II – Pretnje, napadi, sigurnost i metode zaštite

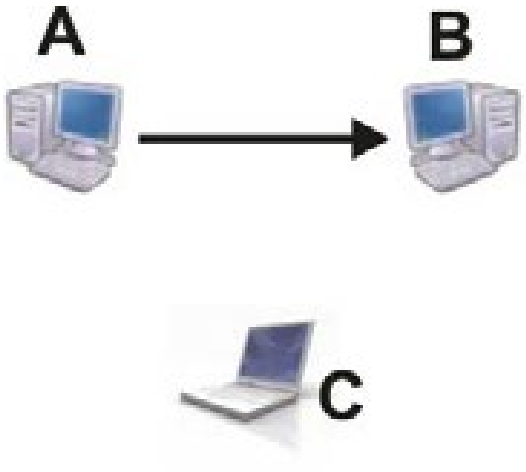
S A D R Ž A J

1. Napadi i pretnje
2. Metode eksplatacije slabosti
3. Programske pretnje
4. Sistemske pretnje
5. Metode zaštite

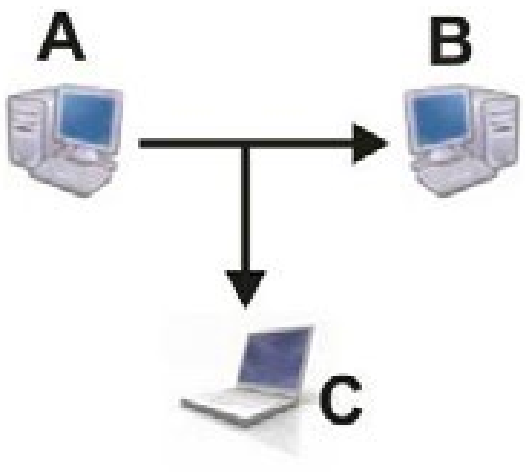
1 – Napadi i pretnje

- Sve većom upotrebom računarskih i komunikacionih tehnologija za savremeno poslovanje, problem sigurnosti sve više dobija na značaju tako da se njemu mora posvetiti posebna pažnja.
- Samim tim javila se i potreba za novim i automatizovanim alatima za zaštitu datoteka i drugih informacija.
- Sigurnost neke informacije možemo da posmatramo kroz tri aspekta:
  1. ***napad na sigurnost*** *(security attack)* bilo koja akcija koja ugrožava sigurnost informacija;
  2. ***sigurnosni mehanizam*** *(security mechanizam)* mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada;
  3. ***sigurnosna usluga*** *(security service)* usluga koja povećava sigurnost sistema za obradu i prenos podataka. **Sigurnosna usluga** podrazumeva primenu jednog ili više sigurnosnih mehanizama.
- Napadi predstavljaju akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža.
- Postoje različite vrste napada, mi ćemo ih kategorisati u 5 kategorija.

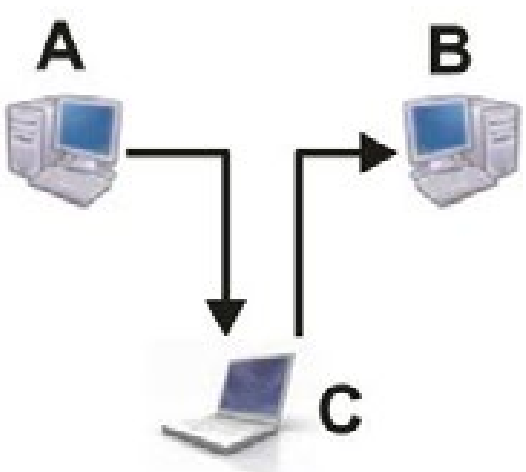
1 - Napadi i pretnje



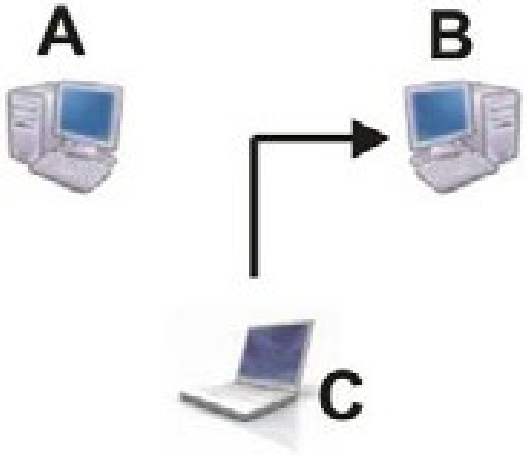
a) Normalan tok



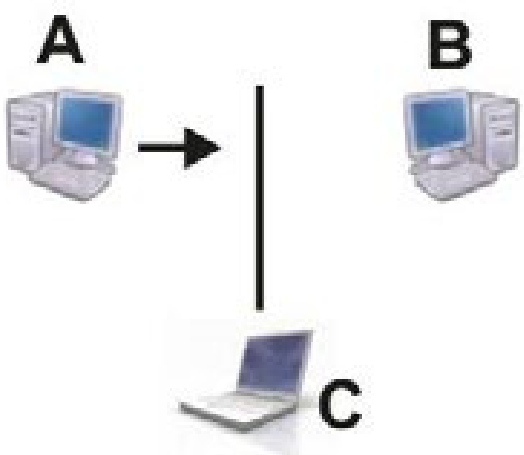
b) Prisluškivanje



c) Modifikacija



d) Uklanjanje informacija



e) Prekid toka

1 – Napadi i pretnje

b) **Hvatanje ili Prisluškivanje** (*interception*) - napad na poverljivost (*confidentialy*). Hvatanje u praksi predstavlja prisluškivanje sabraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije i slično.

c) **Izmena** (*modification*) - napad na integritet (*integrity*) jer je osnovni cilj neovlašćeno brisanje, umetanje ili izmena podataka. Iako menja podatke ili sistem, često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.

d) **Uklanjanje ili proizvodnja** (*fabrication*) - napad na autentičnost (*authenticity*). Napadač izvodi ovaj aktivni napad tako što generiše lažne podatke, lažni saobraćaj ili izdaje neovlašćenje komande.

