18.10.2005.

KOMPJUTERSKI KRIMINALITET

KRIMINALITET – KOMPJUTERSKI KRIMINALITET

- kriminalitet – društveno opasno ponašanje koje je propisima krivičnog zakonodavstva predviđeno kao krivično djelo
- kompjutorski kriminalitet – svi slučajevi zlouporabe kompjuterskih sustava koji su pravno definirani kao kriminalne radnje

KOMPJUTERSKI DELIKVENTI

- mlade obrazovane osobe željne znanja i dokazivanja
- kriminalitet „bijelih ovratnika“ ≈ osobe koje su upoznale mogućnosti računala i koristili u nedopuštene svrhe, zloupotreba sustava
- frikeri (Phreaking = phone + breaking) ≈ izigravale telefonski sustav
- hackeri (to hack = zasjeći, ostaviti trag, udariti, rovariti) ≈ manje opasni od sljedeće kategorije
- crackeri (to crack = praskati, drobiti, uništiti, razbiti)

PRAĆENJE KOMPJUTERSKOG KRIMINALITETA

- početak '60 – prvi radovi u tisku o kompjuterskom kriminalu
- sredina '70 – prve studije, naučna kriminološka istraživanja
- '80 godine – napisi o hakeriranju, kompjuterskim virusima i crvima, širenje piratstva, zloupotreba telekomunikacijskih sustava
- Kompjuterski kriminal se ne ograničava na ekonomski kriminal (stjecanje materijalne koristi), već i ugrožavanje privatnosti (zdravstvene ustanove, banke,…)
- '90 godine – procvat Interneta – različiti ranije poznati oblici kompjuterskog kriminaliteta koriste sve pogodnosti Interneta
- Crna predviđanja – totalna anarhija u informacijskom društvu

KOMPJUTERSKI KRIMINALITET I ZAKONI

- prvi val reformi – donošenje Zakona vezanih uz zaštitu podataka (1973. Švedska, 1974. SAD, 1977. Njemačka,… Hrvatska 2002.)
- Drugi val – zakonima suzbiti nove oblike kompjuterskog ekonomskog kriminala (SAD i Italija 1978.)
- Treći val – početak '80 – potreba za zaštitom intelektualne imovine u elektroničkom obliku (ne više u okviru „druga dijela“) ≈ 1973 u Jugoslaviji
- Četvrti val – kraj '80 i početak '90 – problem odgovornosti osoba koje šire pornografske, rasističke i sl. materijale putem Interneta. Postojeći zakoni proširuju se amandmanima

MOGUĆI NAČINI NAPADA

- neovlašteni pristup tuđem računalnom sustavu
- neovlašteno mijenjanje podataka ili programa
- neovlašteno brisanje i mijenjanje podataka
- presnimavanje nekog malicioznog programa
- korištenje tuđeg računala za pristup u druge računalne sustave
- korištenje tuđeg računala na mreži za pristup drugom sustavu
- nastajanje štete ili uvjeta koji je mogu prouzročiti na infrastrukturi
- krađa. Oštećenje ili uništenje tehničke osnovice ili medija za pohranu podataka

MOGUĆI CILJEVI NAPADA

- korisničke lozinke
- podaci i informacije
- datoteke
- kompjuterski programi
- web stranice
- onemogućavanje korištenja kompjuterskih sustava
- materijalni resursi informacijskih sustava

VRSTE NAPADA

- s obzirom na volju napadača:
  - namjerne napade
  - slučajne napade
- s obzirom na učinak izvršenih radnji
  - aktivni napadi ≈ unutar firme
  - pasivni napadi ≈ bivši zaposlenici, izvan firme
- s obzirom na mjesto s kojeg dolaze
  - unutarnji napadi ≈ ovlaštene osobe
  - vanjski napadi ≈ neovlaštene
- s obzirom na resurse napada
  - napadi na podatkovne resurse ≈ ugrožavanje integriteta podataka
  - napadi na programsku osnovicu
  - napadi na tehničku osnovicu ≈ otežati rad, onemogućiti rad
- s obzirom na cilj napada
  - lažno predstavljanje ≈ socijalni inženjering, telefonsko predstavljanje
  - neovlašteno korištenje resursa
  - uskraćivanje usluga
  - neovlašteno pribavljanje informacija
  - neovlaštena izmjena informacija

RADNJE PRI OSTVARIVANJU CILJA NAPADA

- osigurati pristup računalnom sustavu
- proširiti taj pristup
- poduzeti druge radnje ovisno o svojim motivima
- ukloniti dokaze

METODE KOJE OMOGUĆUJU PRISTUP RAČ SUSTAVU

- društveni (socijalni) inženjering
- lažno predstavljanje
- ispitivanje
- pretraživanje
- prisluškivanje
- optičko špijuniranje
- druženje
- kompromitiranje
- razna programska rješenja

PROŠIRENJE PRISTUPA

- pregledavanje
- korištenje „stražnjih vrata“ i zamki
- legalni programi za analizu i nadzor rada i korištenje sustava
- pomoćni programi (superzap)
- slabosti i greške u računalnim programima

PRIMJENA METODA OVISI O VRSTI NAPADA

- manipulacije s podacima
  - tehnika salame ≈ pomalo skupljanje
  - neposredna izmjena podataka
  - premetanje po podacima
- tehnika uskraćivanja

UKLANJANJE DOKAZA

- brisanje log datoteka

GALERIJA SLAVNIH

- Kevin David Mitnick (Condor)
- John Drapper
- Kevin Paulson („Dark Dante“)
- Richard Pryce („Datastream Cowboy“) i Mathew Bevan („Kuji“)

18.10.05.

MANIPULACIJE POMOĆU RAČUNALA

MANIPULACIJE I RAČUNALO

- računalo kao cilj (objekt, meta) manipulacije
- računalo kao sredstvo (subjekt) manipulacije

RAČUNALO KAO CILJ MANIPULACIJE

- računalni sustav u krivično pravnom smislu predstavlja objekt kriminalnih radnji:
  - napadi na strojnu
  - napadi na programsku
  - računalna špijunaža

RAČUNALO KAO SREDSTVO

- računalo sustav u krivično pravnom smislu služi u svrhu kriminalnih radnji
  - koristeći strojnu
  - koristeći programsku
  - razni oblici manipulacije

RAČUNALO KAO SREDSTVO MANIPULACIJE

- malware – maliciozni software (trojani, crvi…)
- Page Hijacker (otimač stranica)
- Dialer (dial = birati broj) –u trenutku aktiviranja automatski prekida vezu s ISP i uspostavlja vezu s drugim telefonskim brojem – posebne tarifa
- Adware – prikuplja podatke praćenjem navika korisnika tijekom surfanja, ubacuje ciljne mkt i druge promo poruke za vrijeme surfanja
- Spyware – prati korisnikove aktivnosti u radu na računalu (korištene lozinke, broj kreditne kartice, razne druge informacije)
- Cookie ?
- Phishing (password harvesting) = pecanje lozinki, brojeva kreditnih kartica, prodaja korisnikovih podataka
- Spam – svaka elektronička poruka koju korisnik dobije, a koja nema nikakve veze s korisnikom; Hormelov mesni doručak, Leteći cirkus Montyja Pytona
- Hoax – poruka elektroničke pošte neistinitog sadržaja poslane s ciljem dezinformiranja i zastrašivanja. Primatelj prosljeđuje hoax na što veći broj adresa uvjeren da pomaže drugima

25.10.2005.

VIRUSI I ANTIVIRUSNI PROGRAMI

VIRUSI

„Pojavljuju se niotkuda, šire se poput požara i napadaju kako veće tako i manje računalne sustave, oštećuju datoteke čineći računala i mreže neupotrebljivima. Provlače se kroz email..

POVIJEST RAČUNALNIH VIRUSA

- Von Neuman, 1949. g. u knjizi „Teorija i organizacija složenih automata“, teza: *računalni program se može samoreplicirati* ≈ von Neuman iskoristio ideje od C. Babbage
- 1950. Bell Lab, igra“Core Wars“, programi (organizmi) se bore za prevlast nad računalom
- Virusi u stvarnom svijetu pojavom PC (80-tih)

≈ prvi virus po svojstvima samoreplikacije je bio „Rabbit“

≈ ta preteča virusa se otela kontroli i samoreplikacijom usporavala rad računala (disk); UNIVAC 11-15, kopirao se po programima, a ne samo po disku

- 1981. Elk Cloner zarazio Apple II ispisao određenu poruku
- 1983. Len Adleman pri eksperimentalni virus na računalu VAX 11/750

≈ asistent Cohena, Adleman uveo pojam virusa

- 1986. virus Brain, prvi dokumentirani virus infektor datoteka za MS-DOS , ≈ dva Pakistanca, braća, željeli su vidjeti kako brzo i koliko daleko se može širiti zaraza
- 1986. prvi trojan prerušen u shareweare PC Write
- 1990. prvi BBS za kreatore virusa
- 1992. Micheangelo, prvi svjetski raširen virus, 6. ožujska, zarazio oko 20000 računala ≈ po strukturi logička bomba
- 1996. prvi virus za Windows 95, makro virusi za Word i Excel, prvi virusi za Linux
- 1999. Melisa – kombinacija makro virusa i crva, širio se preko maila, crv Loveletter 2000.
- 2002. oko 53000 virusa, mnoštvo mutirajućih virusa

PRVI HRVATSKI VIRUSI

- Bobo-1363 (autor Boris P.) otkriven u Sloveniji 1993.
- Bobo-530, siječanj 1994
- HelpCroatia
- Silent Service

DIJAGNOSTICIRANJE INFEKCIJE

- programi se završavaju ili zamrzavaju
- dokumenti postaju nedostupni
- računalo se zamrzava ili neispravno starta
- povećava se količina datoteka
- na ekranu se pojavljuje čudne poruke
- kolege vas obavještavaju da su primili e-mail, a da se ne sjećate da ste ga uopće poslali
- …..

