Zaštita informacionih sistema i bezbjednost

Ranjivost IS i računarski kriminal

Ključni termini u ovoj oblasti:

- **Kopija** - kopija podataka ili programa koji se čuvaju na obezbjeđenom mjestu
- **Dešifrovanje** - transformacija šifrovanog koda u čitljivu informaciju
- **Šifrovanje** - transformacija podatka u šifrovani kod prije slanja
- **Izloženost** - šteta, gubitak ili oštećenje koje može nastati ako nešto pođe kako netreba u IS
- **Tolerancija na greške** - sposobnost IS da nastavi da funkcioniše kada dođe do greške
- **Mjere za zaštitu IS** - procedure, uređaji ili softver koji pokušavaju da obezbjede da sistem funkcioniše kako treba.

Ranjivost IS i računarski kriminal

Ključni termini u ovoj oblasti:

- **Tačnost i pristupačnost podataka** - garancija tačnosti, potpunosti i pouzdanosti podataka uvijek u toku rada IS
- **Rizik** - vjerovatnoća da će se ostvariti pretnja napada na IS
- **Pretnje (ili opasnosti)** - razne opasnostoi kojima je IS izložen
- **Ranjivost** - pod uslovom da postoji opasnost, osjetljivost sistema na oštećenja koja pretnja izaziva.

Ranjivost IS i računarski kriminal

Sve veći problem i ograničavajući faktor razvoja i primjena računarskih sistema postaje bezbjednost informacionih sistema.

U poslovnim informacionim sistemima računarske konfiguracije su veoma različite, te se u jednom poslovnom sistemu mogu koristiti:

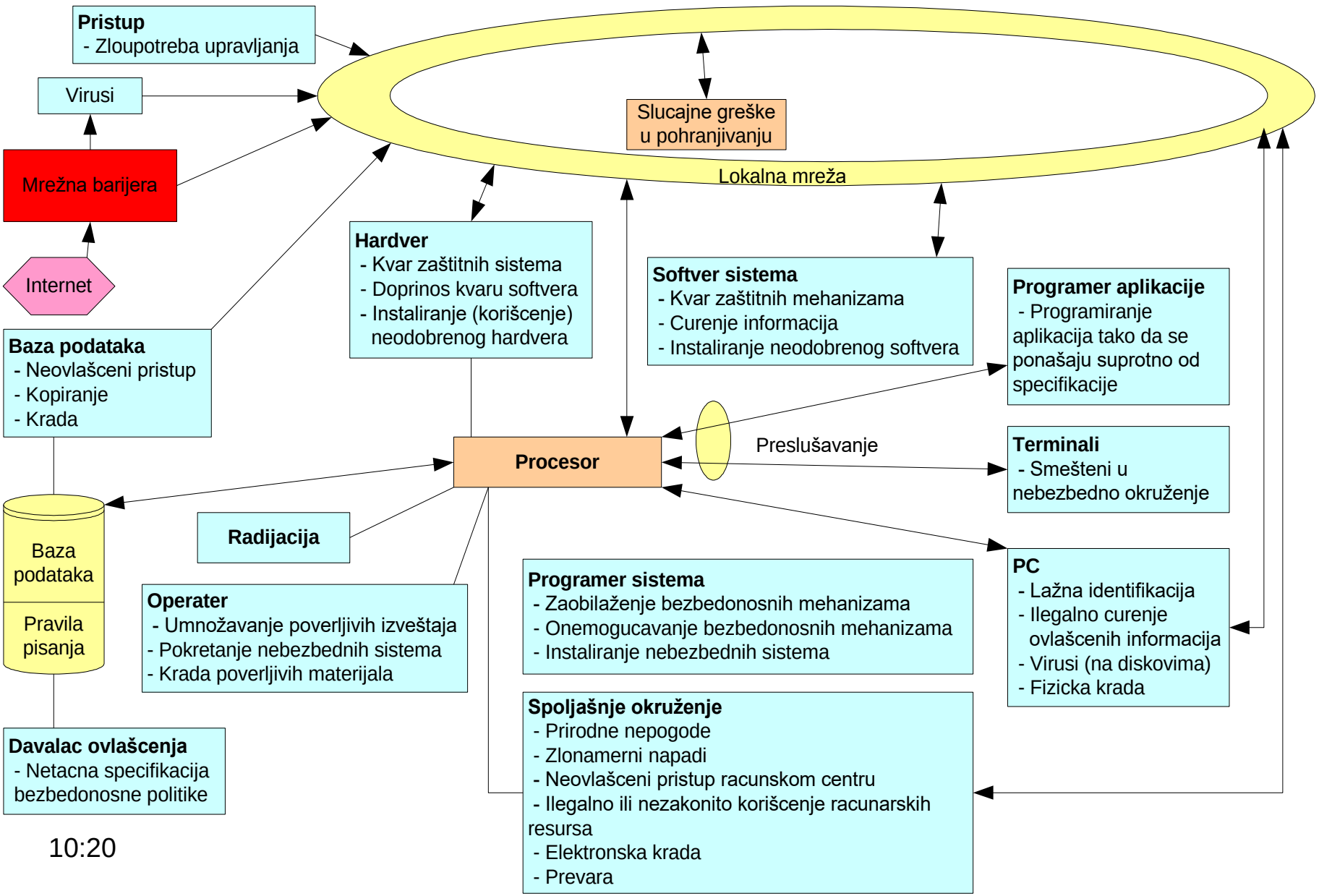
- Veliki računari za centralnu obradu
- Manji računari za decentralizovano prikupljanje i obradu podataka
- Personalni računari za automatizaciju kancelarijskog poslovanja

