TEMATSKA CJELINA

SIGURNOST INFORMACIJSKIH SUSTAVA

ZLOPORABA INFORMACIJSKIH TEHNOLOGIJA

Etički izazovi primjene informacijskih tehnologija

Ciljevi nastavne cjeline

- Definicija pojma sigurnosti informacijskog sustava
  - Istaknuti rizik kao mjeru određivanja razine sigurnosti
- Opisati mjere zaštite svih komponenti IS – a → prvenstveno:
  - Zaštitu podataka
  - Programske mjere zaštite
- Upoznati studente s pojmovima:
  - Backup podataka
  - Schedule time
  - Kriptiranje
  - Dekripcija
  - Privatni i javni ključevi

Ciljevi nastavne cjeline

- Istaknuti razliku između računalnih virusa, trojanaca i crviju
- Objasniti pojmove spam, spyware i pishing
- Nabrojati i navesti osobitosti rješenja za “borbu” protiv svih vrsta malicioznih programa
- Identificirati situacije u kojima se javljaju znatni etički izazovi uslijed primjene informacijskih tehnologija

3

Pojam sigurnosti

- Kod sigurnosti informacijskih sustava možemo govoriti o:
  - Sigurnosti podataka
  - Sigurnosti pristupa podacima
  - Sigurnosti informacijskih tehnologija kao podrške tim sustavima
  - Sigurnosti komunikacija kao izdvojenog dijela IT – a

4

Pojam sigurnosti

Sigurnost informacijskog sustava je niz mjera i postupaka koji se poduzimaju kako bi se osiguralo normalno funkcioniranje informacijskog sustava bez narušavanja njegovog integriteta.

- Kao što smo već naglasili da je nužno planirati informacijske sustave, također je neophodno predvidjeti mjere sigurnosti
- Implementirane mjere sigurnosti cjenovno ne smiju premašiti vrijednost štete koja bi nastala gubitkom cjelokupnog ili većeg dijela sadržaja

5

Rizik i sigurnost

- Da bismo mogli planirati nivo sigurnosti treba biti u stanju procijeniti razinu rizika
- Cilj implementiranog sutava sigurnosti je optimiziranje rada informacijskog sutava s obzirom na rizik kojem je izložen

Rizik izražava vjerojatnost gubitka, oštećenja ili povrede. Drugim riječima rizik je stupanj opasnosti da poduzete akcije mogu završiti s negativnim ishodom – posljedicama.

6

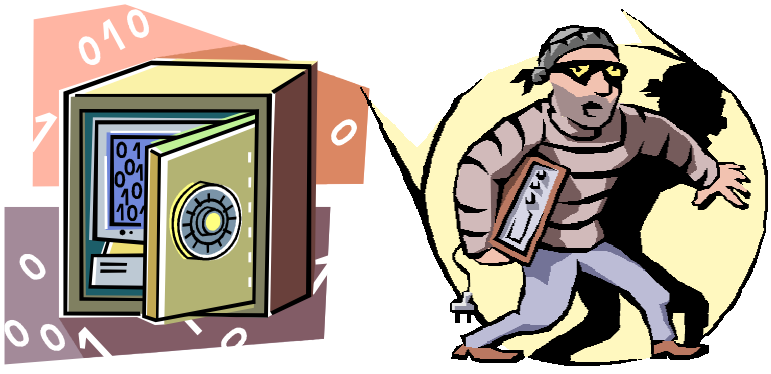
Rizik i sigurnost

- Rizik se procjenjuje s obzirom na:
  - Značaj podataka i sadržaja koji se pohranjuju ili distribuiraju
  - Procijenu izvora i oblika prijetnji tim sadržajima
- Što podaci imaju veći značaj to će štete nastale od njihovog gubitka, oštećenja ili neovlaštenog pristupa biti veće → veći rizik
- Što su prijetnje tim sadržajima veće, kao i broj tih prijetnji rizik će opet rasti

7

Rizik i sigurnost

- Veći rizik zahtjeva i veći stupanj sigurnosti



8

Rizik i sigurnost

- Kod procjene značaja podataka i sadržaja mjerodavno je:
  - Način na koji je država zakonskim aktima zaštitila takve sadržaje
  - Interes upravljačke strukture za promatranim sadržajem
  - Originalnost i novost na lokalnom i globalnom nivou
  - Važnost tih sadržaja za normalno funkcioniranje organizacije

9

Rizik i sigurnost

- Izvori prijetnji informacijskom sadržaju:
  - Prirodni čimbenici (potresi, poplave, požari, ekstremi u temperaturnim rasponima itd.)
    - Na njih se djeluje vrlo teško, ali koliko je moguće mjere se svode na građevinske, tehničke i organizacijske prevencijske mjere
  - Namjera čovjeka
    - Službenik banke prebacuje novac komitenata na svoj račun
    - Skladištar evidentira krive podatke o škart materijalu
      - Možemo ih spriječiti jedino podizanjem zadovoljstva zaposlenika (materijalno) i dobrom radnom klimom

10

Rizik i sigurnost

- Ljudski faktor (nenamjera čovjeka)
  - Blagajnik slučajno zbog premorenosti krivo evidentira neku isplatu
- Tehnička pogreška
  - Najlakše je predvidljiva
  - Ovisi o procijeni vremenske funkcionalnosti korištenih IT – a
  - S njom se lako upravlja

11

Rizik i sigurnost

- Oblici prijetnje informacijskom sadržaju:
  - Neautorizirano služenje informacijskim sadržajem
    - Uposlenik namjerno prenosi povjerljive podatke izvan organizacije u svrhu ostvarivanje materijalne dobiti ili drugih osobnih interesa
    - Nenamjerno “curenje” podataka
      - Nepažnja
      - Nemar
      - Neznanje
    - Krađa podataka iz informacijskog sustava
      - Upadom u sustav
      - Presretanjem poruka kroz komunikacjske kanale