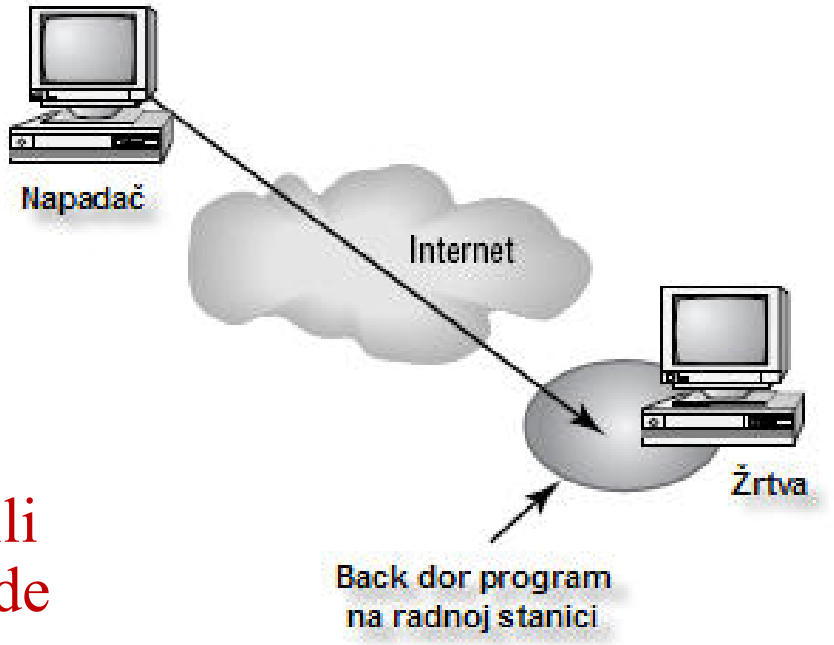
e) **Presecanje** (*interruption*) - napad na raspoloživost (*availability*). Ovim načinom se prekida tok informacija, čime se onemogućava pružanje neke usluge.

f) **Napadi radi „gušenja“ servisa i distribuirano „gušenje“ servisa**

Napadi radi „gušenja“ usluga (*Denial of Service-**DOS***) onemogućavaju ovlašćenim korisnicima pristup računar. resursima i njihovo korišćenje.

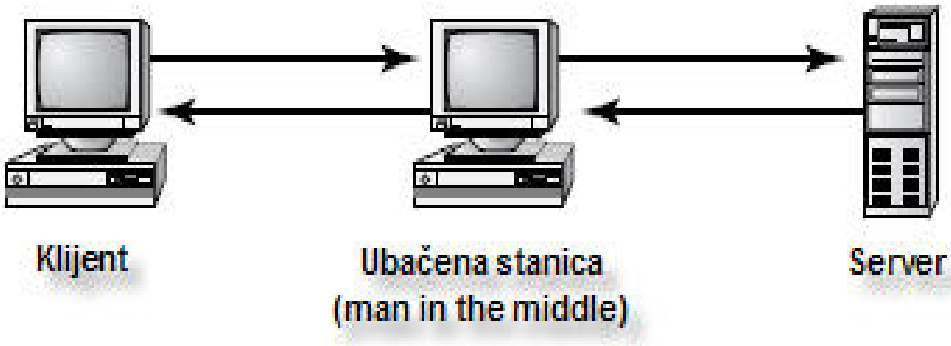
1.1 – Back door napad

- Većina tehnika je dizajnirana da koristi potencijalne slabosti sistema
- Te slabosti mogu biti „vezane“ za proveru programa ili za protokole
- Veliki broj napada je tehnički veoma složen, tako da se retko javljaju.
- Pojam ***back door*** može imati dva različita značenja.
- Programeri su namerno ostavljali prolaze (zadnja vrata) u složene sisteme i aplikacije tokom razvoja.
- Kroz njih su mogli ispitati operacije u samom kodu tokom njegovog izvršenja,a zatim su ih uklanjali pre nego što bi bio prosleđen proizvodnji
- Kada bi proizvođač softvera otkrio prolaz koji nije uklonjen, obično bi objavljivao zakrpu koja bi zatvarala takav prolaz.
- Drugo značenje pojma *back door* vezano je za ostvarivanje pristupa nekoj mreži i ubacivanje programa ili rutine koja kreira ulaz za dalje napade



1.2 – Man in the middle

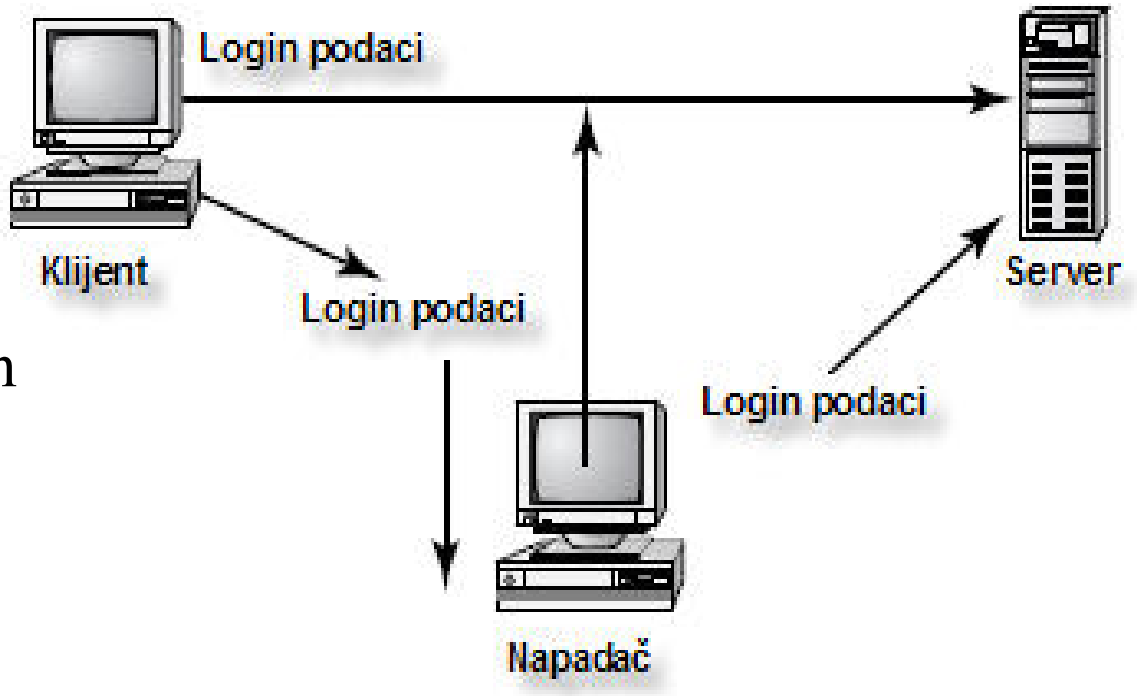
- Napad tipa ***man-in-the-middle*** je prilično složen u tehničkom smislu.
- Pripada grupi pristupnih napada, mada se može posmatrati kao početni korak u napadu s ciljem izmene podatka.
- Ovde se između servera i klijenta postavlja odgovarajući softver tako da administrator i korisnici ne budu svesni njegovog prisustva
- Ubačen softver beleži presretnute podatke radi kasnijeg pregleda, menja podatke ili na bilo koji drugi način ugrožava sigurnost korisničkih sistema i sesije a zatim ih šalje na server, kao da se ništa nije desilo.
- Server reaguje normalno na tako dobijene podatke, uveren da se komunikacija odvija s legitimnim klijentom.
- Softver ``napadač`` i dalje nastavlja slanje podataka na server i kompletan proces se produžava.