POSLJEDICE VIRUSNE ZARAZE

- bezopasni oblici
  - ispisivanje poruke

    - sviranje melodije
    - skakanje znakova po ekanu
- štetni oblici
    - usporavanje sustava
    - zamrzavanje sustava
- opasni oblici
    - formatiranje diska
    - mijenjanje podataka
    - brisanje podataka

ŠIRENJE ZARAZUE
- preko zaraženog medija
- datotekama koje se šalju preko mreže
- datotekama preuzetih s Interneta
- preko chata
- datotekama pomoću makroa
- u privitku
- kroz komercijalni software

PONAŠANJE KORISNIKA
- vrlo sigurno ponašanje
    - rad na samostalnom računalu
    - korištenje isključivo komercijalnog software
- umjereno sigurno ponašanje
    - surfanje webom
    - čitanje e-mail
    - chat i razmjena poruka ≈ postoji firewall
- rizično ponašanje
    - razmjenjivanje medija
    - preuzimanje datoteka
    - korištenje freeware, shareware
    - prebacivanje datoteka
    - P2P
    - pokretanje e-mail
    - prihvaćanje datoteka za vrijeme za chat-a

FAZE INFICIRANJA
1. virus je pokrenut
2. kôd virusa je učitan u memoriju
3. virus isporučuje svoj destruktivni sadržaj
4. virus se kopira u druge programe

VRSTE VIRUSA
- infektori datoteka
- boot sektor
- makro
- skript
- trojani
- crvi

- e-mail virusi

VIRUSI – INFEKTORI DATOTEKA
- najtradicionalniji oblik virusa , nekad 85%
- skriva se u kôdu drugog programa
- program mora biti izvršeni, ekstenzije EXE, COM, SYS, BAT, PIF, SCR
- zaraženi program se pokrene, virus se kopira u memoriju prije kôda samog programa. Učitavanjem u memoriju, virus se nastavlja replicirati.

BOOT SEKTOR VIRUSI
- smješteni su na dijelu diska koji se učitava u memoriju prilikom podizanja sustava
- jednom učitan može zaraziti druge diskove
- prijenos korištenjem disketa
- posebno su bili aktivni početkom 1990.

MAKRO VIRUSI
- kreirani pomoću makro jezika
- manji programi kreirani za specifične zadatke u okviru aplikacije
- napisani u pseudoprogramskom jeziku dizajniranom za rad s aplikacijom
- makro jezik – Visual Basic for Aplications – VBA
- dodaje se u Word dokument, koristi se za modificiranje datoteka, slanje e-maila,…

SKRIPTNI VIRUSI
- temelje se na skriptnim jezicima koji se koriste za izradu Web stranica
- pisani su u jezicima: JavaScript, ActiveX, Java aplet
- izvršavaju se automatski pri posjeti Web stranice, otvaranju Word ili Excel aplikacije
- postaju sve popularniji i opasniji

TROJANI
- program koji tvrdi da radi jednu, a u stvari izvodi drugu aktivnost
- šire se e-mailom u okviru privitka

CRVI
- skenira mrežu tražeći računala s odgovarajućim propustom te se na njega kopira i počinje replicirati
- vrlo brzo može usporiti ili srušiti mrežu

E-MAIL VIRUSI
- distribuiraju se preko privitka uz e-mail poruku
- obično su zasebni programi (trojani) i aktiviraju se otvaranjem privitka
- maskiraju se u slike, Word datoteke, ali i u izvršne datoteke
- mogu se slati i na adrese iz adresara u računalu
- u 2001.g izazvali su 90% svih napada

OSTALE VRSTE VIRUSA
- logička bomba
  - slična trojanskom konju
  - aktivira se pri ispunjenju određenog uvjeta

- zečić - kopira svoju datoteku dok ne nestane prostora na disku
- bakterija – širi se po svim diskovima u sustavu, ali samo u jednoj kopiji

ŽIVOTNI CIKLUS RAČUNALNOG VIRUSA

1. kreiranje (virus se kreira)
2. replikacija (virus se kopira na računalo)
3. aktiviranje (virus se aktivira, isporučuje svoj sadržaj)
4. otkrivanje (virus je detektiran i dokumentiran)
5. asimilacija (u antivirusne programe se dodaje prepoznavanje novog virusa)
6. istrebljivanje (korištenjem antivirusnog programa virus se eliminira)

KARAKTERISTIKE VIRUSA

- većina virusa- kratki životni vijek
- javljaju se nanesu štetu
- otkriju se antivirusnim alatom
- razviju zaštitne mjere
- nestaju vrlo brzo
- mogu se pritajiti, mutirati

TEHNIKE PRIKRIVANJA

- **šifriranje (enkripcija)** prikrivanje sadržaja – nije moguće šifrirati cijeli virusni kôd, dio virusa koji služi za dešifriranje mora ostati nepromijenjen
- **višeobličje (polimorfizam)** – vrši se preoblikovanje izvršnog koda na način da se funkcija kôda očuva, a izgled bitno izmjeni
- **samosakrivanje (stealth)** – najraširenija tehnika, varanje da se sa sustavom ne događa ništa neobično.

ŠTO NAKON ZARAZE

- završiti posao
- ugasiti računalo
- izolirati računalo ako je spojeno na mrežu
- pokušavati utvrditi o kojem se obliku virusa radi
- učitati operativni sustav s originalne instalacije
- antivir alatom pokušati ukloniti virus

ANTIVIRUSNE METODE

- pripremanje obrane
  - regularne i oporavka podataka
  - čisti boot disk
- prevencija
  - stvaranje korisničke savjesti
  - unošenje“pravila higijene“
  - nemogućnost podizanja sustava s diskete
  - korištenje legalnog software-a
- detekcija
  - skeneri
  - checkcummeri
  - monitori
- izoliranje sustava

- povratak podataka
  - identifikacija zaraženog
  - eliminiranje virusa
  - popravak popratnih pojava

8.11.05.

RIZIČNA STANJA U PROCESU ELEKTRONIČKE OBRADE PODATAKA

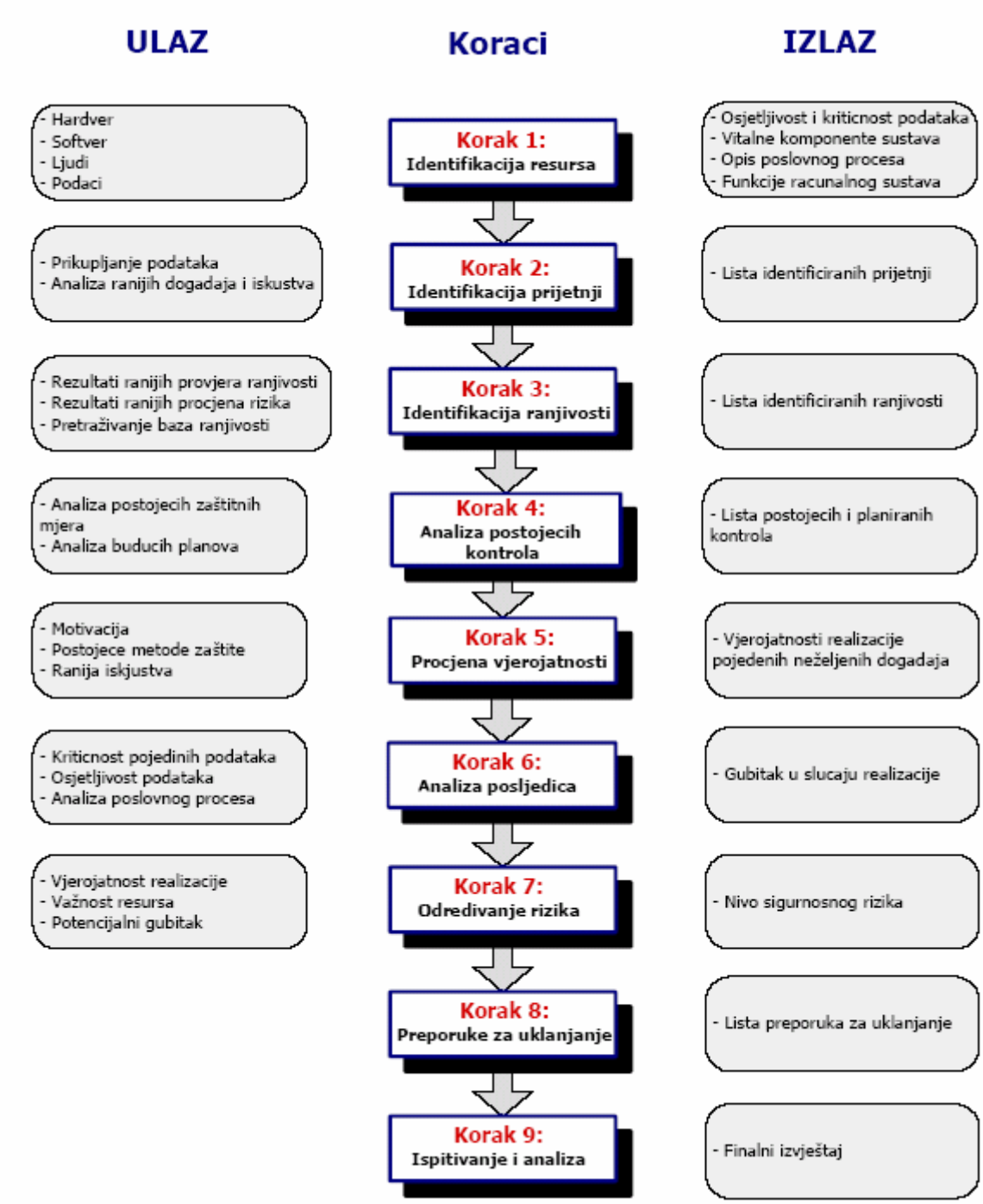
- u pripremi predavanja korišten je rad „Upravljanje sigurnosnim rizicima“ (CCERT-PUBDOC-2003-10-44)
- CARNet CERT, www.cert.hr