12

Rizik i sigurnost

- Neidentificirana promjena informacijskog sadržaja
  - Ulaskom u sustav mijenjaju se izvorni podaci
  - Ti promijenjeni podaci postaju temelj za donošenje poslovnih odluka
  - Ovakvu promijenu podatak je teško identificirati
- Uništenje informacijskog sadržaja
  - Sadržaj je postaje u potpunosti neupotrebljiv
    - "Ako meni ne koristi neće ni tebi!"
  - Lako se uočava → podataka više nema, tj. nisu upotrebljivi

Rizik i sigurnost

- Sadržaj se može uništiti:
  - Fizičkim uništenjem računalnih vitalnih dijelova
  - Suptilnom diverzijom koja izgleda kao tehnički kvar ili programska pogreška
  - Zarazom računalnog sustava virusom → destruktivno dijeluju na sadržaje i programsku podršku
- Prisjetimo se od čega se sastoji naš Informacijski sustav:
  a) Hardware (sklopovske podrške)
  b) Software (programske podrške)
  c) Lifeware (ljudskih resursa)

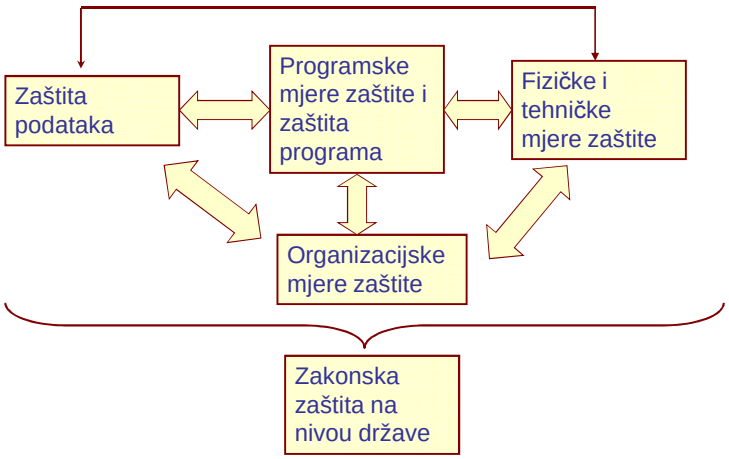
Mjere zaštite

d) Orgware (organizacije)
e) Netware (mrežene komunikacije)
f) Dataware (podataka koji opisuju stvarni svijet) → u posljednje vrijeme ističe se kao zasebna komponenta

- Na svakom od nabrojenih dijelova se može primjeniti odgovarajući stupanj sigurnosne zaštite
- Sve mjere zaštite se trebaju organizirati na način da se međusobno nadopunjuju
- Na sljedećoj slici dat je konceptualni prikaz mjera zaštite
  - Detaljnije ćemo objasniti samo mjere zaštite podataka i programske mjere zaštite

15

Mjere zaštite



Slika 1 - mjere zaštite IS - a

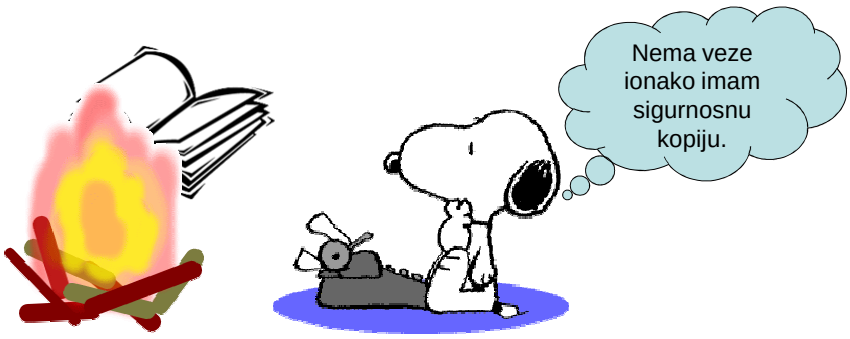
16

Zaštita podataka

- Današnje metode zaštite podataka podrazumijevaju izradu sigurnosnih kopija
  - Sadržaji se kopiraju na više lokacija
    - RAID polje
    - Backup server
    - Prijenosni mediji velikog kapaciteta
  - Princip je jednostavan → podaci se pohranjuju na drugu lokaciju i u slučaju havarije se ponovno vraćaju u sustav (sustav postaje ponovno funkcionalan)

17

Zaštita podataka



Izrada sigurnosnih kopija podataka naziva se backup podataka.

18

Zaštita podataka

Vraćanje podataka iz sigurnosnih kopija naziva se RESTORE podataka

19

Zaštita podataka

- Bilo bi nerazumno uvijek nanovo izrađivati backup svih podataka
- Dovoljno je sigurnosnu kopiju “nadopuniti” datotekama koje su nove ili izmjenjene
- Najpoznatije su tri metode izrade sigurnosnih kopija:
  - Potpuni backup
  - Diferencijalni backup
  - Inkrementni backup

20

Zaštita podataka

- Full Backup – pohranjuju se sve datoteke bez obzira jesu li ili ne označene za pohranu
  - Ovakav način izrade sigurnosne kopije ćete primjenjivati kada prvi put izrađujete sigurnosnu kopiju
- Differential Backup – pohranjuje nove datoteke i one koje su označene kao nearhivirane (svojstvo Archive nije uključeno)
- Incremental Backup – pohranjuje samo izmijenjene datoteke s uključenim atributom Archive

21

Zaštita podataka

- U praksi se diferencijalni i inkrementni backup postavljaju na automatsko pokretanje u točno zadanim vremenima (schedule time)

11:20 je – sad će započeti inkrementni backup podataka.