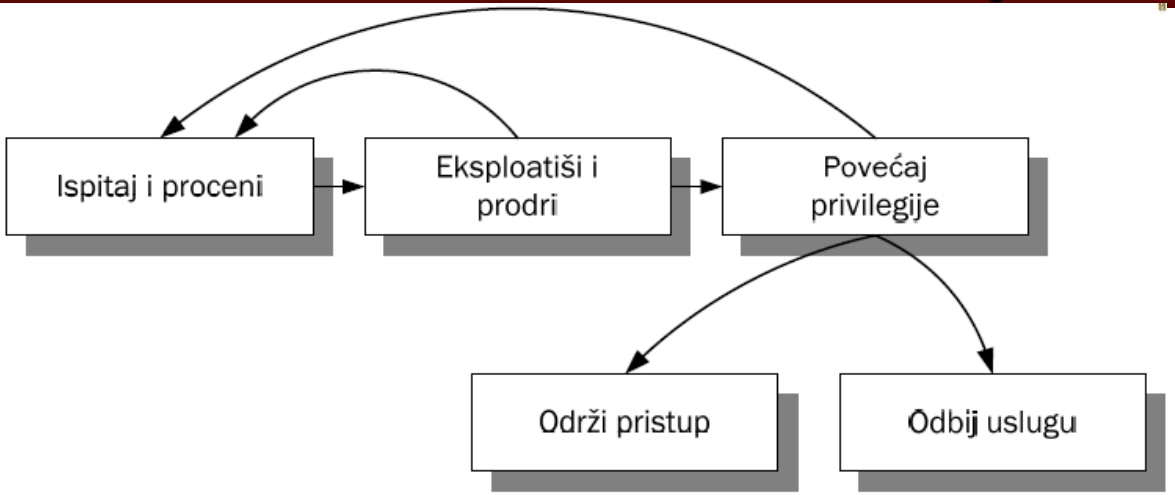
1.3 – Replay napad

- **Replay** napadi postaju sve češći u praksi.
- Izvode se zadržavanjem podataka koji se razmenjuju na mreži, u cilju osiguranja pristupa mreži (pristupni napad) ili izmenu podataka
- U distribuiranom okruženju između klijenata i sistema za identifikaciju se stalno šalju podaci o **imenu** i **lozinci** korisnika.
- Napadač može zadržati takve podatke i naknadno ih ponovo poslati.
- Isto važi i za sigurnosne certifikate u sistemima poput Kerberos-a.

- Napadač može ponovno iskoristiti uhvaćeni certifikat, u nadi da će biti prihvaćen na sistemu za identifikaciju i da će on nadmudriti bilo kakvu zaštitu u vidu vremenske osetljivosti.



1 – Osnovni koraci napadača



1. **Ispitaj i proceni** (*survey and assess*) - istražne radnje radi ispitivanja potencijalne mete i indentifikovanje i procena njenih karakteristika.
2. **Eksoploatiši i prodri** (*exploit and penetrate*) - pokušava da eksploatiše ranjivost i da prodre u mrežu ili sistem.
3. **Povećaj privilegije** (*escalate privileges*). Nakon ubacivanja (*injecting*) koda u aplikaciju, pokušava da poveća svoja prava
4. **Održi pristup** (*maintain access*) - preduzima korake da olakša buduće napade i da prikrije tragove (*back-door* programi, brisanje *log* fajlova)
5. **Odbij uslugu** (*deny service*)-ako ne može da pristupi sistemu, preduzima napad koji prouzrukuje odbijanje usluge (***DoS*** napad)

2 - Metode eksplatacije slabosti

1. **Odbijanje usluga** (*Denial of Service, DoS*).
   DoS izaziva prestanak rada servisa ili programa, čime se drugima onemogućava rad s tim servisima ili programima. DoS napad se najlakše izvršava na transportnom sloju, slanjem velikog broja SYN paketa (TCP CONNECTION REQUEST), zaštita se postiže kontrolisanjem broja SYN paketa u jedinici vremena.
2. **Lažiranje IP adresa** (*spoofing*).
   Napadač prati IP adrese u IP paketima i predstavlja se kao drugi računar. Kako DNS ne proverava odakle dolaze informacije, napadač može da izvrši napad lažiranjem tako što DNS servisu daje pogrešnu informaciju.
3. **Njuškanje** (*sniffing*).
   Napadač specijalnim programima presreće TCP/IP pakete koji prolaze kroz određeni računar i po potrebi pregleda njihov sadržaj. Kako kroz mrežu obično kreću nešifrovani podaci, program za njuškanje (***snifer***) lako može doći do poverljivih informacija.