UPRAVLJANJE SIGURNOSNIM RIZIKOM

- SIGURNOSNI RIZIK – mogućnost realizacije nekog neželjenog događaja koji može negativno utjecati na povjerljivost, integritet i raspoloživost informacijskih resursa
- UPRAVLJANJE SIGURNOSNIM RIZIKOM – **proces identifikacije** onih čimbenika koji mogu negativno utjecati na povjerljivost, integritet i raspoloživost računalnih resursa, kao i njihova analiza u smislu vrijednosti pojedinih resursa i troškova njihove zaštite
- Koraci u procesu upravljanja sigurnosnim rizikom
  - precizna identifikacija
  - klasifikacija informacijskih resursa
  - poduzimanje zaštitnih mjera
- o poduzimanju zaštitnih mjera odlučuje management poduzeća ≈ radi alokacije financijskih sredstava
- proces upravljanja sigurnosnim rizikom sastoji se od 3 faze:
  - procjena rizika
  - umanjivanje rizika
  - ispitivanje i analiza rizika

PROCJENA RIZIKA

- odnosi se na konkretno određivanje sigurnosnog rizika
- uključuje i:
  - detaljnu analizu svih prijetnji
  - vjerojatnost realizacije rizika i mogućih posljedica
  - cost-benefit analizu sigurnosnih kontrola za uklanjanje rizika
- vrlo složen i zahtjevan posao
- proces procjene rizika sastoji se od devet koraka:
  - identifikacija i klasifikacija resursa
  - identifikacija prijetnji
  - identifikacija ranjivosti
  - analiza postojećih kontrola
  - vjerojatnost pojave neželjenih događaja
  - analiza posljedica
  - određivanje rizika
  - preporuka za umanjivanje rizika
  - dokumentacija



Izvor: Upravljanje sigurnosnim rizicima CCERT-PUBDOC-2003-10-44, str 6.

Rizik se može izraziti kao:

***Rizik* = f(*Prijetnje, Ranjivosti, Vrijednost resursa*)**

IDENTIFIKACIJA I KLASIFIKACIJA RESURSA

- identificirati sve resurse i pridijeliti im odgovarajuću (novčanu) vrijednost
- osim inicijalnih troškova nabave treba voditi računa i o:
  - troškovima razvoja
  - troškovima održavanja i administracije
  - troškovima edukacije
  - vrijednost koji taj resurs ima za konkurenciju

  - troškovi zamjene, nadogradnje
- tipični resursi su:
  - hardver
  - softver
  - podaci
  - ljudski resursi
  - ….

IDENTIFIKACIJA PRIJETNJI

- sigurnosne prijetnje – svi neželjeni faktori koji se mogu negativno odraziti na integritet, povjerljivost i dostupnost resursa
- izvor prijetnji
  - namjerni – ciljano iskorištavaju nedostatke u sustavu svrhu neovlaštenog pristupa (virusi, neovlašteni korisnici)
  - nenamjerni – rezultiraju slučajnim iskorištavanjem ranjivosti u sustavu (elementarne nepogode…)
- generirati listu svih prijetnji, važno !
- voditi računa o svim ranijim incidentima
  - motivima koji su podloga za napad
  - lokacijama napadnutih resursa
- u tu svrhu
  - upoznati firmu (analiza postojećeg stanja)
  - spoznati želje i planove firme (odnosi s okolinom, klima prema EOP)
- metode uočavanja rizika:
  - snimanje tokova dokumenata ili podataka
  - intervjuiranje različitih struktura
  - praćenje protokola rada računala
  - provjeravanje financijskih pokazatelja
- prijetnje tipične za informacijske sustave:
  - neovlašteni korisnici
  - maliciozni programi
  - elementarne nepogode
  - korisničke pogreške
  - krađe
  - greške u programiranju
  - neispravno rukovanje resursima
  - industrijska špijunaža
  - interni napadi
  - ….

IDENTIFIKACIJA RANJIVOSTI

- ranjivost – svi propusti i slabosti u sustavu sigurnosti koji omogućavaju provođenje neovlaštenih aktivnosti
- ranjivost može biti posljedica:
  - pogreške u procesu dizajna ili implementacije sustava
  - propusta u provođenju sigurnosnih pravila i procedura
  - pogreške u programskom kôdu
  - površno implementirana fizička sigurnost
  - nepoznavanja i neprikladnog odabira tehnologija, alata
  - propusta u održavanju sustava

- poželjno je ranjivost analizirati u kombinaciji sa identificiranim prijetnjama (parametri su međusobno povezani)
- nema prijetnje koja koristi ranjivost, ne postoji sigurnosni rizik, nema potrebe razvijati zaštitu

Ranjivost	Prijetnja
Sigurnosni propusti u programskom kôdu	Neovlašteni korisnici Maliciozni programi Nezadovoljni zaposlenici Teroristi
Neprikladna konfiguracija vatrozida	Neovlašteni korisnici Maliciozni programi Industrijska špijunaža
Nedostatak protupožarne zaštite	Požar
Nedostatak antivirusne zaštite	Maliciozni programi (virusi, crvi, trojanski konji).
Nekontrolirano korištenje modema	Neovlašteni korisnici Maliciozni programi Bivši i nezadovoljni zaposlenici

Izvor: Upravljanje sigurnosnim rizicima CCERT-PUBDOC-2003-10-44, str 8.

- rezultat ove faze: detaljna lista ranjivosti sustava i mogućih prijetnji, vidi gore

ANALIZA POSTOJEĆIH KONTROLA

- cilj: analizirati kontrole koje su već implementirane ili se namjeravaju implementirati u svrhu zaštite informacijskih resursa
- sigurnosne kontrole:
  - tehničke – implementirane su u oblik hardware, software ili nekog drugog rješenja (vatrozid, AV zaštita, sustav kontrole pristupa
  - ne tehničke – poput sigurnosnih politika, preporuka i procedura…

VJEROJATNOSTI REALIZACIJE

- voditi računa i o:
  - motivaciji i interesu izvora prijetnji
  - karakteru ranjivosti
  - prisutnosti i kvaliteti postojećih sigurnosnih kontrola
- iskazivanje vjerojatnosti realizacije – deskriptivno (visok, srednji i nizak stupanj), svaki stupanj ima svoju težinu

Vjerojatnost	Definicija
Visoka	Izvor prijetnje je posebno motiviran za iskorištavanje ranjivosti s obzirom na mogućnost dolaska do povjerljivih podataka. Postojeće sigurnosne kontrole su nedovoljne ili sadrže slabosti koje omogućuju zaobilaženje definiranih sigurnosnih mjera.
Srednja	Izvor prijetnje je djelomično motiviran. Iako postoje mogućnosti za iskorištavanje ranjivosti postojeće kontrole to otežavaju.
Niska	Izostanak motivacije za iskorištavanje ranjivosti. Sigurnosne kontrole kvalitetno su implementirane i iskorištavanje ranjivosti prilično je otežano.

Izvor: Upravljanje sigurnosnim rizicima CCERT-PUBDOC-2003-10-44, str 10.

- rezultat ove faze: definirane su vjerojatnost iskorištavanja pojedinih ranjivosti identificiranih u prethodnom koraku s obzirom na navedene prijetnje

ANALIZA POSLJEDICA

- analiziraju se mogući gubici u slučaju iskorištavanja pojedine ranjivosti
- potrebno je voditi računa o:
  - namjeni i ulozi resursa u poslovnom procesu
  - kritičnosti resursa
  - osjetljivosti podataka
- podatke je moguće dobiti analizom postojeće dokumentacije (Izvještaj o neželjenim utjecajima na poslovni proces)

ANALIZA POSLJEDICA (KATEGORIZACIJA POTENCIJALNIH GUBITAKA)

Gubitak	Definicija
Visok	Iskorištavanje ranjivosti može rezultirati: – trajnim gubitkom ili uništenjem resursa, – ozbiljnim ugrožavanjem poslovnih ciljeva i misije organizacije, – ozbiljnim ugrožavanjem ljudskih resursa.
Srednji	Iskorištavanje ranjivosti može rezultirati: – djelomičnim gubitkom ili uništenjem resursa, – djelomičnim narušavanjem poslovnih ciljeva i misije organizacije, – djelomično ugrožavanje ljudskih resursa.
Nizak	Iskorištavanje ranjivosti može rezultirati: – lakšim oštećenjem resursa, – primjetnim narušavanjem poslovnih ciljeva i misije organizacije.