22

Programske mjere zaštite

- U najčešće programske mjere zaštite spadaju:
  - Zaštita na razini operacijskog sustava
  - Zaštita na razini korisničke programske podrške
  - Kriptiranje podataka u komunikaciji
  - Antivirus alati
  - Antispyware alati
  - Zaštitni zid (Firewall)

23

Programske mjere zaštite

- Zaštita na razini operacijskog sustava
  - Višekorisnički rad
  - Administratori i korisnici (User)
  - Administratori svakom korisniku određuju:
    - User name – korisničko ime
    - Password – lozinku
  - Za svakog korisnika ili grupu korisnika mogu se odrediti različite ovlasti
  - Svako računalo može imati više administratora i korisnika

24

Programske mjere zaštite

- Veću razinu sigurnosti administrator postiže:
  - Pravilnim definiranjem ovlasti korisnika
  - Pravilnom raspodjelom korisnika u grupe
  - Konfiguracijom User Security Policy
  - Konfiguracijom Group Security Policy
- Svi suvremeni operacijski sustavi omogućuju ovakvu razinu zaštite → Unix, Linux, MacOS, Windows...

25

Programske mjere zaštite

- Zaštita na razini korisničkih programa
  - Nakon odobrenog pristupa radnoj okolini (pravilan User name i Password) pokreće se korisnički program kojim se obavlja određena aktivnost u informacijskom sustavu
  - Zaštita korisničkih programa zaporkom:
    - Prva razina → samo čitanje podataka iz baze
    - Druga razina → promijena podataka u bazi i unos novih
    - Treća razina → podaci se mogu brisati
      - Postoji još jedna mjera sigurnosti za ovaj slučaj

26

Programske mjere zaštite

- Obrisani podaci iz baze ne uklanjaju se direktno, fizički s diska, već u posebno definirane mape kojima pristup imaju administratori sustava
- Administrator sustava će periodički, nakon ponovne provjere podatke fizički izbrisati s diska → DBMS (Data Base Management System)
- DBMS – Upravitelj bazom podataka

27

Programske mjere zaštite

- Kriptiranje kao mjera zaštite u mrežnoj komunikaciji:
  - Poslovni informacijski sustavi trebaju pratiti organizaciju poslovnog procesa
  - Danas nailazimo na primjere distribuirane organizacije → dijelovi poslovnog sustava su prostorno dislocirani:
    - Centrala banke i poslovnice
    - Upravna zgrada u jednom gradu proizvodni pogoni u drugom
    - Itd.

28

Programske mjere zaštite

- Potreba za distribuiranim informacijskim sustavom
  - Osnovni zahtjev je razmjena informacija → umrežavanje računala
- Kako se umrežavanje vrši preko globalnog komunikacijskog sustava (Interneta), potrebno je dodatno zaštiti sadržaj koji se prenosi
- Dva osnovna zahtjeva za zaštitu sadržaja pri prijenosu

29

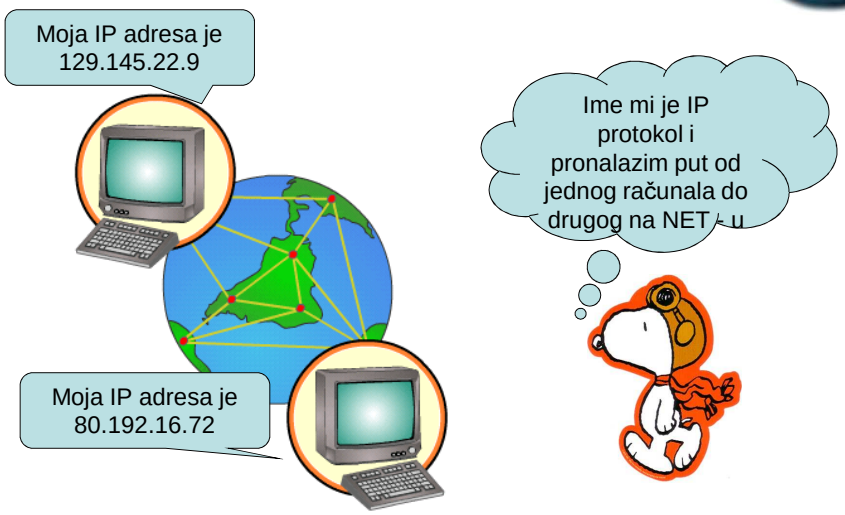
Programske mjere zaštite

1. Osiguravanje jednoznačnosti prijenosa
2. Onemogućavanje neautoriziranog korištenja ili promijene sadržaja u prijenosu

- Osiguravanje jednoznačnosti prijenosa na tehničkoj razini rješava se komunikacijskim protokolima:
  - TCP (Transmission Control Protocol) – vodi brigu da se podaci prilikom prijenosa ne izgube
  - IP (Internet Protocol) – pronalazi put od jednog računala do drugog