Ranjivost IS

Rizici koji prijete jednom računskom sistemu su:

- **Kompjuterski kriminal**
- **Sabotaža**
- **Špijunaža**
- **Nedovoljna čistoća u prostorijama u kojima su smešteni računari**
- **Slučajno ili namjerno kvarenje računarskih sistema**
- **Razne vremenske nepogode**

Pretnje bezbjednosti



10:20

Ranjivost IS

Ranjivost IS se povećava prelaskom na umrežene računarske sisteme.

Opasnosti se mogu podjeliti na dvije grupe:

- **Nenamjerne opasnosti**
- **Namjerne opasnosti**

Ranjivost IS nastavak

Nenamjerne opasnosti:

- ljudske greške
- opasnosti okruženja/sredine
- kvarovi računarskih sistema

Ranjivost IS

Namjerne opasnosti :

- krađa podataka
- neodgovarajuća upotreba podataka
- krađa opreme ili programa
- namjerna manipulacija u rukovanju, unosu, obradi, prenosu ili programiranju podataka
- štrajkovi radnika
- nemiri ili sabotaža
- zlonamjerno oštećenje računarskih resursa
- uništavanje virusima
- razne računarske zloupotrebe i kriminal

S obzirom na svoju prirodu kompjuterski kriminal vrlo brzo nakon svoje pojave dobija karakter međunarodnog kriminala što zahtjeva i organizovanje međunarodne saradnje na planu njegovog suzbijanja. U tom smislu od značaja je i donošenje međunarodnih akta među kojima su:

- **Preporuka Saveta Evrope o kriminalitetu vezanom za kompjutere (1989.)**
- **Rezolucija UN o kompjuterskom kriminalu (1990.)**
- **Rezolucija Međunarodnog udruzenja za krivično pravo (1992.)**
- **Preporuka Saveta Evrope vezana za informacionu tehnologiju (1995.)**

U dopunama ***Krivičnog zakona Srbije*** početkom 2003. godine uvedeno je niz potpuno novih inkriminacija posebno u oblasti zaštite

kompjuterskih programa,

Internet mreže i protokola podataka,

bezbjednosti podataka na Mreži,

hakerskih upada i

raznih zloupotreba...

Izvodi iz Krivičnog zakona Srbije

Kompjuterski kriminal i autorska prava

U ovu oblast spadaju slijedeća krivična djela:

- neovlašćeno korišćenje računara i računarske mreže (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- računarska sabotaža (minimalna kazna – **1 godina,** maksimalna – **8 godina zatvora**)
- pravljenje i unošenje virusa (minimalna kazna – **novčana**, maksimalna – **3 godine zatvora**)
- računarska prevara (minimalna kazna – **6 meseci**, maksimalna – **12 godina zatvora**)

- ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- neovlašćen pristup zaštićenom računaru ili računarskoj mreži (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)
- sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (minimalna kazna – **novčana**, maksimalna – **3 godine zatvora**)
- neovlašćeno korišćenje autorskog i drugo srodnog prava (minimalna kazna – **novčana**, maksimalna – **5 godina zatvora**)

Podvale u programiranju
Metode napada na računarske sisteme

- Virus
- Crv
- Trojanski konj
- Sečenje salame
- Superubijanje
- Tajna vrata
- Logička bomba
- Odbijanje usluga
- Njuškavac
- Podvala
- Drobilica lozinki
- Ratni pozivi
- Pomoćna vrata

10:20

Virusi – najčuvenija metoda napada

Virus je najčuvenija metoda napada, a dobila je ime po sposobnosti programa da se prikači "inficira" za druge računarske programe navodeći ih da i sami stvaraju viruse. Virus može da se širi kroz računarski sistem veoma brzo.

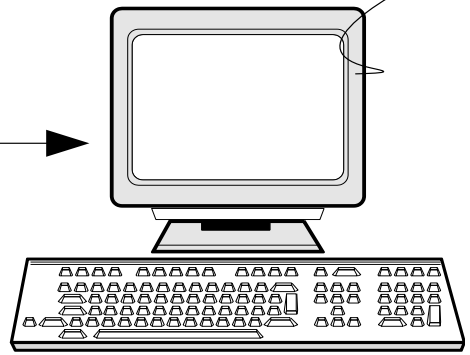
Kada se virus učvrsti u legitimni softverski program, program postaje inficiran, a da vlsnik programa nije svjestan infekcije. Kada se softver koristi, virus se širi oštećujući taj program, a možda i druge. Tako legitimni softver djeluje kao ***trojanski konj***.

Struktura virusa

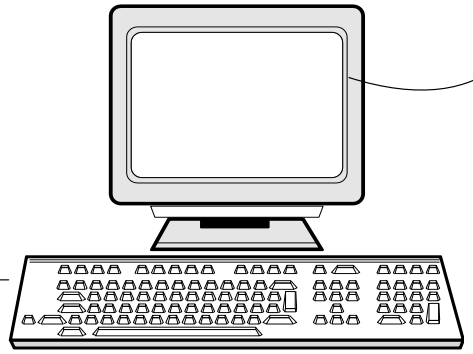
1. Obavezna komponenta
2. Nosiva komponenta(*payload*)
3. Funkcija za okidanje

Kako se širi računarski virus

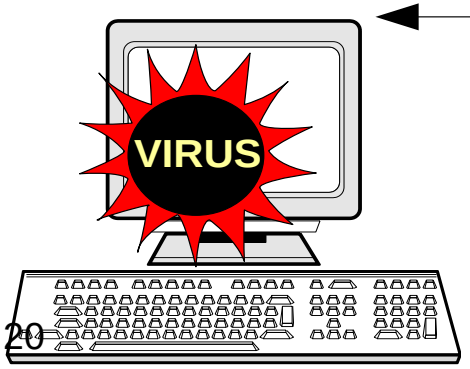
Baš kao što biološki virus remeti žive ćelije I tako prouzrokuje bolest, računarski virus - zlonamerno unesen - ulazi u unutrašnjost računara i remeti normalan rad mašine.



2) Virus se učvršćuje I putuje gde god putuje program-domaćin ili podatak, bilo na disketu, u lokalne mreže ili na elektronske oglasne table



1) Virus nastaje kada programer napiše program koji se smešta u program domaćina



3) Virus se aktivira nakon nekog vremenskog perioda ili određenim okolnostima, npr. Kao posledica nekih računarskih operacija koje izvrši korisnik. Zatim obavi ono što je programer virusa nameravao - npr. odštampa neku poruku ili izbriše neke podatke.

Virusi –

Danas postoji veliki broj raznih virusa. Ovaj broj se kreće do 70.000, a mjesečno se u prosjeku pojavi oko 100-150 novih virusa.

Pritom nijedan antivirusni program neće detektovati apsolutno sve viruse.

Metode napada na računarske sisteme

Crvi za razliku od virusa nemaju prvu obaveznu komponentu , tj. ne inficiraju druge programe, već se šire mrežom i to najčešće preko elektronske poste.