- kvalitativna analiza
  - prednosti: jasni i pregledni rezultati o kritičnim komponentama
  - nedostaci: ne sadrže konkretne brojeve koji bi olakšali analizu dobiti i gubitka
- kvantitativna analiza
  - nedostaci: brojni izračuni i kalkulacije , teško ih je interpretirati
- najbolje – kombinirati obje vrste analize

ODREĐIVANJE SIGURNOSNOG RIZIKA

- potrebno odrediti sve parove prijetnja/ranjivost i uzeti u obzir
  - vjerojatnost iskorištavanja pojedine ranjivosti od strane pripadajuće prijetnje
  - posljedice u slučaju uspješne realizacije
  - kvalitetu i pouzdanosti postojećih i planiranih sigurnosnih kontrola
- kreirati matricu rizika

PREPORUKE ZA UMANJENJE RIZIKA

- cilj : analiza mogućih načina zaštite u svrhu umanjenja rizika
- kod preporuka za implementaciju sigurnosnih kontrola voditi računa i:
  - pouzdanosti i kvaliteta kontrola
  - troškovi implementacije i održavanja
  - sigurnosna politika organizacije
  - pravna ograničenja
  - globalnom utjecaju na poslovanje
  - navikama i mogućim reakcijama korisnika

- krajnji rezultat procjene rizika – preporuke za implementacija sigurnosnih kontrola
- same preporuke su ulazni parametri za analizu i evaluaciju danih preporuka te njihovu implementaciju prema prioritetima i mogućnostima organizacije
- implementiraju se one preporuke koje prođu cost/benefit analizu, analizu funkcionalnosti, analiza ostvarljivosti

ZAVRŠNA DOKUMENTACIJA
- prikazuje dobivene rezultate iz svih faza procjene rizika
- isporučuje s managementu
- management donosi odluku o daljnjim koracima
    - umanjiti rizik(e) i na koji način
    - koje rizike prihvatiti

≈ dodano iz slideova:
UMANJIVANJE RIZIKA

OPCIJE ZA UMANJIVANJE RIZIKA
- *umanjivanje rizika* – implementacija odgovarajućih sigurnosnih kontrola s ciljem umanjivanja identificirajućeg rizika
- *transfer rizika* – rizik i troškovi u slučaju realizacije rizika prebacuju se na drugu organizaciju
- *prihvaćenje rizika* –
    - rizik se prihvaća bez implementacije ikakvih sigurnosnih kontrola (trošak ulaganja u zaštitu je već i od gubitaka ako se rizik ostvari)
    - velika odgovornost ovakve odluke (u pisanom obliku)
- *odbacivanje rizika* – potpuno zanemarivanje sigurnosnog rizika (ignoriranje rizika – neprihvatljiv pristup)

METODOLOGIJA RUKOVANJA RIZICIMA
- pravila:
    - rizik se otklanja po prioritetu
    - implementiraju se ona rješenja koja su financijski isplativa
    - implementiraju se ona rješenja koja će rezultirati što kvalitetnijim i što pouzdanijim sigurnosnim kontrolama
    - određivanje prioritetnih akcija
    - evaluacija preponuđenih sigurnosnih kontrola
    - analiza dobivenog i uloženog
    - odabir sigurnosnih kontrola
    - podjela odgovornosti
    - izrada plana za implementaciju sigurnosnih koraka
    - implementacija kontrola

15.11.2005.

OCTAVE
The Operationally Critical Threat, Asset and Vulnerability Evaluation

OCTAVE

- Razvijena 2001. na Software Engineering Institute na Carnagie Mellon University, SAD
- Metoda je besplatna
- Metoda procjene sigurnosnog rizika
- Evaluaciju rizika provodi interdisciplinarni tim
- Metoda se razvija kroz tri koraka:
    - definirati profil prijetnji
    - identificirati ranjivost infrastrukture
    - razviti sigurnosnu strategiju i planove

- **Prijetnja** : indikacija potencijalno neželjenog događaja. Odnosi se na situaciju u kojoj osoba može učiniti nešto neželjeno ili neki događaj koji može uzrokovati neželjene posljedice

PRIPREMNA FAZA (nulta faza)

- dobiti podršku upravljačkih struktura
- oformiti analitički tima
- odrediti područje primjene metode

FAZA 1: RAZRADA PROFILA PRIJETNI PREMA RESURSIMA

- identifikacija razine znanja viših struktura:
    - poslovno važni resursi
    - sigurnosne potrebe
    - sigurnosne prakse
    - organizacijske slabosti
- identifikacija razine znanja izvršnih upravljačkih struktura: ali s svoje perspektive
    - poslovno važni resursi
    - sigurnosne potrebe
    - sigurnosne prakse
    - organizacijske slabosti
- identifikacija razine znanja zaposlenika:
    - poslovno važni resursi
    - sigurnosne potrebe
    - sigurnosne prakse
    - organizacijske slabosti

  ali sa svoje perspektive
- analitički tim analizira sve informacije prikupljene od viših upravljačkih i izvršnih struktura te radnika
- izrađuje profil prijetnji

FAZA 2.: IDENTIFIKACIJA RANJIVOSTI INFRASTRUKTURE

- analitički tim traži ranjivosti (slabosti, propusti) u komponentama (tehnološke ranjivosti):
    - identifikacija ključnih komponenti

- procjena izabranih komponenti

FAZA 3.: RAZVOJ SIGURNOSNE STRATEGIJE I PLANOVA ZA UMANJENJE RIZIKA

- analitički tim identificira rizike prema poslovno kritično važnim resursima i odlučuje kako dalje postupati
  - izrada analize rizika
  - razvoj strategije zaštite
- izrada analize rizika
  - identificira se utjecaj prijetnji na resurse
  - utvrđuje se kriteriji za procjenu
  - procjenjuju se utjecaji na temelju tih rizika
- rezultat: izrada profila za svaki kritično važan resurs
- razvoj strategije zaštite : za organizacijske planove i planove za umanjenje rizika
- više rukovodstvo pregledava, izabire i odobrava strategiju zaštite i planove umanjenja rizika

NAKON PROVOĐENJA **OCTAVE**

- potrebno odrediti načine provođenja kontinuirane provjere sigurnosnog stanja
- raditi na poboljšanju sigurnosnog stanja
- kompletne (ponovne) procjene raditi periodički ili na temelju nekog specifičnog događaja

OCTAVE

- prijetnje možemo promatrati kroz slijedeće:
  - asset – nešto što ima vrijednost za organizaciju (informacija ili osobe..)
  - actor – netko ili nešto što može povrijediti sigurnosne zahtjeve nekog „asset“, razlikujemo one koji dolaze izvan ili unutar organizacije
- motiv – namjerne ili nenamjerne
- access – kako će „asset“ biti napadnut
- outcome – trenutačni rezultat povređivanja sigurnosnih zahtjeva postavljenih pred neko dobro (razotkrivanje, modifikacija, destrukcija, gubitak, prekid…)
- kategorije prijetnji:
  - osoba koje koriste mrežni pristup
  - osobe koje koriste fizički pristup
  - problemi sustavi -
  - drugi problemi – situacije koje se dešavaju izvan organizacije

≈ nađi na Internetu nešto više o „OCTAVE“

15.11.2005.

METODE PROCJENE OPASNOSTI

- 1970. g. – procjene fizičkih opasnosti (požar, krađa, sabotaža)
- rezultat takvih procjena – plan rada u neuobičajenim okolnostima
- R. Courtney – procjena opasnosti unutar EOP

- osnova svake metode – tehnika procjene:
  - kvalitativne metode
  - kvantitativne metode

KVALITATIVNE METODE

- metoda procjene očekivanih troškova pri realizaciji rizičnih situacija
  - Ilinoisova metoda
  - Courtnijeva metoda
  - Poasonova distribucija
- metoda mjerenja relativnih troškova ugroženosti sustava
  - Delphi metoda
  - Primjena gradacije u analizi rizika

KVANTITATIVNE METODE PROCJENE

- matematičke i statističke tehnike
- najčešće odnos:
  - učestalost pojavljivanja ↔ očekivani gubitak ako se opasnost ostvari
- opisne (deskriptivne)
- onda kada se očekivani gubitak ne može ili ne želi iskazati
- kriteriji:
  - način obrade
  - trajanje obrade
  - učestalost izvođenja
  - podložnost otuđivanju

METODA DJELOVANJA OPASNOSTI

- izbjegavanje opasnosti
  - problem – „usko grlo“ – neažurnost
  - povećanje broja unosnih mjesta
  - rad u više smjena
  - ravnomjerna dostava dokumenata
- umanjivanje opasnosti
  - uvođenje kontrole fizičkog nastupa
  - uvođenje kontrole pristupa sustavu
  - uvođenje procesnih ograničenja
  - uvođenje kriptografskog sustava zaštite
- prihvaćanje opasnosti
  - do koje visine gubitka
  - do koje učestalosti
- prijenos opasnosti
  - način obeštećenja
  - štetu nosi sam vlasnik

- štetu snosi s naslova garancije, proizvođač, prodavač ili treća osoba
- šteta se pokriva s naslova police osiguranja

22.11.05.
- kolokvij iz MM

METODA IDENTIFIKACIJE

METODA AUTENTIFIKACIJE
- **identifikacija** – osoba se predstavlja sustavu nekom metodom identifikacije
- **verifikacija** – sustav utvrđuje da li identifikacija kojom se osoba predstavlja sustavu odgovara toj osobi

PROCES AUTENTIFIKACIJE
- identifikacija
- vezivanje identificirajuće karakteristike uz konkretnu osobu
- verifikacija (ponovna identifikacija)
- usporedba
- odluka DA-NE

METODA IDENTIFIKACIJE
- metode fizičkog prepoznavanja (onim što imaš – posjeduješ)
  - ključ – fizička identifikacija/verifikacija
  - značka – vizualna identifikacija/verifikacija
  - kartica s slikom – vizualna identifikacija/verifikacija
  - markirana kartica (magnetski kôd) – identifikacija/verifikacija sadržajem zapisa
- metode logičkog prepoznavanja (onim što znaš)
  - lozinka (određeni niz znakova kojima osoba dokazuje svoju autentičnost)
  - izboru lozinke posvetiti posebnu pažnju
    - jednostavna
      - niz lako pamtljivih znakova
      - niska razina zaštite
      - poboljšati umetanjem znakova
    - jednokratna
      - lista lozinki
      - kombinacije – lozinka za identifikaciju, posebno za prijavu, posebno za odjavu
      - teško pamtljiva
    - identifikacija dijalogom
      - dijalog korisnika i sustava
      - slučajni izbor pitanja
      - ista pitanja svim korisnicima, svaki korisnik svoj odgovor
    - identifikacija procedurom
      - korisnik se identificira
      - računalo šalje pseudo slučajni broj
      - korisnik izvodi poznati algoritam
      - rezultat vraća računalu
      - računalo nad istim brojem izvodi isti algoritam

        - računalo verificira rezultat korisnika
    - tajna lozinka
        - korisnik pamti riječ, frazu, broj
        - računalo traži da korisnik unese samo određene znakove koje selektira generiranjem pseudo slučajnog niza
    - prinudna lozinka
        - samo za iznimne situacije
        - aktivira poziv u pomoć
        - primjenjiv bilo koji način logiranja
- metode biometričkog prepoznavanja (onim što činiš / onim što jesi)

29.11.05.