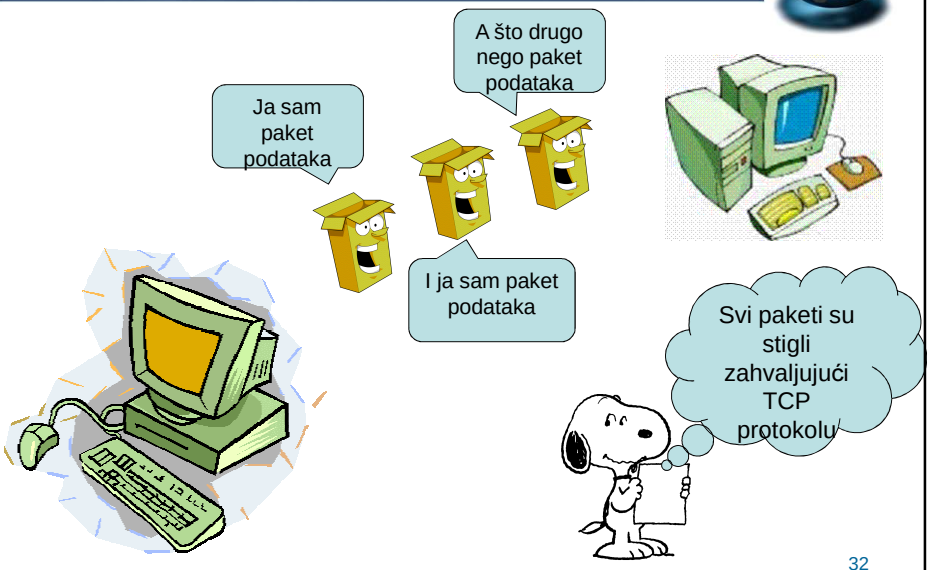
30

Programske mjere zaštite



31

Programske mjere zaštite



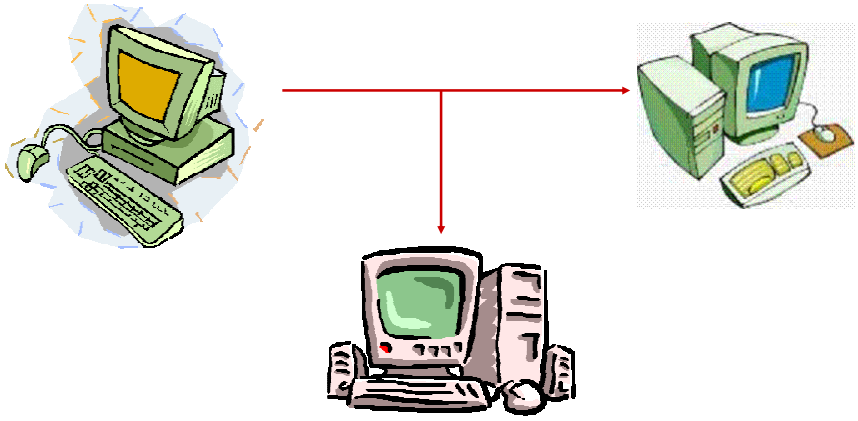
32

Programske mjere zaštite

- Što se u komunikacijskom kanalu može dogoditi?
  - Netko može prisluškivati kanal
  - Netko može prekinuti komunikaciju
  - Netko može presresti pakete i promijeniti im sadržaj
  - Netko može generirati nepostojeći sadržaj
- Na sljedećim slajdovima su prikazane spomenute situacije

33

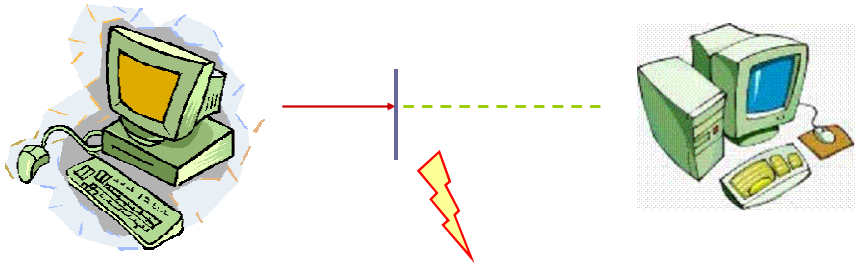
Programske mjere zaštite



Računalo koje prisluškuje komunikacijski kanal

34

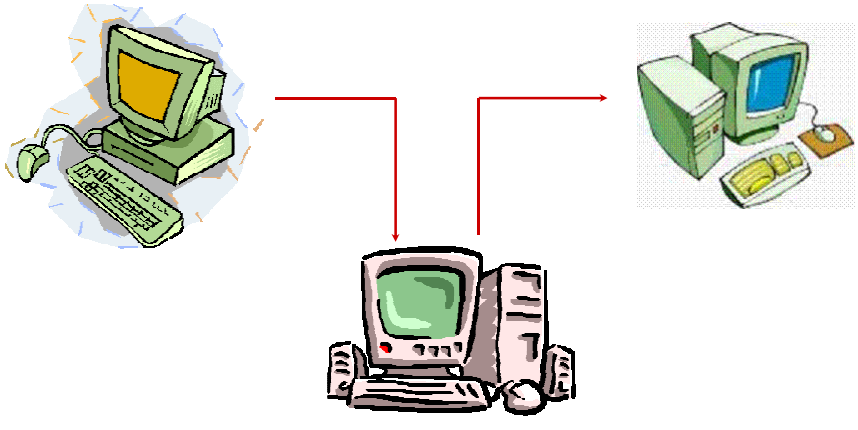
Programske mjere zaštite



Prekid u komunikaciji

35

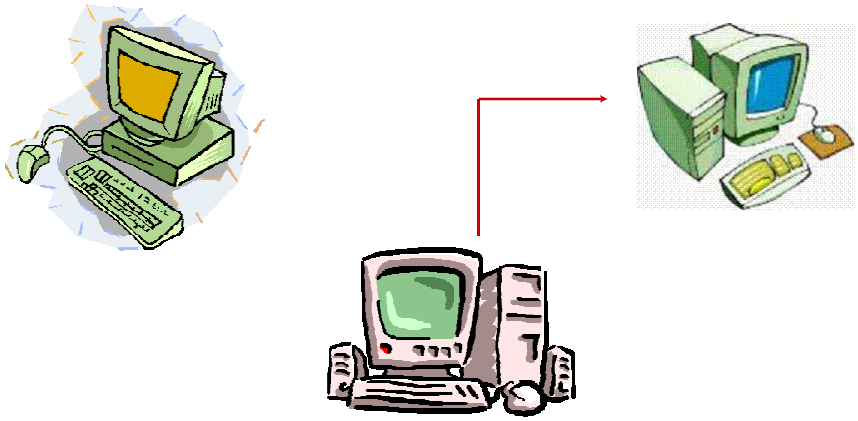
Programske mjere zaštite



Računalo koje mijenja originalni sadržaj

36

Programske mjere zaštite



Računalo koje generira nepostojeći sadržaj

37

Programske mjere zaštite

- Prema očekivanom obliku prijetnje u komunikacijskom kanalu postavljaju se mjere zaštite
- Najčešće mjere zaštite od neautorizirane upotrebe su mjere kriptozaštite
- Uzmimo za primjer riječ:

KRIPTO → Izvorni tekst

38

Programske mjere zaštite

- Probajmo je šifrirati po principu:

  Slovo+1

- Pa naša riječ postaje:

  Kodirani tekst

  LSJRUP

- Ovo je jednostavan primjer šifriranja i jednostavno ga je probiti
- Onaj tko primi poruku dekodira je po principu:

  Slovo - 1

39

Programske mjere zaštite

Kriptiranje (šifriranje – encription) → je postupak kojim se razumljiv tekst po određenom principu pretvara običnom korisniku u nerazumljiv tekst

Dekripcija (dešifriranje – decription) → postupak pretvaranja kodiranog teksta u razumljiv tekst

- Danas se koriste metode koje su poznate pod nazivom asimetrična enkripcija
- Prisjetite se našeg primjera šifriranja Slovo + 1

40

Programske mjere zaštite

- U tom slučaju koristi se jedan te isti ključ za kodiranje i dekodiranje poruka → simetrična enkripcija
- U asimetričnoj enkripciji postoje dva ključa:
  - Javni ključ za kodiranje
  - Privatni ključ za dekodiranje
- Princip zaštite se zasniva na izmjeni javnih ključeva

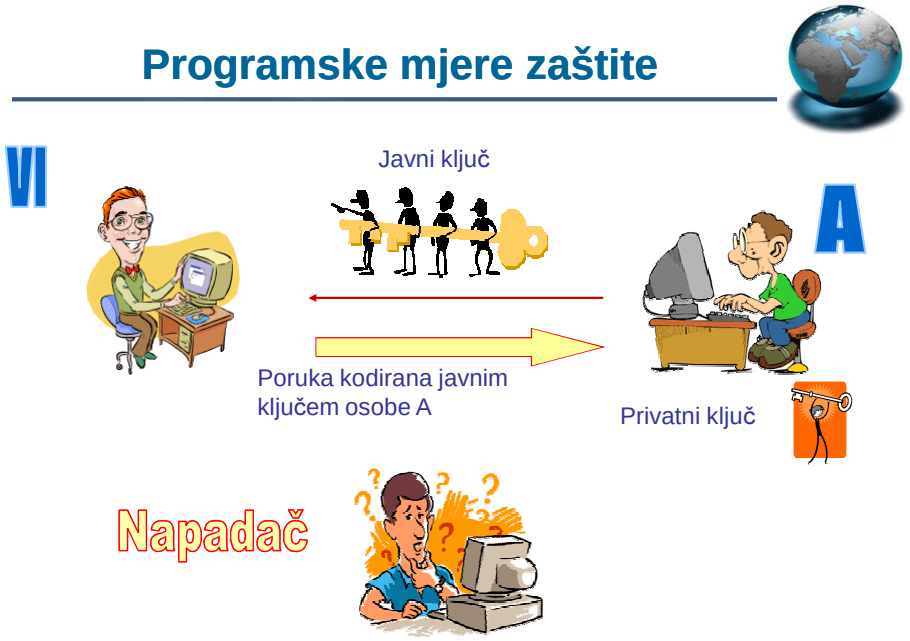
41

Programske mjere zaštite

- Primjerice:
  - Šaljete word datoteku važnog sadržaja osobi A
  - Osobu A pitate njezin javni ključ (npr. e – mailom se pošalje)
  - Word datoteku kodirate tim ključem i pošaljete je osobi A → poruka se samo može dešifirirati privatnim ključem osobe A (dobro ga čuva)
  - Osoba A prima dokument i dešifrira ga svojim privatnim ključem

42

Programske mjere zaštite



43

Programske mjere zaštite

- Program koji se zasniva na primjeni javnih i privatnih ključeva je PGP (Pretty Good Privacy) www.pgpi.com
- Opisani sustav zaštite predstavlja osnovu e – businessa
- Programske mjere zaštite trebaju pružiti sigurnost i od virusa, crviju, trojanaca, spywarea i drugih tzv. malicioznih programa

44

Programske mjere zaštite

- Virusi su destruktivni računalni programi koji imaju cilj uništenje podataka ili funkcionalnosti programa na zaraženom računalu
  - u nekim slučajevima samo troše resurse računala bez drugih vidljivih šteta
- Svaki virus ima tri osnovne komponente:
  - Infekcija – programski dio koji omogućava širenje virusa
  - Nosiva komponenta (payload) – predstavlja glavnu aktivnost virusa (brisanje podataka ili onemogućenje programa)

45

Programske mjere zaštite

  - Funkcija okidanja (trigger) – definira vrijeme ili događaj koji će pokrenuti izvršavanje nosive komponente virusa
- Osnova je onesposobiti kopiranje virusa na računalo
- Virus se neće pokrenuti sve dok nije zadovoljen uvjet iz treće komponente → funkcije okidanja virusa
- Virusi se najčešće aktiviraju pokretanjem zaražene datoteke