Trojanski konj se za razliku od crva i virusa ne širi sam već je za to potrebno da korisnik vrši kopiranje na drugi računar. Oni su često destruktivni i mogu ukrasti informacije s računara.

Virusna infekcija bankomata

Bankomati dvije američke banke, koji su bili temeljeni na operativnom sistemu Windows-a, pogođeni su crvom Nachi. To je prva do sada poznata virusna infekcija, koja je pogodila bankomate.

Virusna infekcija mobilnih telefona

Mobilni telefon je danas vrlo aktuelna meta.
Telefon se danas ne koristi samo za razgovaranje već i za:

- prenos podataka
- pristup internetu
- elektronska plaćanja
- identifikaciju ljudi

Zaštita IS

Odbrambene strategije. Kako se zaštititi?

- Sprečavanje i odvraćanje
- Otkrivanje
- Ograničavanje
- Obnova
- Ispravka

Zaštita IS

Tehničke mjere obuhvataju zaštitu hardvera, softvera, prenosa i obrade podataka.

Mogu se podjeliti na:

- Fizičke
- Mjere zaštite u računarskom sistemu

Fizička zaštita treba da obezbjedi zaštitu od

- Neispravnih instalacija
- Požara
- Poplava
- Zagađene okoline
- Štetnih zračenja
- Neurednog napajanja električnom energijom
- Nepovoljnih klimatskih i temperaturnih uslova
- Elementarnih nepogoda
- Fizička krađa opreme

Sredstva za kontrolu pristupa

Kontrola pristupa je onemogućavanje neovlašćenog pristupa korisnika djelu računarskog sistema ili čak čitavom sistemu.

Pristup računarskom sistemu se sastoji od 3 koraka:

- Fizičkog pristupa terminalu
- pristupa sistemu
- Pristupa konkretnim komandama, transakcijama, privilegijama, programima i podacima u okviru sistema

Biometrijska kontrolna sredstava

- Fotografija lica
- Otisci prstiju
- Geometrija šake
- Skeniranje dužice oka
- Šara krvnih sudova u mrežnjači oka
- Glas
- Potpis
- Dinamika udara na tastaturu
- Termografija lica

Pošto su slike obradili pomoću nekoliko filtera, većina algoritama izdvaja “digitalni potpis” metodom traženja završetaka ili razdvajanja linija otisaka, poznatom kao minutae tačke. Pri tome se pohranjuju samo relativne koordinate minutae tačaka. Kako se iz otiska izdvaja oko 30 do 40 minutae tačaka, datoteke “digitalnog potpisa” mogu biti jako male – između 40 i 1000 byte, često oko 256 (256=28).