BIOMETRIČKE METODE IDENTIFIKACIJE

- biometrija = bios + metrika
- identifikacija:
    - onim što jesi
    - ono što činiš
- fizičke osobine:
    - prst
    - šaka
    - zjenica oka
    - šarenica oka
    - lice
- osobine ponašanja
    - govor
    - vlastoručni potpis
    - dinamika tipkanja po tastaturi
    - dinamika hodanja

PROCES IDENTIFIKACIJE/VERIFIKACIJE

- uzimanje identificirajućeg otiska
- pohranjivanje u bazu predložaka
- identifikacija
- verifikacija uzetog i pohranjenog otiska
- odobravanje ili uskraćivanje obavljanja daljnjih postupaka

≈ middleware – software-ski biometrički proizvod koji se koristi za osiguranje komunikacije klijenta i poslužitelja
≈ metoda otiska prsta – dominantna na tržištu
≈ rast prihoda s 250,9mil u 1999. na 1905,4mil u 2005.; djelomično zbog početka primjene tehnologija u industrije koje to nisu prije koristile

case_study: IDENTIFIKACIJA LICA

- do 50 karakteristika lica
- može se koristiti postojeća infrastruktura
- višestruke kamere, stvaranje 3D slike – smanjivanje grešaka
- traženje karakteristika – landmark finding

- koristi se u londonskoj policiji, njemačke putovnice, švedska aviokompanija, maloprodajni lanci koristili morali ukloniti zbog prigovora javnosti
- pitanja:
  - Koja je prednost metode identifikacije lica? „ne zahtijeva fizički kontakt s kamerom i upotreba postojećih uređaja“
  - Navedi primjere korištenja metode identifikacije lica? „ olimpijske igre u sydneyu, londonska policija, njemačke putovnice, švedska aviokompanija

case_study: IDENTIFIKACIJE DLANA

- fizičke karakteristike dlana se ne mijenjaju se tokom života i za svakog čovjeka su jedinstvene
- dosada razvijena 6 uređaja
- ponekad kombinacija otiska prsta (identifikacija) i dlana (verifiakcija)
- širina i duljina prstiju je bitna
- stroj se može prevariti ne prepoznaje živo biće ili lutku
- upotreba: zrakoplovne luke, vrtići, banke, bolnice, fakultetima
- količina podataka za identificiranje korisnika je minimalna
- nedostaci: veličina uređaja i cijena; ozljede na dlanu mogu prouzročiti teškoće kod čitača pri identifikaciji, mala količina podataka koja se traži može doći do dupliciranja podataka
- pitanja:
  - Kako funkcionira uređaj za identifikaciju dlana? „ skenira se širina i duljina prstiju, skenirana slika se obrađuje
  - Koje su prednosti identifikacije dlana? „ vrlo jednostavno za upotrebu, nema dodatnih problema, količina potrebnih podataka je minimalna“

case_study: IDENTIFIKACIJA POMOĆU OKA

- 1935. početak istraživanja – napis da kombinacija žilica čini jedinstvenu sliku, čak i kod jednojajčanih blizanaca
- 1987. prvi patent
- 1994. prvi algoritam za prepoznavanje
- 1998. prva praktična primjena u ZOI Naganu
- 2004. SAD uvodi biometričku zaštitu za osobe bez vize
- najsigurnija metoda provjere identitete
- retina sa stražnje strane očne jabučice
- nakon smrti brzo propada
- moguće 400 točaka usporedbe nasuprot 30-40 točaka kod otiska prsta
- prvi prototip skenera 1981.
- samo jedan proizvođač
- smetnje skeniranju: naočale, prljavština leće, svjetlo iz okruženja
- registracijski uzorak težak je samo 96B i najmanji je od svih
- skeniranje šarenice, sadrži 266 različitih točaka, formira se krajem 8 mjeseca života
- binarni kod 512B
- vidljiva izvana, uzorci se uzimaju izdaleka, uzorci se uzimaju jednostavno, zjenica se mijenja prema osvjetljenju onemogućava zloupotrebu
- upotreba: 1997. – zrakoplovne luke, bankomati, računala, hoteli
- ugrožavanje ljudskih prava; stalno promatranje građana
- pitanja:
  - Koje su dvije metode identifikacije okom? „skeniranje mrežnice i šarenice“
  - navedite neka mjesta primjene identifikacije okom? „zračne luke, …

case_study: EDGE GRUPA

- IdentiXL BoneID – sustav za praćenja prisutnosti na poslu, kombinira kartice i biometrijske metode
- Fingerscan osnovica BoneID podsustava
- KadEv – podsustav,
- Plaće – podsustav, koji može biti samostalan
- Identix BioLogon – zaštita pristupa IT resursima
- pitanja:
  - Što je IdentiX BoneID sustav – sustav za praćenje prisutnosti na radnom mjstu i obračun radnog vremena
  - navedite aplikacije sustava : klijent-server i porta

POSTUPAK IDENTIFIKACIJE

- jedan –prema-više
  - slijedno pretraživanje svih pohranjenih zapisa
  - direktno pretraživanje upisom šifre osobe koja se identificira
- jedan-prema-jedan
  - identificirajući zapis pohranjen na pametnoj kartici

POSTUPAK VERIFIKACIJE

- jedan prema jedno

KRITERIJI ODABIRA METODA

- **jednostavnost uporabe** (s aspekta korisnika):
  - *identifikacija rukopisom*
  - *glasom*
  - *otiska prsta*
  - *šake*
  - *lica*
  - *šarenice oka*
  - *karakteristikama*
  - *mrežnice oka*
- **pouzdanost metode**

PRIMJENA BIOMETRIČKIM METODA

- tipična područja primjene:
  - pristup u prostore
  - obavavljanje novčanih transakcija
  - pri obavljanju transakcija e-poslovanja

IDEALAN BIOMETRIČKI SUSTAV

- temelji se na
  - apsolutno jedinstvenoj biometričkoj osobini
  - ne-invazivnoj metodi
  - što jednostavniji postupak identifikacije/verifikacije
  - što brža procedura identifikacije/verifikacije

- visoka razina sigurnosti cijelog postupka

TRENDOVI U BIOMETRIJI

- primjena middleware-a
- višeslojna identifikacija
- migracija identificirajućeg uzorka na pametnu karticu
- standardizacija

BIOMETRIČKI MIDDLEWARE

- je softver koji povezuje dvije odvojene aplikacije
- spona između odvojenih aplikacija ili baza podataka

VIŠESLOJNA IDENTIFIKACIJA

- multimodalni identifikacijski sustavi zahtijevaju da se proces identifikacije verifikacije temelji na provjeri više od jednog identificirajućeg parametra
- multimodalnost „ili/ili“ – zahtijevaju verifikaciju samo po jednoj identificirajućoj karakteristici odnosno samo po jednom uzorku
- asinkrona multimodalnost – slijedno verificirati s više biometričkih karakteristika
- sinkrona multimodalna – u jednom procesu autentifikacije zahtijevaju multimodalni prostup
- ako se id postupak temelji na karakteristikama lica i glasa, osoba se u procesu verifikacije mora verificirati istodobno karakteristikama lica i glasa

BIOMETRIČKA PAMETNA KARTICA

- Mach-On-Card(MOC) – identificirajući biometrički uzorak pohranjuje u čipu karticu
- identifikacija/verifikacija 1:1
- BAI pametna kartica s modulom za autenkaciju
- korisnik odgovoran za čuvanje uzorka

6.12.05.
METODE PROVJERE PRISTUPA I OVLAŠTENJA

KARAKTERISTIKE IS-a
- **otvoren** – pristup dozvoljen svima osim onih kojima je pristup formalno zabranjen
- **zatvoren** – pristup dozvoljen samo onim korisnicima kojima je posebno odobren

Privilegirani minimum – najmanja količina ovlaštenja kojom korisnik može normalno obavljati povjerene mu zadatke
- dodjela ovlaštenja može biti:
  - izvođenje aplikacija
  - rad s podacima
  - rad s uređajima

DODJELA OVLAŠTENJA PRI RADU S PODACIMA
- **kontrola pristupa povezana s sadržajem** – korisnik može pristupiti samo podacima koji se sadržajno odnose na njegov djelokrug rada. neke podatke može samo pogledati, neke ažurirati i sl.
- **kontrola funkcionalnog pristupa** - korisnik može imati pristup zbirnim, ali ne i pojedinačnim podacima.
- **kontrola pristupa povezana s kontekstom podataka** – korisniku treba ograničiti pravo raspolaganja podacima koji imaju istovremeni pristup
- **kontrola pristupa povezana s ranije pribavljenim rezultatima obrade**- potrebno je spriječiti mogućnost stvaranja neželjenih semantičkih zaključaka

ZAŠTITA PODATAKA
- ostvarivanje zaštite vrši se na razini operacijskog sustava
- zaštita se realizira:
  - utvrđivanje …..