46

Programske mjere zaštite

- Najveću štetu prouzrokuju tzv. boot virusi
  - Ti virusi inficiraju boot sektor računala, te samim tim onemogućuju njegovo pokretanje (onemogućavaju podizanje operacijskog sustava računala)
- Web odredište na kojem možete saznati nešto više o virusima je www.wildlist.org
- Postoje dvije vrste zaštite od djelovanja virusa:
  - Preventivne mjere
  - Sanacijske mjere

47

Programske mjere zaštite

- Preventivne mjere zaštite:
  - Organizacijske
  - Nadzorne
  - Sanacijske
- Organizacijske mjere zaštite →onemogućavanje instaliranja neautoriziranih programa, te kopiranja sadržaja s rizičnih lokacija – medija
  - Potrebno je osigurati "slobodno" računalo koje nema fizičke veze s ostalim računalima i ne koristi se u svakodnevnom poslu → na njemu se testiraju sumnjivi programi i sadržaji

48

Programske mjere zaštite

- Nadzorne mjere → Korištenje antivirusnih alata
  - Potrebno je uključiti funkciju On access scanning
  - Potrebno je uključiti automatsku provjeru i download definicija virusa (ažuriranje baze virusa)
  - Antivirusom skenirati sve sumnjive datoteke prije njihovog kopiranja ili otvaranja
  - Antivirusna zaštita e – mail boxa
- Nedostatak → antivirusni alat nije ažuriran ili nije izbačena definicija za neki virus (prepoznavanje po potpisu)

49

Programske mjere zaštite

- Svaki virus sastoji se od dva dijela:
  - Tijela virusa
  - Slučajnog ključa za enkripciju – s njim je kodirano i tijelo

50

Programske mjere zaštite

- U okviru zaštite od virusa u nekom IS – u svako računalo vrši update antivirusnog alata sa odgovarajućeg servera (schedule time)
- Mjere sanacije:
- Računalo je zaraženo → najčešće usporen rad; uočen nedostatak nekog sadržaja ili smanjena funkcionalnost nekih programa
  - Isključivanje zaraženih računala iz mreže
  - Prikupljanje sumnjivih medija
  - Uklanjanje virusa → ako je moguće antivirusnim alatom ili ručno (ekspert iz područja zaštite IS –a)
  - Ponovna instalacija cijelog sustava na zaraženim računalima (krajnja, ali najsigurnija mjera) → lako ako imamo sigurnosnu kopiju sustava

51

Programske mjere zaštite

- Većina današnjih antivirusnih alata nam daje zaštitu i od:
  - Trojanaca
  - Crviju
- **Crvi** predstavljaju najveću prijetnju u današnje vrijeme
  - Crv je program koji se širi preko mreže
  - Koristi slabe točke umreženog računala
  - Kada se pokrene potpuno automatski se širi na druga računala s istom slabom točkom → šalje pakete podataka

52

Programske mjere zaštite

- Crvi se ne spajaju na druge datoteke i programe
  - Nemaju svojstva virusa
- Osim klasičnih mrežnih primjeraka crviju postoje i e – mail crvi
- E – mail crvi se šire preko attachmenta mail poruka
- Ponekad ih uopće nije potrebno pokrenuti (sami se pokreću) → šalju se na mailove iz adresara zaraženog računala
- Crvi koji se šire mailom i posebno se označavaju od strane antivirusnih kompanija
  - VBS/OnTheFly@mm → mm = mass mailer

Programske mjere zaštite

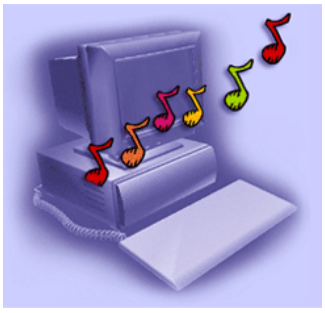
Zašto pokrećeš privitak koji ima datoteke s ekstenzijama **.exe .com .bat .vbs .pif .scr**

Programske mjere zaštite

- Danas postoji čitav niz hibridnih crviju:
  - Crvi koji u sebi nose i svojstva virusa
  - Crvi koji sa sobom nose trojanca
- **Trojanci –** maliciozni programi koji nemaju mogućnost samostalnog repliciranja
  - program koji izvršava drugu funkciju od one za koju je deklariran
  - Koriste ga hakeri za preuzimanje nadzora na računalima

55

Programske mjere zaštite



- Pokrenete neki program za “miksanje” muzike koji je u stvari trojanac
- Za vrijeme slušanja trojanac vam instalira stražnji ulaz preko kojeg haker može daljinski preuzeti nadzor nad vašim računalom

56

Programske mjere zaštite

RAT (Remote Access Tools) – alati za potpunu kontrolu računala s udaljene lokacije

Backdoor – trojanci koji omogućuju stvaranje nezaštićenih ulaza kako bi im se pristupilo RAT alatima i to pod administratorskim ovlastima

- Ponekad trojanci mogu poslužiti i za krađu korisničkih lozinki
- Primjerice lažni klijent za upisivanje korisničkih podataka pri prijavi na pojedini servis → primjer Login trojanac

