- Обединувачки концепт на безбедноста, доверливоста, интегритетот и достапноста

Информациска безбедност

- **Информациска/компјутерска безбедност**– се однесува на спречувањето и откривањето на неовластени активности од страна на корисниците на компјутерскиот систем
- **Информациска безбедност**– се однесува на контролирање на пристапот до информации и ресурси

- **Нема една дефиниција за безбедност!!!**

Принципи на безбедноста

- **Фокус на контрола**
  - Во дадена апликација дали механизмите за заштита на компјутерските системи треба да се фокусираат на податоци, операции или на корисници?
- **Ниво човек-машина**
  - Во кој слој од компјутерскиот систем треба да се постави безбедносниот механизам?
- **Сложеност наспроти осигурување**
  - Дали претпочитате едноставност или поголемо осигурување за сигурносна средина со многу карактеристики?

Принципи на комп. безбедност

- **Централизирана или децентрализирана контрола**
  - Дали задачите за дефинирање и спроведување на безбедноста треба да се дадат на централен ентитет или треба да бидат оставени на идивидуалните компоненти на системот?
- **Долен слој**
  - Како да го спречите напаѓачот од добивање пристап до слојот под заштитниот механизам

Автентикација и авторизација

- Автентикација
  - Автентикација е процес на при кој што се одредува дали на даден корисник би требало да му се дозволи пристап од системот. Автентикацијата е т.н. бинарна одлука т.е. пристапот е дозволен или не.
- Авторизација
  - За разлика од автентикацијата авторизацијата се занимава со доделување на соодветни рестрикции и лимитирања за пристап до некаков ресурс на системот. Значи авторизацијата е процесот кој што следува после автентикација.

Автентикација и авторизација

- Разликата помеѓу автентикација и авторизација може да се разбере на тој начин што би се поставиле следниве прашања:
  - Автентикација: Дали си тој кој што кажуваш дека си?
  - Авторизација: Дали ти е дозволено да го правиш тоа?
- Според ова може да се заклучи дека автентикацијата се занимава со корисниците кои што бараат пристап до системот за разлика од авторизацијата која што се занимава со корисниците на кои веќе им е доделен пристап до системот и побаруваат пристап до одредени ресурси од тој систем.

Автентикација

- Во денешно време постојат неколку методи кои што се воедно и најкористени за автентикација на корисници. Овие методи можат да се поделат на:
  - Нешто што поседуваш (Картица за банкомат, смарткарица)
  - Нешто што знеш (Лозинка, ПИН)
  - Нешто што си (Скенирање на отпечатоци, скенирање на глас, ирис)
  - Нешто што правиш (Овој метод најчесто се користи кога корисникот има физички пристап до системот на пример WPS – Wi-Fi Protected Setup каде од корисникот се бара да стисне одредено копче за да може да биде автентициран)

Авторизација

- Системот за авторизација дава одговори на прашањата:
  - Е овластен пристап до ресурси R?
  - Е овластен за вршење на работата P?
  - Е овластен за вршење на работата P на ресурси R

- Овозможува:
  - Контрола на тоа дали одреден корисник има дозвола да користи одреден ресурс или да изврши одредена акција;
  - Верификација на идентитет на корисник или апликација;
  - Верификација на авторски права врз одредна содржина.