- kontrola:
  - pristup sustavu
  - pristup resursima
  - pristup podacima
  - funkcija sustava

OBLICI ZAŠTITE
- **lozinkom** – kreirati korisnički profil (omogućava identifikaciji i verifikaciju te ovlaštenja; definiraju se klase korisnika
- **terminala** – verifikacija ovlaštenja nad terminalima
- **kod prijavljivanja na sustav**
- **zaštita ograničavanjem sposobnosti** – određuje se u korisničkom profilu: naredbe koje se smiju koristiti početni programi, početni meni, biblioteke
- **zaštita resursa** - osigurava da korisnici prema dodijeljenim ovlaštenjima koriste upravo te resurse; glavni tipovi su:
  - **specijalna ovlaštenja**: specificiraju se klasa korisnika i specijalna ovlaštenja, omogućuju izvođenje operacija kontrola sustava koja se ne odnose na specifične objekte

        - **specifična ovlaštenja**: ovlaštenja koja definira korisnik (operacije na objektima /podacima); koja definira sustav
- zaštita biblioteka – štite se osjetljivi objekti
- autorizacijske liste
- grupni profil
- vlasnička ovlaštenja – svaki objekt ima svog vlasnika. određeni program ili objekt pokreće se korisničkim profilom. vlasnik određen
- posjednici ovlaštenja

SIGURNOSNE RAZINE

sig. razina 10

- nije potrebna lozinka, nije aktivna razina resursa
- sustav sam kreira korisnikov korisnički profil i dodjeljuje mu ovlaštenja (piši/briši, čitaj, modificiraj, pokreni)

sig. razina 20

- aktivna min. zaštita, treba lozinka
- sve ostalo kao u 10

sig. razina 30

- korisnički profil i ostalo

IDENTIFIKACIJA KORISNIKA I VERIFIKACIJA OVLAŠTENJA

- korisnički profil
    - kreira SECOFR, na najnižoj razini sam sistem (jedan profil-jedan korisnik)
    - ime korisničkog profila
    - lozinka
    - trajanje lozinke
    - korisnička klasa
    - tekuća biblioteka

OVLAŠTENJA BAZAMA PODATAKA

- zaštita pogleda: sustav omogućava selektivno grupiranje podataka u podskupove prema zahtjevu korisnika. Određenim nalozima može se onemogućiti pravo pogleda nad tim podacima
- zaštita autoriziranog rada s podacima – vezana uz dodjelu specijalnih ovlaštenja

ZAŠTITA OSOBA U PROCESU EOP

- zaštita zaposlenih
- zaštita od zaposlenih
- zaštita pomoću zaposlenih

ZAŠTITA ZAPOSLENIH

- **ergonomija** – multidisciplinarna znanstvena disciplina istražuje na koji se način okolina i alati koji se upotrebljavaju u radu mogu prilagoditi psihičkim i fizičkim osobinama ljudi.
- Murell, eng. psiholog, 1949
- radno mjesto – prostorno ograničen i funkcionalno prilagođeno
    - čovjek
    - sredstva za rad (računalo +software)
    - prostor za rad (radna okolina)

Monitor

- elektromagnetsko zračenje (prirodni / umjetni), ne može ga se osjetiti
- mjerenja karakteristima EM polja oko izvora
- snaga zračenja (crno bijeli manje, kolor više)
- oštrina slike (jednobojnio – oštrije, kolor – manje oštro)
- ergonomski zahtjevi:
    - veličina monitora ne manja 14“
    - veličina znakova - najmanje 4mm
    - frekvencija rada monitora – ne manja od 70Hz
    - ne upotrebljavati jake boje (epileptični napadi)

Tipkovnica

- raspored tipki
- oblik kućišta
- sindrom zapestnog prolaza – CTS – ponavljajuće stresne ozljede
- računalna šaka
- ergonomija zahtjevi
    - nagib u odnosu na površinu 5-10º
    - visina tipki 12-15mm
    - razmak među tipkama 18-20mm
    - konkavna površina
    - forma šišmiša

Miš

- vrste:
    - elektromehanički
    - optički
    - pomoćna kugla
    - senzorsko polje
- ergonomski zahtjevi
    - prati oblik šake
    - oblik tipke

Razgibavanje

ZAŠTITA OD ZAPOSLENIH

- **ugrožavanje sustava**
  - *namjerno*: da se dokaže, iz bojazni ugrožavanja radnog mjesta, osvete , koristoljublja
  - *nenamjerno* – nesmotrenost, brzopletost
- **mjere zaštite**:
  - edukacija
  - voditi računa o sposobnosti i sklonostima
  - metode zaštite ne nametati
  - upoznati zaposlene s ciljem mjera zaštite
  - ukazati na kontrolne mehanizme
  - motivirati – sankcionirati
- **socijalni inženjering**
  - alati: telefon, služenje specifičnim jezikom, informacije o sredini u kojoj će se uloga odigrati
  - posebno osjetljivi resursi:
    - lozinke
    - povjerljivi terminali i konzole
    - operativni podaci
    - informacije o klijentima
    - podaci o proizvodima
  - ključne mjere zaštite:
    - lozinke (mijenjati, ne dijeliti)
    - provjera poziva i verifikacija
    - testiranje korisnika
    - izvještavanje o sumnjivim aktivnostima.

ZAŠTITA S ZAPOSLENIMA

Zadovoljan zaposlenik može najbolje zaštiti IS i sve njegove raspoložive resurse.

KRITOLOGIJA

- znanstvena disciplina koja se bavi proučavanjem svih oblika tajne komunikacije
  - razvija se kroz tri područja
    - kriptografija
    - kriptovizija
    - kriptofonija
  - osnovna obilježja kriptologije:
    - namjerno mijenjanje (transformiranje) zapisa
    - tajnost zapisa

Kriptografija

- bavi se proučavanjem i primjenom metoda zaštite pisanih informacija sa ciljem da sadržaj pisane inf bude nerazumljiv neovlaštenom korisniku, a poznat uz primjenu metoda dekripcije autoriziranim korisniku
- počinje se razvijati u društvenim zajednicama nakon što takva zajednica dosegne određenu razinu pismenosti
- da bi se osigurala određena privatnost (tajnost), počinju se razvijati metode i tehnike tajnog komuniciranja
- kriptografija se spontano razvijala u potpuno prostorno odvojenim
- Egipat – cca 1900 pne na grobnica Khnumhetopa II namjerno zamijenjeni neki hijeroglifski znakovi drugima. kasnije nadgrobni spomenici pisani u obliku rebusa
- Kina – slaba primjena kriptografije, više steganografije
- Indija – poznato nekoliko oblika tajnog komuniciranja: tajno pismo, tajni govor, govor prstima
- Mezopotamija – najstariji kriptogram 1500 pne; kodna knjiga iz Suze
- Skandinavija (7-8-9st runsko pismo)
- Perzija 10st – primjera monoalfabetske zamjene – slova alfabeta zamjenjuje se imenima ptica, slova alfabeta astronomskim lunarnim terminima

Kriptografske metode

- transpozicija (premještanje) – kojom se slova OT premještaju, razbacuju u odnosu na OT prema određenoj metodi
  - linearno, …
- supstitucija (zamjena) – metoda kojom se slova OT zamjenjuju slovima alfabeta šifarske zamjene
  - mono – mono
  - mono – poli
  - poli –mono
  - poli – poli
  - nomenklature
  - kodne knjige

Naprave za ručno šifriranje

- maske
- zasunke : obične, dva ili više alfabeta
- diskovi i kotačići – cirkularne ploče, alfabetski kotač

Strojevi za šifriranje

- pisači strojevi s promjenom šablone
- pisači strojevi s promjenom slovčanih oznaka

- B-21 naprava koja je funkcionirala na principu šahovske ploče (Boris Hagelin, 1925.)
- M-209 sustav zupčanika s varijabilnim brojem zubaca
- električni stroj za šifriranje (Edward Hugh Hebern 1915.)
- ENIGMA – Artur Sherbius

KRIPTOANALIZA

- bavi se razbijanjem kodova, šifri
- kriptoanalitičar ne poznaje algoritam po kojem je poruka kriptirana ali uspijeva pretvoriti kriptogram u otvoreni tekst
- dekripter – osoba koje se bavi
- Freudman – kriptoanaliza

Klasična kriptoanaliza

- izvrsno poznavanje teorije i metoda kriptiranja
- dobro poznavanje semantičkih i sintaktičkih karakteristika jezika
- matematičar i statističar

Postupak dekriptiranja:

- poznavati učestalost pojave znakova u jeziku
- utvrditi učestalost pojavljivana svakog slova u kriptogramu
- utvrditi veze među slovima: koja se slova dodiruju, koliko različitih slova dodiruje jedno slovo

STEGANOGRAFIJA

- metoda koja se bavi pronalaženjem postupaka kojima je moguće prikriti postojanje same tajne poruke
- klasične metode: u tijelu, na tijelu, u odjeći u uporabnim predmetima
- metode punktiranja
- simpatetičke (nevidljive) tinte

Noviji oblici steganografije

- semagrami – tajni simboli (različit položaj marke na kuverti, dječji crteži. kvazi narudžbe)
- mikrodoti – minijaturne fotografije veličine tiskane točke zalijepljene na pismo kao prijenosni medij

Steganogafija digitalnih podataka

- tajna poruka u digitalnoj slici:
  - umetanjem na mjestu najmanje značajnog bita
    - slika se mijenja ispod razine zamjetljivosti
    - kompresija kao način pred obrade
  - maskiranje i filtriranjem
    - tajna informacija unosi se slično „vodenom žigu“
    - maskiranje samo na dijelu slike
  - algoritmi i transformacijom
    - porijeklo iz digitalne obrade slike i signala

case_study: STEGANOGRAFIJA – SLIKE

- skriveno pisanje
- brijanje glave i tetoviranje (stari grci i II. rat)

- LSB metoda – least sigifiant bit (BMP 1024x768 ima 288KB prostora)
- image downgrading – skrivanje slike u sliku, jednake veličine, 4bita se mijenjaju; slike koje sadrže nepravilnih oblika i prelijevanje boja , mora sadržavati dovoljno redudantnih bitova
- Steganography 1.6.5

pitanja:

1. Što je steganogarfija – znan. disco bavi sakrivanjem podataka
2. koji format slika najćešće koristi LSB metoda? – BMP
3. Kakve slike su dobra steganografska podloga? - puno boja,preljeva i nepravilnih oblika

case_study: STEGANOGRAFIJA zvuka - Boris Belec; Maro

- alat MP3stego, CLI
- alat steganography 1.6.5

pitanja:

1. koji format je najbolja podloga za audio steganografiju

13.12.2005.