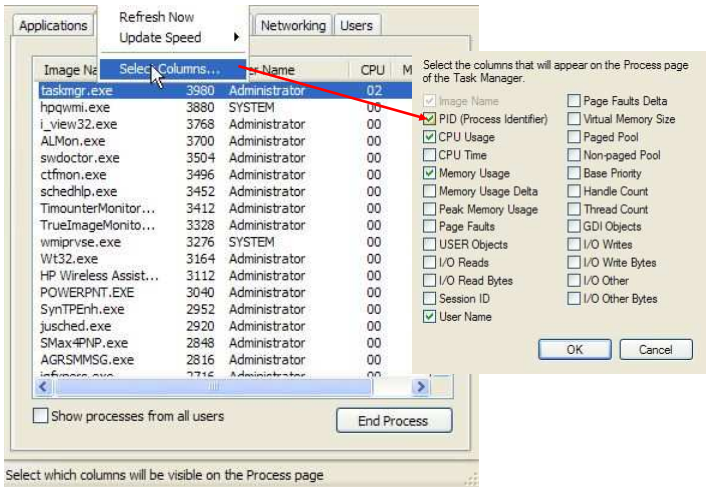
57

Programske mjere zaštite

- Login trojanac potpuno simulira izgled ekrana za korisničku prijavu na računalo
- Želite li pod Windowsima XP provjeriti koji su programi uspostavili vezu i osluškuju veze trebate pokrenuti naredbu Netstat
  1. CTRL + ALT +DEL (pokrenite Windows Task Menager)
  2. Prebacite se na karticu **Processes**
  3. Odaberite **View → Select columns…**
  4. Uključite **PID (Process Identifier)**

58

Programske mjere zaštite



Programske mjere zaštite

- Preko **start** → **Run**… pokrenite komandnu liniju
- U polje **Run**… upišite **cmd**
- U otvorenoj komandnoj liniji upišite

  netstat –ao
- Dobit ćete popis koje ulaze osluškuju određeni procesi → prikazano slikom na sljedećem slajdu

Programske mjere zaštite

```
C:\>netstat -ao

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    your-a9279112e3:epmap  your-a9279112e3:0      LISTENING       1304
  TCP    your-a9279112e3:microsoft-ds  your-a9279112e3:0      LISTENING       4
  TCP    your-a9279112e3:8888   your-a9279112e3:0      LISTENING       688
  TCP    your-a9279112e3:netbios-ssn  your-a9279112e3:0      LISTENING       4
  TCP    your-a9279112e3:1026   your-a9279112e3:0      LISTENING       2360
  UDP    your-a9279112e3:microsoft-ds  *:*                                   4
  UDP    your-a9279112e3:isakmp  *:*                                    1072
  UDP    your-a9279112e3:1025   *:*                                    1816
  UDP    your-a9279112e3:1042   *:*                                    1816
  UDP    your-a9279112e3:1053   *:*                                    1816
  UDP    your-a9279112e3:4500   *:*                                    1072
  UDP    your-a9279112e3:ntp    *:*                                    1344
  UDP    your-a9279112e3:netbios-ns  *:*                                       4
  UDP    your-a9279112e3:netbios-dgm  *:*                                      4
  UDP    your-a9279112e3:1900   *:*                                    1892
  UDP    your-a9279112e3:ntp    *:*                                    1344
  UDP    your-a9279112e3:1037   *:*                                    2216
  UDP    your-a9279112e3:1900   *:*                                    1892

C:\>
```

61

Programske mjere zaštite

- Popis prikazuje sve procese koji su kreirali vezu na Internet
- Prvi stupac pokazuje protokole (TCP i UDP)
- Drugi stupac prikazuje ime ili IP adresu vašeg računala i potom slijedi dvotočka sa brojem ulaza vašeg računala kojeg proces koristi
- Treći stupac prikazuje ime ili IP adresu računala s kojim proces komunicira – slijedi dvotočka i broj ulaza

62

Programske mjere zaštite

- Četvrti stupac pokazuje status veze
- Posljednji stupac pokazuje ID procesa → usporedbom tog stupca s vrijednostima pod stupcem PID u Windows Task Manageru možete pronaći koji su programi pokrenuli navedene procese

Trojanci se najčešće distribuiraju piratskim programima i preko P2P (Peer To Peer) alata (KaZaA, e – Mule, LimeWire itd.).

63

Programske mjere zaštite

- Od trojanaca se štitimo upotrebom **vatrozoida (firewall)**
- Trojanac pokušava otvoriti ulaz, a vaš firewall će vas pitati treba li mu to dozvoliti → ako ste dovoljno pažljivi možete otkriti trojanca prije nego što postane opasan
- Na web adresi

  http://www.download.com/3000-2092-10039884.html

Možete skinuti besplatnu verziju vatrozoida **ZoneAlarm**

64

Programske mjere zaštite

Firewall osigurava:

- **da neautorizirani korisnici ne mogu pristupiti u lokalnu mrežu**
- **da se s okolinom razmjenjuju samo protokolirani sadržaji**

65

Programske mjere zaštite

- Nadzor nad razmjenom poruka:
  - Autorizacijski server
  - Odabirom i kontrolom ulaznog sadržaja
- Autorizacijski server – provjerava ovlasti korisnika koji preko Interneta pokušavaju pristupiti lokalnoj mreži
  - Provjera u više razina
  - Višerazinska ovlaštenja korisnika – posebno kod otvorenih IS – a
- Ograničena propusnost kontrole ulaznog sadržaja – u zaglavlju pristupne poruke ugrađuju se identifikacijski elementi koji se provjeravaju
  - Potom se provjeri autorizacija pristupa mreži

66

Programske mjere zaštite

- Adware programi
  - Omogućavaju pop – up oglašivačima da se pojavljuju za vrijeme vašeg surfanja Netom
  - Najčešće se instaliraju zajedno s nekim programima za koje mislite da su pod Open Source licencom
- Spyware programi
  - Uključuju nekoliko komponenti
    - Keylogger – program koji snima vaše tipkanje po računalnoj tipkovnici
    - Password capture – program koji bilježi vaše lozinke
    - Spamware – program koji koristi vaše računalo kao lansirnu rampu za spamanje
  - Često se koriste i za snimanje vaših surferskih navika webom
  - Instaliraju se primjenom trikova → navode se kao besplatni programi koji će vam donijeti neku korist (npr. upravo "osloboditi" vaše računalo od spyware programa)
- Adware su manje opasni od Spyware programa
- Jedni i drugi znatno troše računalne resurse
- Besplatni programi koji vam mogu pružiti dobar nivo zaštite od Adware i Spyware programa su Ad – Aware se i SpyBot Search and Destroy
  - http://www.lavasoftusa.com/software/adaware/
  - http://www.safer-networking.org/en/download/index.html