3 – Zlonamerni programi

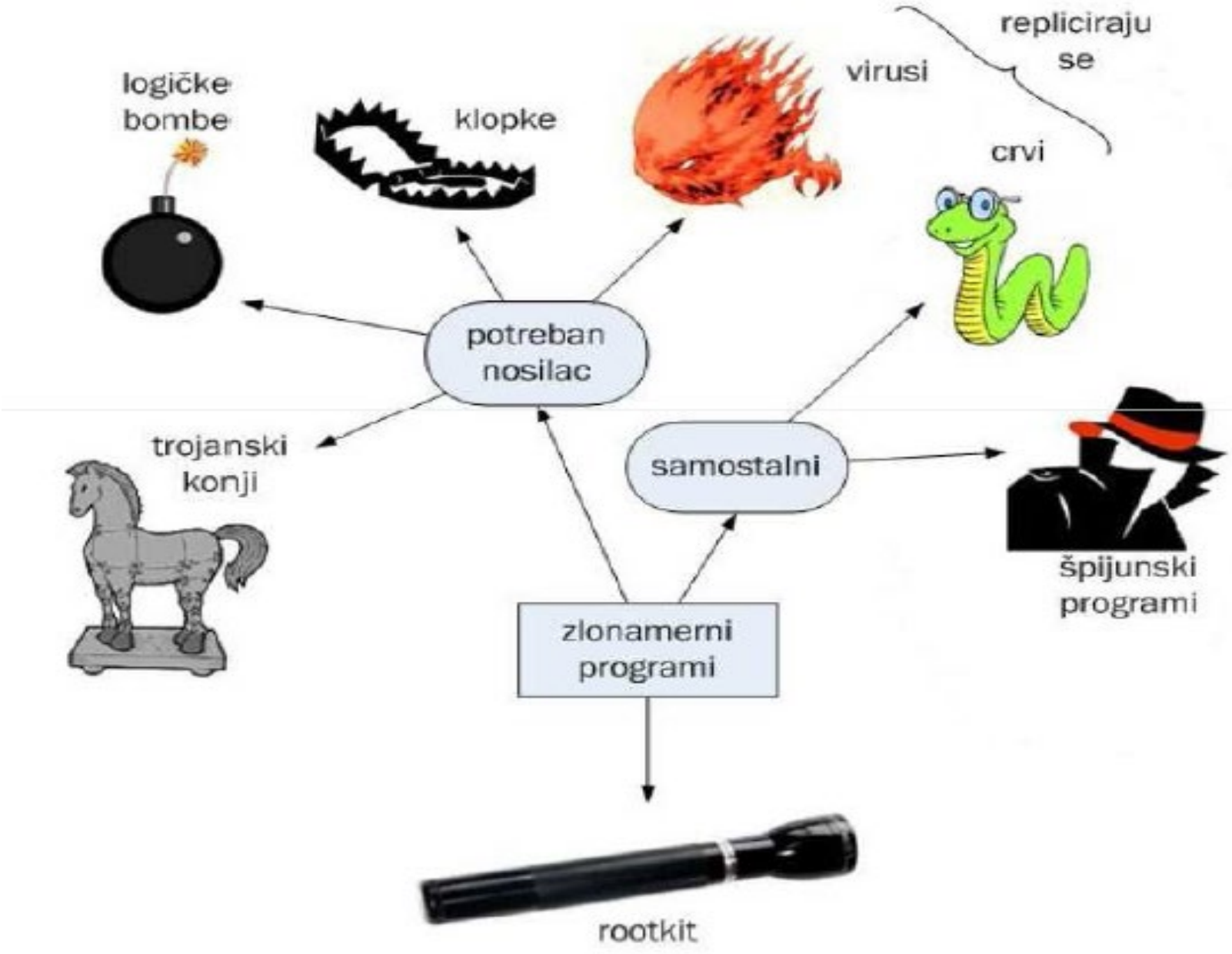
- Označavaju široku kategoriju softverskih pretnji usmerenih na mreže i računarske sisteme.
- Takve pretnje obuhvataju viruse, „trojance“, logičke “bombe“ i „crve“.
- Administrator sistema zaštite treba da pomogne svojim korisnicima u stvaranju uslova za siguran rad i za odbijanje takvih napada.
- Ukoliko je takav napad uspešan, on može napraviti pustoš na računaru, uz dodatno širenje preko čitave mreže.

Vrste zlonamernih programa

- Zlonamerni programi se klasifikuju na dva načina:

1. **Zavisne** programe kojima je nephodan nosilac odnosno program u kome će biti sakriveni(trojanski konji, virusi) i **nezavisne** (samostalne) kojima nije neophodan nosilac (crvi, špijunski programi).
2. Prema drugom kriterijumu, zlonamerni programi se dele na one koji se **repliciraju** (virusi, crvi) i na one koji se **ne repliciraju** (trojanski konji, logičke bombe).

3 – Zlonamerni programi



3.1 – Programske pretnje

1. **Trojanski konj** (*trojan horse*) ilegalan je segment koda, podmetnut u kod nekog programa. Na primer, u editor teksta može biti podmetnut potprogram koji pretražuje otvorenu datoteku, i u slučaju da pronađe željenu sekvencu kopira datoteku na mesto dostupno programeru koji je napisao taj editor.

2. **Klopka** (*trap door*) Autor programa može slučajno ili namerno ostaviti prazna mesta u svom kodu (klopku) pa potencijalni uljez koji zna za ta mesta može da podmetne svoj kod i time ostvari dobit.

3. **Prekoračenje** tj. **prelivanje bafera** (*buffer overrun, bufer overflow*) na steku ili u dinamičkom delu memorije. Prekoračenje bafera je najčešći napad sa mreže pri pokušaju neovlašćenog pristupanja sistemu. Ovlašćeni korisnici takođe mogu da odaberu ovu vrstu napada kako bi prevarili sistem i ostvarili veća prava od onih koja imaju. Napadač koristi grešku u programu, to jest, neodgovarajuću kontrolu razdvajanja steka, podataka i koda.

3.2 – Trojanski konji

- ***Trojanac koji otvara zadnja vrata*** program koji omogućava udaljenom korisniku da pristupi inficiranom računaru (*Back Orifice*)
- ***Kradljivci informacija*** PSW trojanac pokušaće da pretraži inficirani računar kako bi došao do poverljivih informacija kao što su lozinke, privatni i javni ključevi, sertifikati i podaci sa kreditnih kartica.
- ***Trojanski špijuni*** (*trojan spy*) i ***obaveštajci*** (*keylogging*), snima ekrane ili na neki drugi način omogućava napadaču da prati rad korisnika.
- ***Nosioci softvera*** su obično realizovani u vidu trojanskih konja koji se nakon instalacije ponašaju kao magnet za drugi zlonameran softver.
- ***Trojanski proksi server****(trojan proxy)* pokušaće da pretvori inficirani računar u proksi server, čime se udaljenim korisnicima dozvoljava da preko inficiranog računara anonimno pristupe Internetu (DoS napad).
- ***Programi koji pozivaju telefonske brojeve*** Cilj programa jeste da žrtva dobije ogroman telefonski račun.

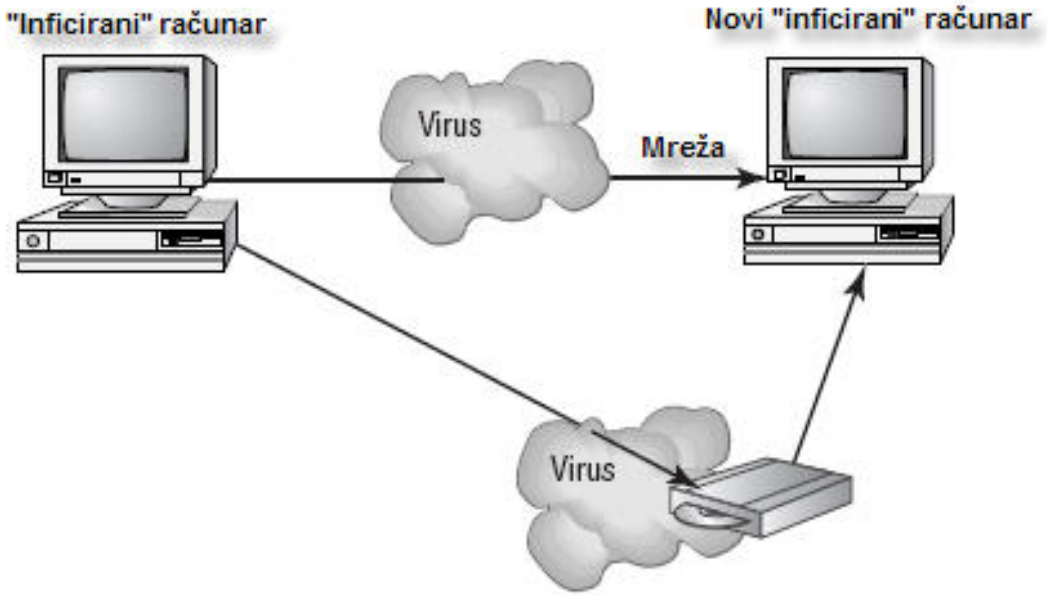
➢ Trojanci se mogu iskoristiti za narušavanje sistema zaštite ciljnoj mreži, pri čemu mogu proći godine pre nego što budu detektovani.