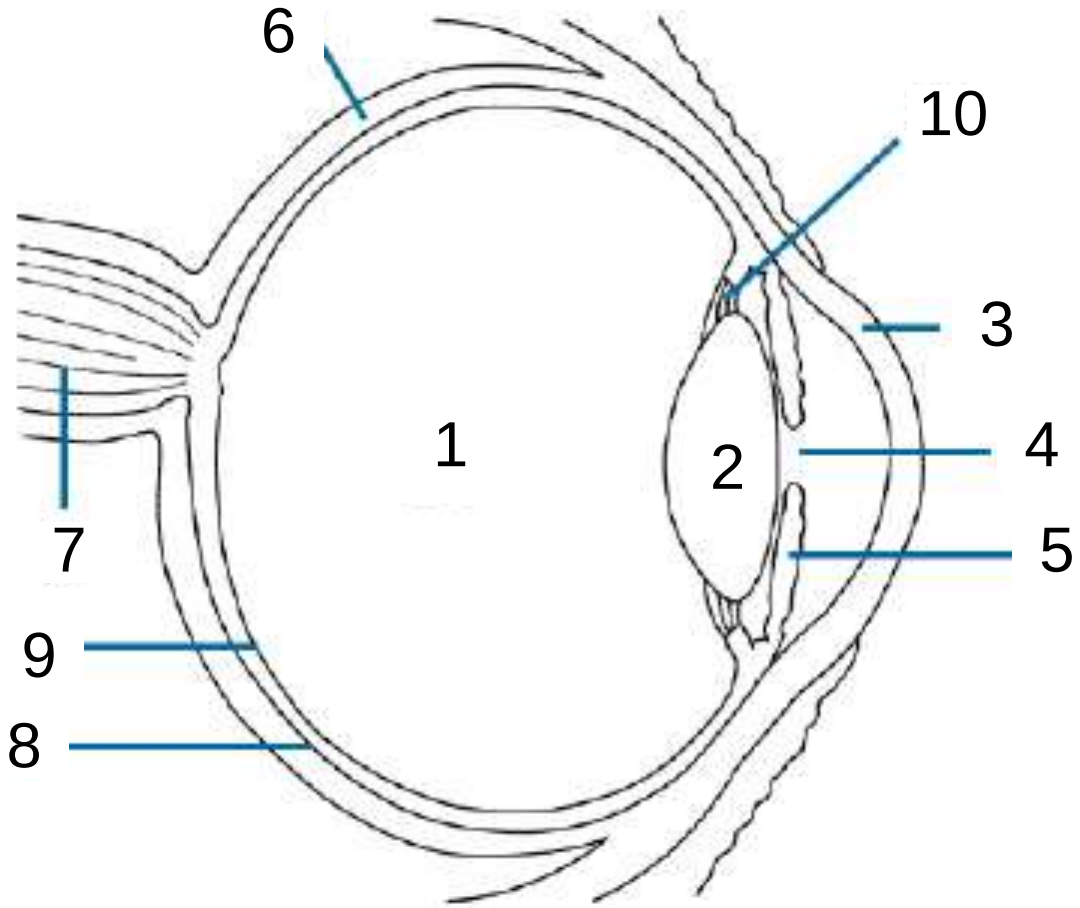
SKENIRANjE OKA

Ako se uzme u obzir činjenica da čovjek živi u svijetu slika i da 75 odsto informacija dolazi preko čula vida. Onda je sasvim jasno zašto se u savremenim sistemima identifikacije, u bezbjedonosne svrhe, ubrzano nastoji da se razviju i lansiraju sistemi za identifikaciju pomoću zjenica oka.

Postoje dvije metode prilikom određivanja identiteta osobe pomoću oka:

skeniranje dužice (irisa) i

skeniranje mrežnjače (retine) oka.



1. staklasto tijelo
2. sočivo
3. rožnjača
4. zjenica
5. dužica - iris
6. beonjača
7. očni nerv
8. sudovnjača
9. mrežnjača
10. cilijarno tijelo

6. BUDUĆNOST BIOMETRIJSKE ZAŠTITE

Upravo je ponedeljak 07:45. Zaposleni dolaze na posao kroz ulaz firme i idu ravno prema vratima sistema kontrole pristupa. Čudno, niko od njih ne kopa po novčaniku, torbi ili džepovima u potrazi za zagubljenom karticom za identifikaciju. Nema gužve ni na pultu za zamjenu bar nekoliko kartica predviđenih za taj dan. Ljudi jednostavno dolaze do automatskih vrata, prelaze prstom preko malog senzora postavljenog sa strane i vrata im se gotovo trenutno otvaraju. Kad su došli do svojih računara, više ne ukucavaju svoje lozinke već se isto tako prelaskom prsta preko senzora loguju na lokalnu mrežu sa svim njima pridruženim pravima.

ANTIVIRUS PROGRAMI

Srećom, infekcije računarskim virusima, crvima ili trojancima mogu se spriječiti, a poslijedice njihovog dejstva ublažiti ili potpuno sanirati primjenom kvalitetnog **antivirus programa**.

ANTIVIRUS PROGRAMI

Postoje dva smjera razvoja pretraživanja antivirusnih programa:

1. Generički
2. Specifican za pojedine viruse

Danasnji antivirus programi koriste obadvije metode u cilju prepoznavanja malicioznih programa.

ANTIVIRUS PROGRAMI

Generičko pretraživanje se vrši traženjem određenih "osobina" virusa. Ovako se ne može identifikovati virus već samo generička maliciozna aktivnost.

ANTIVIRUS PROGRAMI

Pretraživanje specifično za pojedine viruse se vrši tako što se u datoteci koja se pregleda traži određeni potpis koji ukazuje na virus. Ali ovako se ne može detektovati novi virus, već samo oni čiji se potpisi nalaze u internoj bazi.