Programske mjere zaštite

- Spam
  - Neželjene e – mail poruke u cilju oglašavanja proizvoda ili usluga
  - Ne radi se samo o "gnjavatorskim" porukama, već i o ozbiljnoj prijetnji tvrtkama u vidu izgubljenog vremena, a samim tim i novca
    - U SAD – u se procjenjuje da gubici uzrokovani Spam porukama premašuju 20 milijardi USD
      - Ti gubici proizlaze iz spriječavanja mail sustava
      - Potrebe za povećanjem prostora za pohranu poruka
      - Dodatna korisnička podrška
      - Antispam rješenja
  - Danas se antispam zaštita uglavnom pruža na nivou ISP – ova
    - Inteligentni antispam vatrozoidi

Programske mjere zaštite

- Phishing
  - Prikupljanje osjetljivih osobnih informacija kao što su brojevi računa, lozinke, brojevi kreditnih kartica i sl. najčešće preko “maskiranih” e - mailova koji na prvi pogled izgledaju kao službeni mailovi renomiranih tvrtki
  - Primjer
    - “Napad” na eBay → korisnici bi dobili mailove “kao” da se radi o službenim mailovima eBay službe za korisnike
    - Ti mailovi bi ih obavještavali da se aukcija za predmet za koju su bili zainteresirani ponavlja zbog tehničkih razloga
    - U mailu bi se nalazio link koji bi ih vodio na stranice koje su predstavljane kao zamjenske stranice eBaya dok se ne riješe “tehnički” problemi na stalnim stranicama
    - Veliki broj korisnika bi “nasjeo” i obavljao kupnju preko tih stranica → pored osobnih podataka unosili su i brojeve kreditnih kartica
  - Gotovo svi web preglednici novije generacije imaju u sebi ugrađene pishing filtere → OPREZ - ipak ne pružaju potpunu zaštitu

69

Programske mjere zaštite

Antivirus, Antispam, Antispyweare, Phishing filteri, Firewall – sad sam siguran → bar tako mislim.

70

Etički izazovi primjene IT - a

- Pojednostavljeno etika podrazumijeva ispravno ponašanje
- Neetično ne mora nužno povlačiti ilegalno, tj. nezakonito ponašanje
- Sve ozbiljnije tvrtke razvijaju vlastiti etički kodeks
- Primjena informacijskih tehnologija postavila je pred menadžment tvrtki nove etičke izazove:
  - Problem privatnosti
  - Problem ispravnosti podataka
  - Autorska prava
  - Problemi pristupa podacima

71

Četiri kategorije etičkih izazova

- ***Problem privatnosti***
  - Uključuje prikupljanje, pohranu i distribuciju informacija o pojedincima
- ***Problem ispravnosti podataka***
  - Uključuje autentičnost, pouzdanost i točnost prikupljenih i procesiranih podataka
- ***Autorska prava***
  - Odnosi se na vlasnička prava i vrijednost informacija
- ***Problem pristupa podacima***
  - Određuje se tko ima pravo pristupa podacima i informacijama, u kojem obimu, te da li se pristup naplaćuje ili ne

72

Zaštita privatnosti

- **Privatnost**
  - Definira se kao pravo pojedinca da bude sam ili da bude slobodan od bezrazložnog ometanja
- **Informacijska privatnost**
  - Pravo da se odredi kada i do koje granice informacije o pojedincu mogu biti prikupljane i prenošene
- Dva osnovna pravila koja se nalaze kao zakonska osnova za zaštitu privatnosti u mnogim zemalja su:
  - *Pravo na privatnost nije apsolutno. Privatnost se treba uskladiti s potrebama društva*
  - *Pravo javnosti da zna iznad je prava osobne privatnosti*

73

Zaštita privatnosti

- **Elektronički nadzor (Electronic Surveillance)**
  - Praćenje aktivnosti pojedinaca online ili offline uz primjenu digitalnih računala
- **Osobne informacije u bazama podataka (Personal Information in Databases**)
  - Osobne informacije pojedinaca čuvaju se u mnogim bazama podataka:
    - Banke
    - Tvrtke koje se bave e – trgovinom
    - Osiguravajuća društva
    - Telekomunikacijske kompanije
    - Državne institucije
    - Škole i fakulteti
    - Itd.

74

Zaštita privatnosti

- **Postoji bezbroj pitanja koja vas sigurno zanimaju kada u nekoj od navedenih baza podataka ostavite osobne podatke:**
  - Gdje se nalaze podaci
  - Da li su podaci točni
  - Možete li promijeniti netočne podatke
  - Kako se podaci mijenjaju
  - Koliko dugo se podaci čuvaju
  - Tko sve ima pristup podacima
  - Jamči li se sigurnost podataka
  - Pod kojim uvjetima se podaci puštaju u opticaj
  - Kome se podaci mogu dati, prodati i pod kojim uvjetima

75

Zaštita privatnosti

- **Kodeks privatnosti i politika privatnosti**
  - Skup mjera koje tvrtka poduzima i jamči kako bi se odsigurala privatnost kupaca, klijenata, korisnika i zaposlenika
- **Internacionalni aspekti privatnosti**
  - Problemi privatnosti s kojim se suočavaju međunarodne organizacije i vlade država kada se informacijski kanal proteže kroz nekoliko država

76

KRAJ

TEMATSKE CJELINE