➢ Zabrana pristupa trojancima je najbolja preventiva protiv njih.

4 - Sistemske pretnje

- Zlonamerno korišćenje datoteka i sistemskih resursa nazivaju se sistemske pretnje.
- Dve metode kojima se one mogu postići jesu crvi i virusi.

1. **Crvi** su samostalni zlonamerni programi koji se šire s računara na računar. Uobičajne metode prenošenja na žrtvu jesu upotreba elektronske pošte i Internet servisa.
2. **Virusi** su delovi (fragmenti) koda koji se ubacuju u druge legitimne programe, virus zahteva nosioca u vidu izvršne datoteke.



4.1 - Sistemske pretnje - crvi

- Crvi (*worm*) se razlikuju od klasičnih virusa po tome što imaju moć reprodukcije, predstavljaju zaokruženu celinu i ne zahtevaju host-aplikaciju za prenošenje.
- Veliki broj virusa koji zaokupljaju pažnju medija i štampe u principu i ne pripada virusima, već je reć o crvima.
- Ipak, crvi mogu čak sadržati i viruse, tako da se mogu iskoristiti za isporuku virusa na ciljni sistem.
- Postoje:
  - E-mail crvi,
  - IM *crvi(Instant messaging*)
  - Internet crvi,
  - *File sharing* crv.

4.2 - Sistemske pretnje - virusi

- Virus je softver koji je kreiran radi „inficiranja“ računarskog sistema.
- U najvećem broju slučajeva virusi pokušavaju da postignu jedan od dva moguća cilja: da onesposobe računarski sistem ili da se prošire na druge sisteme.
- Pojedini virusi ne preduzimaju nikakve druge akcije, osim što se smeštaju na napadnutom računaru.
- Drugi oblici virusa mogu oštetiti podatke na hard disku, uništiti operativni sistem i proširiti se na ostale računare.
- Virusi dospevaju na računar na jedan od tri moguća načina: preko „zaražene“ diskete/CD diska, elek.poštom ili kao deo drugog programa
- Ukoliko je računar „zaražen“, virus će verovatno pokušati da se „prikači“ na sve datoteke na računaru da bi mogao da pređe i na ostale sisteme prilikom slanja dokumenata drugim korisnicima.
- Kada „zaraženi“ disk damo drugom korisniku ili ga postavimo u drugi računar, virus će „zaraziti“ i taj računar.
- Virusi se mogu naći u sistemima datoteka i okruženjima za izvršenje makroa i skriptova (*script host*).

4.2 - Sistemske pretnje - virusi

- Računarski virus se obično sastoji od tri dela.
  1. deo koji omogućava razmnožavanje virusa - obvezan deo virusa
  2. nosiva komponenta (*payload*) koja može biti bezopasna ili opasna i nije obavezna
  3. funkcija za okidanje ili takozvana *trigger* funkcija-određuje vreme (a ponekad i događaj) kada će se aktivirati nosiva komponenta virusa, nije obvezna
- Prema svom načinu delovanja, virusi se dele se na dve vrste:

Nerezidentne viruse-nalaze se u RAM memoriji samo u vreme njihovog izvršavanja. Njihovo širenje se zasniva na principu da deo njihovog koda pronalazi datoteke koje mogu biti zaražene (.exe., .doc i slično), a drugi deo koda kopira virusni (zaraženi) kod u pronađenu datoteku.

Rezidentne viruse-prilikom njihovog izvršavanja učitaju se u memoriju i njihov kod ostaje u memoriji sve vreme rada računara. Da bi se zadržali u memoriji oni koriste tehnike TSR („*terminate and stay resident*“) i manipulaciju memorijskim blokovima (MBC)

- Maliciozni kod rezidentnih virusa koristi mehanizme OS za aktiviranje

4.2 – Vrste virusa

Virusi koji napadaju sisteme datoteka **-** za svoje širenje koriste jednu ili više vrsta sistema datoteka, a najčešće inficiraju izvršne datoteke.
Prema metodima inficiranja, virusi ovog tipa mogu se podeliti na:

- **prepisujuće** (*overwriting*), virusi koji prepisuju postojeći kod
- **parazitske viruse** (*parasitic*) – dodaju svoj kod u datoteku na početku, kraju ili u sredini koda. Ovi virusi se lako otkrivaju i čiste sa izvršnih datoteka na osnovu antivirusnih definicija.
  Kao posebna kategorija izdvajaju se **EPO virusi** koji upisuju rutinu koja izvršava telo virusa negde pri sredini datoteke.
- **pridružujući**(*companion*)-ne menjaju sadržaj orginalne datoteke, već samo njeno ime, a prave novu datoteku sa virusem pod istim imenom
- **viruse startnog zapisa**(*boot-sector*)-svoj kod upisuju u glavni startni zapis čvrstog diska(MBR record) ili startni zapis(boot sector) aktivne particije na disku. Po potrebi, virus ovog tipa može upisati svoj kod u neki sektor na disku, a zatim promeniti vrednost u MBR-u. Zasnovani su na principima na kojima radi rutina(potprogram) za podizanje OS.

4.2 – Vrste virusa

Makro virusi

- Koriste poboljšanja koja su dodata brojnim aplikativnim programima.
- Word podržava mini-BASIC prog., koji osigurava automatiziranje rada
- Takvi programi koji postoje u okviru datoteka nazivaju se makroi.
- Makro virusi mogu zaraziti sva dokumenta na ciljnom računaru, uz mogućnost širenja na druge računare putem elektronske pošte.
- imaju mogućnost da sami sebe kopiraju, brišu i menjaju dokumente

Skript virusi

- Podskup virusa koji napadaju sisteme datoteka koji su pisani na script jezicima (VBS, JavaScript, BAT, PHP).
- Script su sposobni da inficiraju datoteke u drugom formatu, kao što je HTM, ukoliko te datoteke dozvoljavaju izvršavanje skriptova.

