BEZBEDNOST RAČUNARSKIH MREŽA

BEZBEDNOST RAČUNARSKIH MREŽA

- U procesu razvoja informatičkih tehnologija, organizacije širom sveta se suočavaju sa sve sofisticiranijim sajber pretnjama, a istovremeno i sa nemogućnošću da pronađu ravnotežu između optimalne primene bezbednosnih mera i otvorene komunikacije unutar sistema koja omogućava nesmetano donošenje odluka .
- Bezbednost računarskih mreža podrazumeva aktivnosti zaštite mrežne infrastrukture, kako od eksternih napada putem interneta, tako i internih u okviru lokalne mreže.

BEZBEDNOST RAČUNARSKIH MREŽA

- Pristup umreženim sistemima ima mnoge prednosti za računarske siseme ali pored toga omogućava i da druge osobe imaju pristup našem računaru.
- Na taj način potencijalne opasnosti postaju sve brojnije.
- Enkripcija je matematički proces kodiranja i dekodiranja informacija.
- Za mnoge korisnike je bežični LAN idealno rešenje zbog dometa, brzine prenosa i različitih mogućnosti povezivanja.

BEZBEDNOST RAČUNARSKIH MREŽA

- Osobine bezbedne komunikacije
- Poverljivost
- Integritet poruke
- Provera autentičnosti krajnjih tačaka
- Operaciona bezbednost.

BEZBEDNOST RAČUNARSKIH MREŽA

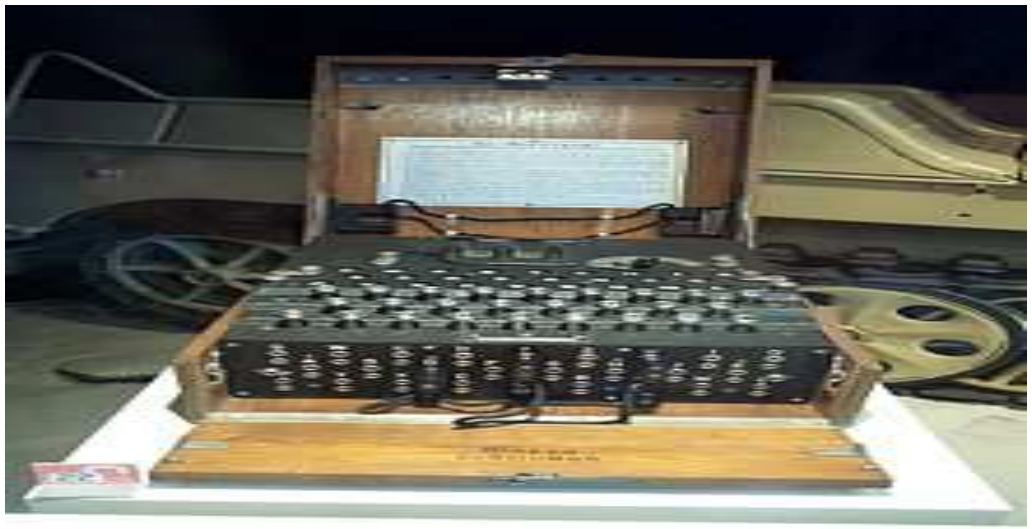
- **Kriptografija** je nauka koja se bavi metodima očuvanja tajnosti informacija. Od samog početka, enkripcija podataka koristila se prvenstveno u vojne svrhe. Jedan od prvih velikih vojskovođa koji je koristio šifrovane poruke bio je Julije Cezar. Iako kriptografija ima dugu istoriju koja datira još od Julija Cezara, savremene kriptografske tehnike, uključujuci i mnoge od onih koje se koriste na današnjem internetu, zasnovane su na dostignućima iz poslednjih 30 godina..