ANTIVIRUS PROGRAMI

Pretraživanje virusa antivirus programom se može vršiti na dva načina:

-U stvarnom vremenu-vrši se provjera svake datoteke prije njenog izvršavanja

- Na zahtjev korisnika-pregleda hard disk

ANTIVIRUS PROGRAMI

Kvalitet antivirusnog programa se ocenjuje na osnovu:

- Brzine skeniranja
- Sposobnosti da otkrije viruse
- Lakoca instalacije
- Konfigurisanja i azuriranja liste potpisa poznatih virusa

Antivirusni programi sprečavaju zarazu tako što skeniraju fajlove koji su pokrenuti u potrazi za kodom koji bi odao prisustvo virusa.

Ukoliko ga nađu zabrane pokretanje zarazenog programa.

Već zaražene fajlove čiste tako što unutar zarazenog fajla brisu kod za koji su sigrurni da je virus.

10:20

Ako ste zaraženi nekim novim virusom o kome ne postoji podatak u internoj bazi vaseg antivirusnog programa on neće otkriti ništa ili će ga otkriti kao “mogući virus” koji neće uspjeti da očisti jer ne razlikuje ostatak koda od pravog programa u koji se ugnjezdio virus.

ANTIVIRUS PROGRAMI

10:20

Obezbjeđenje Weba i interneta

-Bezbjedonosne mjere

-Mrežna barijera

-Krađa identiteta

Firewalls

Internet

Firewall

Interna mreža

- Firewall mora da odredi šta će se propustiti u internu mrežu i/ili šta će se dopustiti da iz nje izađe
- **Kontrola pristupa** za mreže

Firewall predstavlja mehanizam zaštite u računarskim mrežama. To je sigurnosni element smješten između neke lokalne mreže i javne mreže (Interneta), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautorizovanih korisnika.

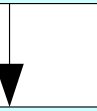
Firewall se obično nalazi na ulazu u mrežu, tj. između unutrašnje spoljašnje mreže, tako da se cjelokupan saobraćaj mora odvijati preko njega.

Namjena firewalls-a se sastoji iz sljedećih koraka:

- blokira neželjeni saobraćaj;
- usmjerava dolazeći saobraćaj na povjerljiviji interni sistem;
- prikrivaju ranjive sisteme koji se ne mogu lako zaštititi sa Interneta;
- loguje saobraćaj od i prema VPN (virtuelnoj privatnoj mreži);
- prikrivaju informacije od Interneta kao što su: imena sistema, topologija mreže,
  tipovi uređaja mreže i interna korisnička ID;
- obezbeđuje robustniju autentifikaciju nego standardne aplikacije.

Upravljanje rizikom

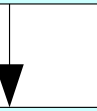
Korak 1. Procena imovine (sredstava)
Utvrdivanje vrednosti I znacaja imovine kao što su podaci, hardver, softver I mreže.



Korak 2. Ranjivost imovine (sredstava)
Registrovanje slabosti u postojecem zaštitnom sistemu u pogledu potencijalnih opasnosti.

Korak 3. Analiza gubitaka
Provena verovatnoce nastanka štete i specifikacija opipljivih i neopipljivih gubitaka.

Korak 4. Analiza zaštite
Opis postojecih kontrolnih sredstava koje treba razmotriti, verovatnoce uspešne odbrane uz njihovu pomoc i troškova.



Korak 5. Analiza odnosa troškova i koristi
Uporedivanje troškova i koristi. Razmatranje verovatnoce da dode do štete i uspešne zaštite od štete. I na kraju, donošenje odluke koje zaštitne mere instalirati.

Pitanja upravljanja

- **Programi za jačanje svijesti o bezbjednosti sistema su važni za svaku organizaciju, posebno ako je jako zavisna od IT.** Ovakvi programi trebalo bi da postoje na nivou korporacije i to uz podršku višeg rukovodstva. Pored toga, praćenje bezbjedonosnih mjera i obezbjeđenje pridržavanja administarativnih kontrolnih sredstava su bitni za uspješnost plana obezbjeđenja.

- **Kontrola IS treba da bude institucionalizovana i ugrađena u organizacionu kulturu.** Potrebno je da organizacije kontrolišu IS ne zato što to zahtjeva osiguravajuća kompanija, već time što mogu da uštede znatne sume novca.