Link virusi

- u trenu inficiraju napadnuti računar i mogu izazvati pravi haos na disku

4.2 - Metode prikrivanja virusa

Enkriptovani virusi - kriptovanje binarnog tela virusa enkripcijskim algoritmom sa namerom da se teže detektuje. Kriptovani virus se tipično sastoji od 2 dela, prvi deo je kriptovano telo virusa a drugi deo je kod za dekripciju. Kada se inficirani program pokrene prvo se telo virusa dekriptuje u memoriji a onda se kontrola prebacuje na dekriptovano telo

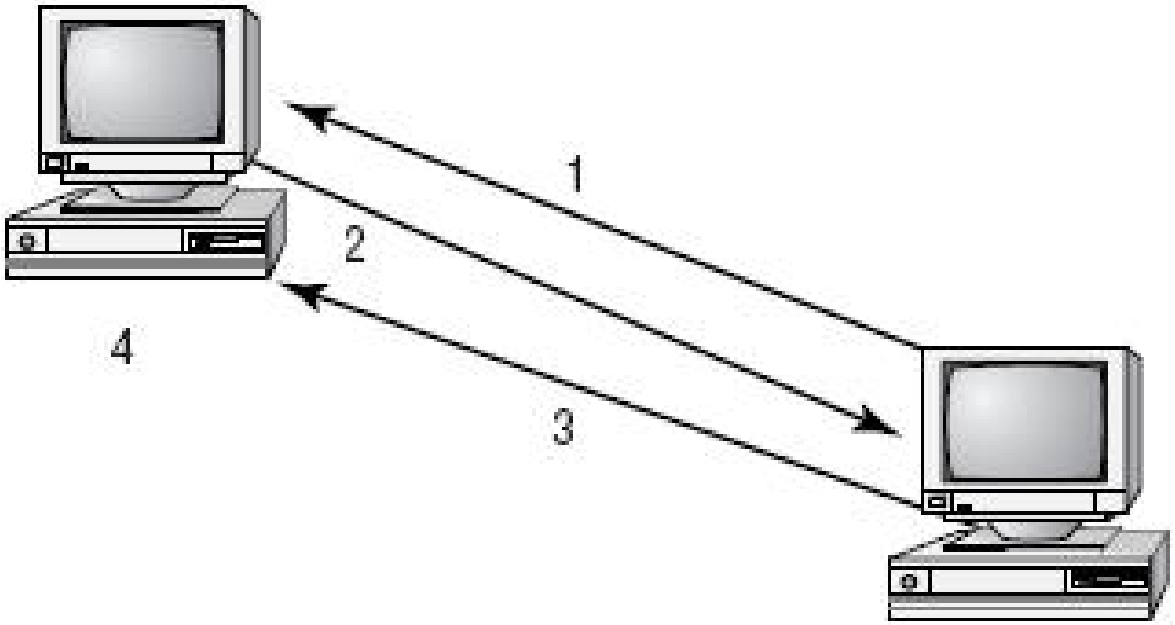
Oligomorfni virusi - kriptovani virusi koji zahtevaju više različitih kodova za dekripciju. Teže ih je otkriti nego viruse koji koriste samo jednu metodu dekripcije.

Polimorfni kod - inficira datoteke s kriptovanom kopijom sebe i modulom za dekriptovanje, gde se taj modul menja (mutira) kod svake infekcije. Dobro napisani polimorfni virusi nemaju delova koji ostaju isti nakon infekcije, što otežava otkrivanje virusa metodom potpisa.

Metamorfni kod- menja (mutira) celo telo virusa kod novih infekcija. Nije ih moguće otkriti upoređivanjem s popisima virusnih "potpisa". Prednost nad polimorfnim virusima je što se telo virusa ne dekriptuje u memoriji pa ga je nemoguće presresti i analizirati.

4.3 – Logičke bombe

- Logičke bombe predstavljaju programe ili delove programskog koda koji se izvršavaju nakon pojave unapred definisanog događaja, na primer u određeno vreme ili određenog datuma, ukoliko na disku postoji određena datoteka ili ako se na sistem prijavi određeni korisnik.
- Kada se aktivira, logička bomba se najčešće ponaša destruktivno.



1.Napadač implantira logičku bombu
2. "Žrtva" izvještava o instalaciji
3.Napadač šalje poruku o napadu
4."Žrtva" radi po nalogu logičke"bombe"

4.4 - Spyware/adware

- Predstavljaju varijante malicioznog softvera koji prikuplja i šalje podatke o ponašanju korisnika računara bez njegovog znanja.
- Ovi programi mogu vršiti puno različitih funkcija uključujući prikazovanje neželjenih reklama, prikupljanje privatnih podataka kao što su brojevi kreditnih kartica, re-rutiranje zahteva za web stranicama kako bi se ostvarili prihodi od referisanja novih korisnika, instaliranje teško uočljivih "dialera", itd...
- Adware se u mnogome poklapa sa definicijom spyware-a, sa tom razlikom da adware-a isključivo služi u komercijalne svrhe (ad je skraćenica od advertisment).
- Adware programi prikupljaju informacije o ponašanju korisnika, web sajtovima koje korisnik posećuje i uz pomoć različitih mehanizama (najčešće cookie, activex, javascript), istim korisnicima se serviraju odgovarajuće reklame, nude odgovarajući proizvodi putem emaila i sl.
- Zanimljiv podatak je da je čak 90% računara u svetu zaraženom nekom vrstom ***spyware*** programa.

4.5 – Exploiti i Rootkit

- **Exploiti** su programi koji koriste određnu slabost nekog programa, oni najčešće sami po sebi ne nanose štetu i postoje samo da bi se demonstrirala slabost nekog programa, ali njihove "usluge" često vrlo rado koriste crvi, virusi, ***spyware*** i sl.
- **Rootkit** je softver koji se ubacuje na računar pošto je napadač dobio kontrolu sistema, sa zadatakom da olakšaju *remote* kontrolu i da sakrije tragove upada brisanjem log fajlova ili sakrivanjem procesa koji su pod kontrolom napadača.
- Često ***rootkit-ovi*** sadrže i ***backdoor-ove***, omogućavajući olakšani naknadni upad ili *exploit* programe za napade na druge sisteme.
- Važno je primetiti da se ciljani napadi obično izvode sa sistema koji su takođe prethodno bili ugroženi, da bi se sa njih mogli ukloniti dokazi o identitetu napadača, jer napadač dobija mogućnost da ukloni dokaze
- ***Rootkit-ovi*** se vrlo često vezuju za kernel nivo, pa ih je teško otkriti, a kada se jednom otkriju vrlo je bitno da se kompletno reinstalira sistem, kako bi se sigurno uklonili svi tragovi ***rootkita***.