SIMETRIČNI I ASIMETRIČNI KRIPTOSUSTAVI

SIMETRIČNI

- ključ kriptiranja je ključ dekriptiranja
- DES (data encription standard)
  - najrašireniji
  - razvijem 1977. IBM
  - baza logička funkcija XOR
  - kriptira blokove duljine 64 bita ključem duljine 56 bita
  - broj mogućih kombinacija ključeva 256
- AES (advanced encription standard)
  - simetrična blok šifra
  - veličina ključa 128, i 192 i 256 , blokovi od 128bitova
- IDEA (international data encription algorithm)
  - 1991., X. Lai i J.L.Massey
  - 64 bita blok i ključ 128 bita
- Blowfish
  - B.Schneier, 1993.
  - Koristi blokove od 64bita i ključeve varijabilne dužine (do 448bita)
- RC2
  - RSA data sec
  - blok 64 i varijabilni ključ
- RC5
  - 128 bita blok, ključ do 2048 bitova

ASIMETRIČNI

- postoje dva komplementarna ključa koji se koriste pri kriptiranju i dekriptiranju
  - privatni ili tajni ključ
  - javni ili opće poznati ključ
- svaka strana kreira par ključeva (tajni i javni) pri čemu se razmjenjuje javni ključ
- postupak kriptiranja: pošiljatelj poruke koristi javni ključ primatelja, primatelj dekriptira koristeći privatni ključ za dešifriranje
- RSA
  - najpoznatiji asimetrični sustav
  - Rivest, Shamir, Adleman
  - algoritam spada pod posebne zakone SAD-a
  - zabranjen izvoz ključeva većih 512B
  - algoritam koristi velike prim brojeve kao osnovu za kriptiranje

DIGITALNI POTPIS

- elektronički generiran potpis
- generira se korištenjem privatnog
- provjera autentičnosti poruke javnim ključem pošiljatelja
- u slučaju naknadne izmjene poruke digitalni potpis neće biti ispravan

≈ Narodne Novine – Zakon o elektroničkom potpisu

- HASH funkcija – matematička funkcija koja se koristi za izračunavanje sažetka poruke fiksne dužine, obično od 128 do 256 bita na temelju ulazne poruke varijabilne duljine.
  - SHA-1

- slaba strana – primatelj mora biti siguran kome pripada javni ključ
- povjerljiva stranka – stranka kojoj obje strane vjeruju i kojoj donose svoje javne ključeve na ovjeru
- prema funkcionalnim karakteristika ne odgovara potpisu tintom
- zakonska regulativa
    - ne određuje tehnologiju (duljinu)
    - mora biti jedinstven
    - mora postojati mogućnost provjere kome digitalni potpis pripada
    - SAD
        - 10.2000. E-sign zakon
        - 1994. DSS digital signature standard (NSA)
        - DSS koristi DSA algoritam
    - RH
        - zakon 2002. o elektroničkom potpisu, ali se stvarno gotovo ne koristi

13.12.05.

PROTOKOLI

SECURE SOCKETS LAYER (SSL)

- Netscape Communications u suradnji s RSA
- ugrađen u većinu aplikacija za razvoj web stranica
- kriptira komunikaciju između kupca i prodavatelja
- podržava različite kriptografske algoritme
- sadrži dva potprotokola
    - SSL Record Protocol – definira format podataka
    - SSL Handshake Protocl – omogućuje razmjenu podataka
- najpoznatiji napad na SSL je: „man-in-the-middle-attack“ - presretanje komunikacije između servera i klijenta; nužna i dodatna provjera domene

SECURE ELECTRONIC TRANSACTION (SET)

- nasljednik SSL
- razvile kartičarske kuće
- objavljen 1996. kao osnovni industrijski standard za zaštitu plaćanja kreditnim karticama preko Interneta
- upravlja grupa kartičara: SET Co. (Visa, MasterCard, American Express, JCB Co.)

ZAŠTITA PODATAKA U PRIJENOSU

Distribuirani računalni sustavi

- je skup neovisnih računala povezanih komunikacijskom mrežom radi obavljanja poslovnih funkcija
- osnovno svojstvo – transparentnost
- evolucija:
    - terminali
    - lokalna mreža
    - globalna mreža

Uređaji za povezivanje mreža različitih arhitektura

- *most* – brine se o izvršnoj i odredišnoj adresi paketa podataka, ima tablicu, izdvaja paketa za lokalnu mrežu

- *usmjernici* – samo protokol lokalne mreže, služi kao firewall
- *pristupnici* – pretvara pakete jedne mreže u pakete druge mreže

Problemi pri umrežavanju
- nepoznate granice
- nepoznati putovi
- neujednačena razina zaštita
- dijeljenje resursa
- kompleksnost sustava

Problemi pri umreženom radu
- korištenje višekratnih lozinki
- rijetko korištenje enkripcije
- rijetko korištenje autentifikacije
- konfiguracije i tehnologija mreže za male, povjerljive mreže
- nedostatak svijesti o opasnostima

Što učiniti?
- nadzor nad svim aktivnostima u mreži –analiza zapisa
- firewall
- enkripcija

Pojednostavljena politika zaštite
- omogućiti korisnicima našeg sustava na Internet, a pristup iz Interneta u naš sustav samo onima koji imaju za to ovlaštenja

Kerberos
- sustav za provjeru autentičnosti
- razvio ga je MIT
- omogućava razmjenu privatnih informacija putem mreže između dviju strana
- jednokratna dozvola – ticket

Firewall
- sprječava neautorizirani pristup iz i u mrežu
- packet filter
  - nadgleda svaki paket u prometu
  - efikasan i transparentan
  - sprečava IP spoofing
- aplication gateway (telnet, ftp…)
- circuit-level gateway
- proxy server

20.12.05.

case_study: PGP , VIDI PREZENTACIJU, U FOLDERU

case_study: SIGURNOSNI PROTOKOLI
- SET i SSL
- SET:
  - 1996, Visa i mastercard

    - koristi certifikate i enkriptira komunikaciju, autentifikacija stranica preko certifikata
    - trgovci vide iznose, ali ne i podatke o karticama, dok kartičar ne vidi o kojim proizvodima se
    - kompatibilnost unutar industrije, zahtjeva posebnu tehnologiju
- SSL:
    - najrašireniji sigurnosni protokol na Mreži
- pitanja:
    - Koja su dva najpoznatija sigurnosna protokola? – SSL i SET
    - Od kojih protokola se sastoji SSL? – SSL handshake i SSL record protokol

case_study: PROTOKOLI, Dalibor Sokolović i Aleksandar Radulović
Internet Protocol (IP)
- omogućava prijenos datagrama od izvora do odredišta koji su opisani konačnom adresom
- dvije osnovne funkcije:
    - adresiranje
    - fragmentacija
- IP je pozvan od strane host-to-host protokola, nakon čega IP zove lokalne mrežne protokole.

Transmission Control Protocol (TCP)
- host-to-host protokol
- šalje i prima segmentirane informacije
- koristi se kao sučelje između viših protokola kao FTP i nižih protokola kao što je IP

File Transfer Protocol (FTP)
- dizajniran za upotrebu od strane programa
    - logični
    - transferni – 8 bitova
- univerzalni prijenos podataka bez obzira na logičku i fizičku strukturu podataka na hostovima

Sigurnost ovih protocola:
- TCP/IP osnova današnjeg Interneta
- nedostatak čak i osnovnih sigurnih mehanizama poput enkripcije i autorizacije
- tipovi napad:
    - TCP „SYN“ napadi
    - IP spoofing
    - pogađanje sekvence
    - connection hijacking
    - RIP napadi, ICMP napadi, DNS napadi
- zaštita:
    - firewall
    - TCP omotači
    - dodatni autorizacija
    - enkripcija SKIP
    - IPv6
        - duljina paketa na 64bita
        - autorizacija

        - ekripcija
        - smanjenje propusnosti zbog enkripcije, problem protokola za razmjenu ključa

- pitanja:
    - Koliko iznosi transfer bajt veličina kod FTP- 8 bitova
    - Glavni nedostatak Internet protokola (v4) – nedostatak autorizacija i enkripcije

PRIJEDLOG MODELA ORGANIZACIJE SUSTAVA ZAŠTITE

Organizacija sustava zaštite

- proces računalne obrade podataka postavlja pred sustav zaštite tri zahtjeva:
  - sigurnost
  - raspoloživost
  - tajnost podataka
- sustav zaštite direktno je povezan s ustrojem samog poduzeća. razina organiziranosti sustava zaštite mora pratiti razinu organiziranosti procesa obrade u poduzeću
- prema načinu organiziranosti procesa računalne obrade podataka razlikujemo:
  - proces računalne obrade podataka organiziran na *centralizirani način* na jednom ili više zasebnih računala
  - na decentraliziran na više umreženih računa na jednoj ili više lokacija
- organiziranost sustava zaštite s aspekta podataka (informacija) pratimo prema kriterijima:
  - sigurnost izvođenja obrade
  - raspoloživost
  - tajnost

CENTRALIZIRANI NAČIN OBRADE PODATAKA

- karakteristike:
  - manji obuhvat
  - obradu obavlja jedna ili više osoba, ali autonomno

Kriterij: Sigurnost izvođenja obrade

- razlikujemo:
  - aktivnosti koje prethode samom procesu obrade
  - postupke prikupljanja podataka
  - proces obrade
  - postupke pohranjivanja rezultata obrade
  - postupke distribucije rezultata obrade
- aktivnosti koje prethode samom procesu obrade:
  - radno ispravno, dovoljno snažno računalo
  - legalno pribavljen software
  - kvalitetan software
  - dobro educirano osoblje
  - osigurani izvori napajanja
  - servis održavanja
  - „plan poslije“
  - „hladni back up“
- prikupljanje podataka:
  - odrediti način dostave podataka
  - osigurati ispravnost ulaznih podataka
  - osigurati ispravnost unosa podataka
- proces obrade: moguće ga je uspješno obaviti ako su predradnje i unos korektno obavljeni
- rezultati obrade:
  - privremeni
  - trajni
- potrebno je osigurati:

- pohranjivanje rezultata obrade na najsigurniji raspoloživ način
- stvaranje sigurnosnih kopija
- pohranjivanje sigurnosnih kopija na najmanje dva izdvojena mjesta

Kriterij: Raspoloživost informacija

- jedna osoba – bez mjera provjera identiteta
- više osoba – svakoj odrediti konkretne oblike identifikacije (obavezna provjera identiteta i ovlaštenja)

Kriterij: Tajnost podataka

- ako je potrebno, odrediti mjere zaštite. inače, na ovoj razini se ne predviđa zaštita tajnosti podataka

Prijedlog ustrojstva zaštite – centralizirani način obrade podataka

- u pravilu- razvijanje metoda zaštite vezanih uz kriterij sigurnosti
- ako više osoba koristi isto računalo : provjera identiteta i ovlaštenja

DECENTRALIZIRANI NAČIN OBRADE PODATAKA

- mogućnosti
  - na jednoj lokaciji
  - na dislociranim lokacijama

Kriterij: sigurnost izvođenja obrade

- uz sve navedeno za isti kriterij pri centraliziranom načinu obrade i:
  - korektno instalirana mreža
  - komunikacijski software
  - dodatni uređaji (firewall, gateway)
  - služba održavanja

Kriterij: raspoloživost podataka

- identifikacija/verifikacija
- provjera ovlaštenja korisnika

Kriterij: tajnost podataka

- kriptografske metode zaštite
  - metode nadkriptiranja
- digitalno potpisivanje i sl.