5 – Metode zaštite

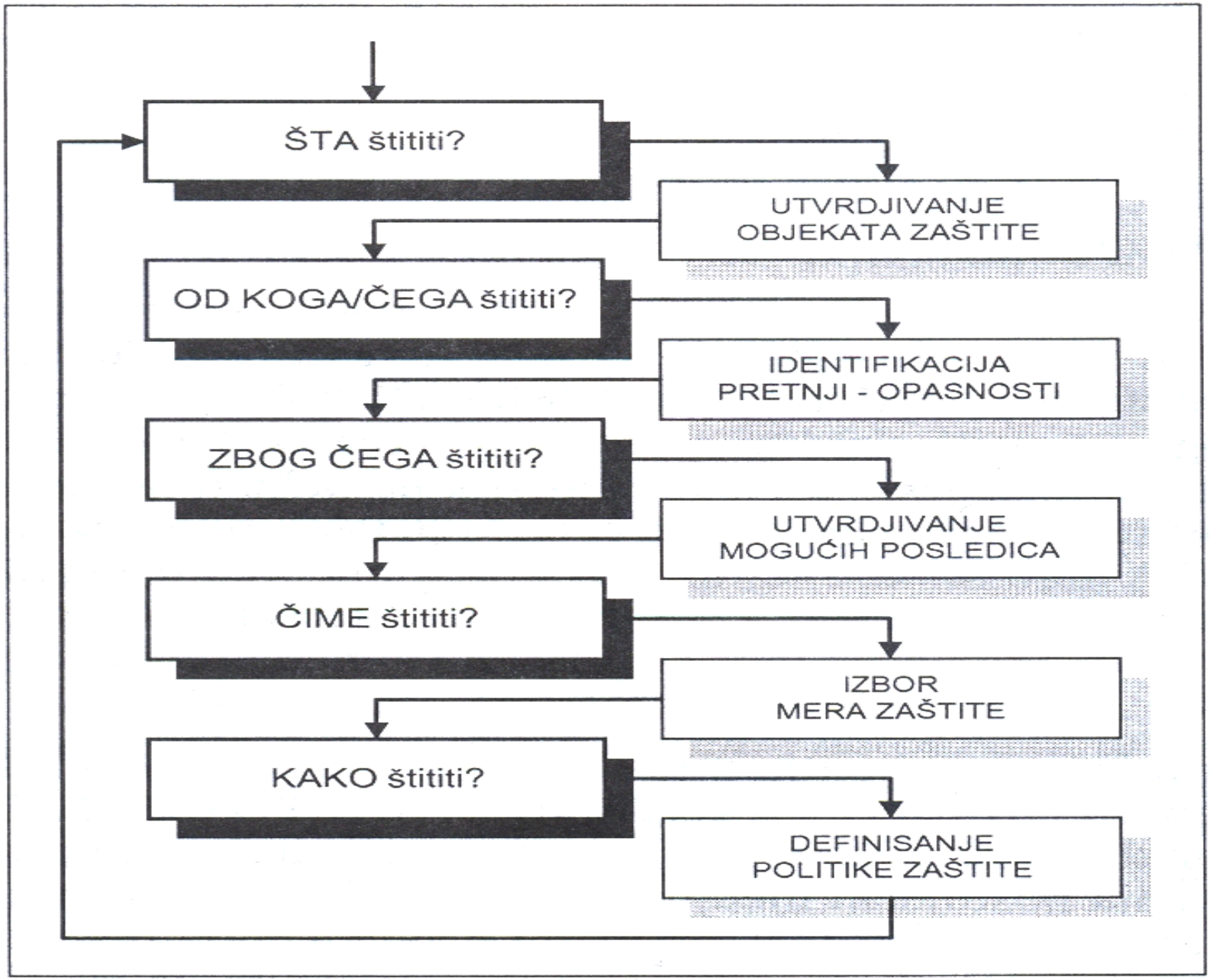
- Zaštita informacionih sistema podrazumeva preduzimanje odgovarajućih mera i akcija kako bi se zaštitili podaci i oprema od mogućih nepredviđenih događaja sa neželjenim posledicama.
- Treba da se onemogući svako slučajno ili namerno, narušavanje, sužavanje ili sprečavanje funkcija računarskih sistema, tj. otuđenje, uništenje, oštećenje, izmena ili neovlašćeno korišćenje inform.resursa
- Treba omogućiti neophodne uslove kako bi se sve funkcije, podaci i informacije koristile na **očekivan i unapred definisan** način.
- Sve potencijalne pretnje koje mogu ugroziti inform.sistem možemo klasifikovati u tri kategorije i to: **nesreće**, **greške** i **kriminal**.
- Shodno tome možemo navesti **četiri razloga**, čijom se analizom može dobiti odgovor koje i kakve metode treba upotrebiti u zaštiti:

1. vrednost hardvera i softvera;
2. raznovrsnost funkcija računarskih sistema;
3. raznovrsnost, priroda i značaj podataka i informacija koji se u okviru računarskih sistema prikupljaju, uređuju, skladište i obrađuju,
4. karakteristike računarskih sistema.

5 – Metode zaštite

- U cilju pronalaženja i razrade sve obuhvatnog pristupa, koji bi trebao da pruži pouzdan osnov za osmišljeno, organizovano, stručno i racionalno razrešavanje problema zaštite računarskih sistema, potrebno je uvek imati u vidu nabrojane razloge.
- Uvek treba poći od nesporne činjenice da bilo koji sistem zaštite ima smisla **ako i samo ako** se njime **nešto**, **od nečega** i **zbog nečega** štiti, a da bi se postigao cilj on svoju funkciju mora izvršavati **sa nečim** i **na neki način**.
- Iz ovakve opšte konstatacije nije teško uočiti logičke celine i, što je vrlo bitno, njihov redosled kojim je moguće obaviti neophodno izučavanje i očekivano razrešavanje razmatranog problema.
- Ove logičke celine se, po principu "**zlatnih pitanja**" kriminalistike, mogu iskazati odgovarajućim "zlatnim pitanjima" informatičke zaštite koja su prikazana na sledećem slajdu
- Na sva ova pitanja potrebno je da se daju potpuni odgovori i to u prikazanom redosledu i bez preskakanja pojedinih pitanja

5 - Metode zaštite



5 - Metode zaštite

- Glavni entiteti problema zaštite u oblasti informacionih sistema su **objekti**, **pretnje**, **posledice**, **mere** i **politika zaštite**.
- Ovakav pristup omogućava da se problem zaštite, radi jasnoće i lakšeg uočavanja postojećih međuzavisnosti, prikaže u vidu 3-dimenzije

$$Mz=M(Oi, Pj, Sk)$$

pri čemu svaki element matrice **Mi,j,k** predstavlja skup mera koje bi trebalo primeniti da bi se sprečila **posledica Sk**, koja može nastupiti ako **pretnja Pj** ugrozi **objekt Oi**.

1. **Objekti** - Nalaženje odgovora na pitanje ***Šta štititi?*** je prvi ključni korak u izučavanju i razrešavanju problema zaštite u inform.sistemima

- Ukoliko je skup odgovora na postavljeno pitanje prazan skup, otpada i svaka potreba preduzimanja bilo kakvih aktivnosti na ovom planu.
- U svakom informacionom sistemu postoji čitav niz objekata čije vrednosti nedvosmisleno nameću potrebu njihove zaštite: **podaci**, **datoteke**, **baze podataka**, **optičke slike dokumenata**, **digitalni zapis zvuka i slike**, **softver**, **programi**, **komunikaciona oprema**, **hardver...**

5 – Metode zaštite

2. **Pretnje** - Na pitanje ***od koga*** ili ***od čega*** se trebamo štititi dobićemo odgovore koji sadrže sve klasične rizike, kao što su vatra, voda, eksplozija, računarski kriminal, greške i druge, ali i specifične pretnje, kao što je kompromitujuće elektromagnetno zračenje.

- Ovi specifični rizici najčešće imaju nematerijalno poreklo, ili manifestaciju, što dokazivanje njihovog postojanja, kao i procenu mogućih gubitaka, čini vrlo teškim.
- Određenu teškoću predstavlja i neograničen broj pretnji koje mogu ugroziti informacioni sistem, pa ih je i nemoguće sve predvideti.
- Među pojedinim pretnjama postoji određena međuzavisnost koja usložnjava uticaj na informacioni sistem.
- Pretnje koje su usmerene na ugrožavanje sigurnosti toka informacija u računarskim sistemima i mrežama generalno se mogu klasifikovati u četiri osnovne kategorije:

1. **Prisluškivanje**
2. **Modifikacija**
3. **Uklanjanje**
4. **Pekid toka informacija**.

5 – Metode zaštite

3. **Posledice** - Odgovorom na pitanje ***Zbog čega štititi?*** utvrđuju se negativne posledice koje identifikovane pretnje mogu da izazovu.
   - Neke katrgorije ovih posledica su: delimično ili potpuno oštećenje, otuđenje, modifikacija hardvera i softvera, otkrivanje podataka, prekid rada sistema, ...

4. **Mere** - Na pitanje ***Čime štititi?*** dobijamo identifikaciju svih mera koje stoje na raspolaganju u izgradnji celovitog i pouzdanog sistema zaštite.
   - Sve te mere, po svojim prirodnim svojstvima koja ih karakterišu, mogu se razvrstati kao:

   I. Mere ***normativnog karaktera***, - *pravne, organizacione i kadrovske mere,* pripadaju kategoriji ***netehničkih mera***. Osnovna karakteristika ovih mera je da ne degradiraju rad sistema, već znatno doprinose povećanju njegove raspoloživosti i produktivnosti, a istovremeno značajno utiču na efikasnost sistema zaštite (npr. prava pristupa I korišćenja podataka).

5 – Metode zaštite

II. ***Fizičko-tehničke*** mere uslovljavaju ih finansijske investicije pre nego što počnu da dejstvuju, plus troškovi njihovog tekućeg održavanja. Efikasnost ovih mera opada kada normativne mere nisu primenjene na adekvatan način (npr. fizičko obezbeđenje IS, restriktivni prostor, Faradejev kavez, kripto uređaji i slično).

III. ***Logičke*** mere su snažno sredstvo zaštite čijom primenom se postiže visok stepen efikasnosti "u paketu". Ove mere povlače za sobom tzv. prikrivene troškove, jer direktno utiču na smanjenje raspoloživosti i efikasnosti računar.sistema, a to je dovoljan razlog da se njihovoj primeni pristupi krajnje odgovorno, osmišljeno i racionalno

IV. ***Kriptološke*** mere zaštite predstavljaju veoma značajne mere i zajedno sa merama zaštite od kompromitujućeg elektromagnetnog zračenja omogućavaju ostvarivanje visokog nivoa zaštite.

5. **Politika** - Glavno pitanje je *Kako štititi?* a to znači utvrđivanje strategije za upravljanje rizikom u ambijentu informacionih sistema. Radi toga pristupa se procesu analize i procene rizika.

5 – Metode zaštite

1. *kriptografske metode,*
2. *organizacione metode*
2. *programske metode,*
4. *fizičke metode.*

- Mnogi smatraju da je ova podela zastarela i sve češće se koristi šema zasnovana na 10 domena sigurnosti koje je definisala organizacija **(ISC)²** (*International Information Systems Security Certification Consortium):*

1. **sistemi za kontrolu pristupa,**
2. **sigurnost razvoja aplikacija i sistema,**
3. **planiranje oporavka od napada i obezbeđivanje kontinuiranog poslovanja,**
4. **kriptografija,**
5. **pravni i etički aspekti sigurnosti,**
6. **fizička sigurnost,**
7. **sigurnost operative,**
8. **upravljanje sigurnosnim sistemima,**
9. **sigurnosne arhitekture i modeli,**
10. **sigurnost komunikacionih i računarskih mreža.**

5 – Metode zaštite

Različiti aspekti zaštite

1. ***Zaštita na nivou aplikacije -*** obuhvata softversku zaštitu aplikacije (recimo, zaštitu od prekoračenja bafera), primenu specifičnih protokola(na primer, kriptografski zaštićenog protokola SSH umesto nezaštićenog protokola Telnet).
2. ***Zaštita na nivou operativnog sistema -*** obuhvata i vezu operativni sistem-aplikacije, kao i odnos prema mrežnoj arhitekturi tj. vezama sa drugim sistemima.
3. ***Zaštita na nivou mrežne infrastukture -*** misli se na sledeće osnovne elemente: pimenu mrežnih barijera (*firewalls*), blokiranje nepotrebnih portova, šifrovanje putanje, izolovanje putanje pomoću rutera i komutatora ili pomoću posebne infrastrukture.
4. ***Proceduralna i operativna zaštita –*** odnosi se na definisanje i sprovođenje pravila zaštite, politike i procedure, detekciju napada, proaktivno delovanje.

5 – Metode zaštite

1. **Procena** (*assessment*) - priprema za ostale tri komponente. Smatra se posebnom akcijom, zato što je u vezi s pravilima, procedurama, pravnom i drugom regulativom, određivanjem budeta i drugim upravljačkim dužnostima, i još je povezana s tehničkom procenom stanja sigurnosti. Greška u proceni bilo kog od ovih elemenata, može naškoditi svim operacijama koje slede.
2. **Zaštita** (*protection*) - podrazumeva primenu protivmera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primenjuje se sledeći korak – otkrivanje.
3. **Otkrivanje** (*detection*) - predstavlja proces identifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost. Neki autori definišu incident kao svaki nezakonit, neovlašćen ili neprihvatljiv postupak koji je preduzet, a odnosi se na računarski sistem
4. **Odgovor** (*response*)-predstavlja proces oporavka, tj. lećenja posledica upada. U aktivnosti reakcije spadaju postupci "zakrpi i nastavi", ili "goni i sudi". Ranije se na prvo mesto stavljalo oporavljanje funkcionalnosti oštećenih resursa, kao što je korišćenje rezervnih kopija podataka

Hvala na pažnji !!!

Pitanja

? ? ?