20.12.05.

INTEGRACIJA U MODEL

Prijedlog modela

- model sustava zaštite treba razvijati kroz tri razine zaštite tako da svaka slijedeća viša sigurnosna razina uključuje i prethodnu razinu zaštite
- prva razina : osigurati kontinuirani proces obrade
- druga razine: autentifikacija, ovlaštenja i raspoloživost resursa, zaštita na mreži
- treća razina: dodatni oblici zaštite

Prva razina modela zaštite

- metoda fizičke zaštite
- provjera ispravnosti strojne potpore
- zaštita ispravnosti programske potpore
- zaštita osiguravanja tehničkog pogona
- zaštita korektnosti unosa podataka
- zaštita pohranjenih nosilaca podataka
- zaštita načina distribucije rezultata obrade

Druga razina modela zaštite

- identifikacija mjesta ulaska u sustav
- identifikacija korisnika
- autorizacija korisnika
- autentifikacija korisnika
- zaštita podataka u prijenosu

Treća razina modela zaštite

- Dodatni oblici zaštite u segmentima obrade gdje je to potrebno
    - razvrstati prema kriterijima važnosti
        - svima dostupni
        - podaci za internu uporabu
        - povjerljivi podaci
        - tajni podaci
    - gradacija mjera zaštite
        - nisu potrebne nikakve
        - jednostavne
        - pooštrene
        - rigorozne mjere zaštite

20.12.05.

VRIJEDNOST INFORMACIJA

- osnovna pitanja:
  - koliko su troškovi pribavljanja željenih informacija
  - kolika je njihova uporabna vrijednost
  - koliko je period iskoristivosti informacija
- direktni troškovi
  - troškovi projektiranja IS
  - eksploatacija hardvera i softvera
  - troškovi obade (od prikupljanja podataka do distribucije rezultata)
  - režijski troškovi
  - potrošni materijalni
- uporabna vrijednost informacija
  - korisnost
  - što je informacija – roba, intelektualna usluga,…
  - dva oblika:
    - ulazna informacija – uporabna vrijednost to veća što se može iskoristiti za više različitih obrada
    - izlazna informacija – uporabna vrijednost to veća što je više situacija u kojima se ta informacija može koristiti
  - koeficijent korisnosti informacija $= \frac{efekti\_od\_korištenja}{troškovi(prikupljanje, obrada)}$
- vijek trajanja informacija
  - eksploatacijom se ne uništava sadržaj
  - korištenje ne smanjuje uporabnu vrijednost
  - traje, kolika je potražnja

20.12.2005

PROCJENA USPJEŠNOSTI ORGANIZACIJE ZAŠTITE

koeficijent (uspješnosti) zaštite (K) $= \frac{ukupni\_efekti}{ukupni\_troškovi\_zaštite}$

- potrebno je utvrditi troškove zaštite prema mjestu nastajanja troška (mjesta primjena metoda mjera zaštite)
- efekte od primjene metoda zaštite teško kvantitativno odrediti (procijeniti)
- pri izračunavanju koeficijenta uspješnosti zaštite tri su odnosa posebno važna:
  - K >1 ulaganja manja od efekata
  - K = 1 ulaganja jednaka efektima
  - K< 1 ulaganja veća od efekata

17.1.2006.

SIGURNOSNA POLITIKA

Sigurnosna politika

- strategija ponašanja – kako zaštiti dobra tvrtke
- potreban osnovni dokument koji određuje strategiju ponašanja tvrtke i daje smjernice za razvijanje dokumenta poznatog pod nazivom „plan poslije“ ili „plan za nepredviđene okolnosti“ (Disaster Recovery Plan)
- informacija je najvažniji resurs poduzeća, premda se ona uopće ne smatra resursom od osobite važnosti.

Razlozi razvijanja sigurnosne politike

- Sigurnosnom politikom definiraju se uloge i odgovornosti zaposlenika (korisnika, davatelja informatičkih usluga, osobe zadužene za sigurnost sustava, poslovodstva,…)
- Glavni principi
  - podjela odgovornosti
  - razdvajanje uloga

Sigurnosna politika obuhvaća (www.borea.hr)

- rad osoblja
- fizička sigurnost i sigurnost radne okoline
- sigurnost produkcijskog sustava
- plan djelovanja u slučaju nepredvidivih okolnosti
- kontrola pristupa
- vođenje promjena na sustavu
- vođenje evidencije o radu sustava
- korištenje elektroničke pošte
- obaveza pridržavanja

17.1.2006.

PRAVNA ZAŠTITA PROGRAMSKIH PROIZVODA I OSOBNIH PODATAKA

MOGUĆI OBLICI PRAVNE ZAŠTITE RAČUNALNOG SOFTWARE-A

- zaštita autorskim pravom
- patentnim pravom
- ugovorom
- trgovačkim znakom

AUTORSKOPRAVNA ZAŠTITA

- polazi od prava intelektualnog vlasništva
- računalni programi – intelektualna tvorevina, nastala naporom stvaratelja, pripadaju sva prava koja su u vezi s tvorevinom
- zakon o autorskom pravu – 1978., 1986., dopuna iz 1990., eksplicite spominje računalni program, ne software
- autor djela
  - imovinska prava (objavljivanje, reproduciranje, umnožavanje, stavljanje u promet), prenosiva
  - moralna prava (da bude priznat, označen kao autor djela, može se suprotstaviti uporabi djela) u pravilu neprenosiva, samo nasljeđivanje
- iskorištavanje računalnog programa – dobiva se i plaća pravo na korištenje
  - reproduciranja

    - umnožavanja
    - preradu
    - stavljanja u promet
- računalni program može biti stvoren:
    - u radnom vremenu
        - imovinska – poslodavac
        - moralna – autor
    - u okviru ugovora o djelu
        - moralna i imovinska pripadaju autoru, imovinska prava dalje prema ugovoru
- korištenje autorskog djela bez dozvole autora i plaćanje naknade:
    - nastava
    - osobno usavršavanje
    - davanje recenzija
    - reproduciranje ili pribavljanje kopija za svrhu za koju je program pribavljen (arhiviranje, zamjena izgubljenog, dotrajale kopije…)
- trajanje zaštite
    - pojedinac – za života + 50 godina nakon
    - poduzeće – 50 godina od stvaranja
    - moralna – autor za života, nakon toga nasljednici
- kaznene odredbe:
    - to pod svojim imenom ili imenom drugoga objavi, prikaže, izvede ili prenese tuđe djelo – novčana kazna ili zatvor do 5 godina
    - tko bez navođenja imena objavi, prikaže ili prenese tuđe djelo – novčana kazna ili kazna zatvora do 1 godine
    - tko unese tuđe djelo u svoje – novčana kazna ili kazna zatvora do 1 godine
    - tko mijenja ili skraćuje tuđe djelo – novčana kazna ili kazna zatvora do 6 mjeseci

PATENTNOPRAVNA ZAŠTITA

- pravo koje štiti nositelja patenta u pogledu gospodarskog iskorištavanje izuma
- patentabilni izum – priznaje se izum koji je nov, ima invetivnu razinu i koji se može industrijski primijeniti
    - industrijska – ako se može primjenjivati u bilo kojoj grani industrije, uključivo poljoprivredu
    - invetivnost – ako za stručnu osobu izum ne proizlazi iz stanja tehnike
- za računalne programe se priznaju samo ukoliko njegova primjena ima tehnički učinak

ZAŠTITA ZAKONOM O ŽIGU

- grafički prikaz i koji je prikladan za razlikovanje proizvoda i usluga jednog sudionika u gospodarskom prometu od drugog

ZAŠTITA POSLOVNOM TAJNOM

- zakon o zaštiti tajnosti podataka (19.12.1996.)
- podatak koji je zakonom ili drugim aktom na temelju zakona određen tajnom
- vrste:
    - državna
    - vojna
    - službena
    - poslovna

    - profesionalna tajna
- na dokumentima na vidljivom mjestu – vrsta tajne i stupanj tajnosti
- elektroničke baze podataka označene tajnom moraju biti osigurane lozinkom od neovlaštenog pristup
- poslovnu tajnu čine podaci koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te drugi podaci zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese

PRAVNA ZAŠTITA BAZA PODATAKA:
- po autorskom pravu – arhitektura
- EZ direktive – spriječiti nepošteno saznavanje podataka iz baze podataka

case_study: RAČUNALNI KRIMINALITET
1. Kako se zove zakon u kojem su uređena pravila ponašanja na Internetu? [*Kazneni zakon]*
2. Koje kazneno djelo se najstrože kažnjava u računalnom kriminalitetu? *[Dječja pornografija, do 8 godina]*