BEZBEDNOST RAČUNARSKIH MREŽA

- Prvu poznatu raspravu o kriptografiji napisao na 25 stranica italijanski arhitekta Leone Batista Alberti 1467. godine. On je takođe tvorac takozvanog šifarskog kruga i nekih drugih rešenja dvostrukog prikrivanja teksta koja su u XIX veku prihvatili i usavršavali nemački, engleski i francuski šifrantski biroi.
- Kriptografske tehnike dozvoljavaju pošiljaocu da maskira podatke tako da uljez ne može da dobije nikakvu informaciju iz presretnutih podataka. Primalac mora da bude u stanju da izvuče originalne podatke iz maskiranih podataka.

BEZBEDNOST RAČUNARSKIH MREŽA

- U II svetskom ratu pojavila se mašina koja je šifrovala poruke na do tada još neviđen način. Nemci su mašinu nazvali Enigma. Međutim ma koliko je ona u to vreme bila revoluciona saveznici su uspeli da razbiju poruke šifrovane Enigmom.



BEZBEDNOST RAČUNARSKIH MREŽA

- Posle Drugog svetskog rata i pojavom prvih računara otvorila su se nova vrata kriptografiji.
- Računari su vremenom postajali sve brži i brži, radeći i po nekoliko stotina, a kasnije i miliona operacija u sekundi. Novom brzinom rada je omogućeno probijanje šifri za sve manje vremena.
- Uporedo s tim, radilo se i na izmišljanju novih, sigurnijih i komplikovanijih algoritama za šifrovanje.

BEZBEDNOST RAČUNARSKIH MREŽA

- **Savremene tehnologije zaštite podataka**
- Sigurnosni protokoli bazirani na kriptografiji:
- SSL (Secure Socket Layer),
- IPSec (*Internet Protocol Security)*
- TLS (Transport Layer Security),
- VPN (Virtual Private Network),
- KERBEROS,
- SESAME,
- PGP (Pretty Good Privacy)
- Firewall uredjaji zadnje generacije

BEZBEDNOST RAČUNARSKIH MREŽA

- SSL sertifikat je digitalni sertifikat koji služi za uspostavljanje bezbedne, kriptovane, HTTPS komunikacije između servera i browsera. Zahtev za sertifikat (Certificate Signing Request - CSR) je kriptovani tekst koji se obično generiše na serveru na koji se planira instalacija SSL sertifikata.
- CSR sadrži podatke o sajtu i vlasniku sajta. U CSR se upisuje domen, odnosno common name (hostname), naziv firme koja je vlasnik sajta, grad i država. Taj deo je bitan za autentifikaciju, odnosno utvrđivanje identiteta.

BEZBEDNOST RAČUNARSKIH MREŽA

SSL

Kome treba SSL?

Svakome kome je potreban bezbedan prenos informacija preko interneta. Koristite SSL da zaštitite:

•Online transakcije kreditnim karticama, web forme i login podatke korisnika.

•Email i webmail aplikacije (Microsoft Outlook Web Access, Exchange i Office Communications Server).

•Korporativne komunikacije na intranetu, ekstranetu, internim mrežama, file sharing i Microsoft SharePoint.

•Komunikacije na cloud platformama i virtualizovanim aplikacijama

BEZBEDNOST RAČUNARSKIH MREŽA

IPSec

Internet Protocol Security

IPSec (engl. *Internet Protocol Security*) je proširenje IPv4 protokola koje obezbeđuje sigurnosne usluge privatnosti, integriteta, autentifikacije i neporecivosti. IP protokol obezbeđuje komunikacioni kanal sa kraja na kraj i nezavistan je od nižih slojeva, pa se i IPSec može koristiti bez obzira na način implementacije fizičkog sloja i sloja veze. Komunikacioni uređaji na putu između dva entiteta ne moraju podržavati IPSec.

BEZBEDNOST RAČUNARSKIH MREŽA

U novoj verziji IP protokola, IPv6, ispravljeni su nedostaci što se tiče sigurnosti, odnosno, IPSec je postao standardan integralni deo IPv6 skupa protokola.
IPSec implementira sigurnosne mehanizme mrežne komunikacije na mrežnom sloju OSI referentnog modela, odnosno na Internet sloju skupa protokola TCP/IP, pošto se integriše sa IP protokolom.

BEZBEDNOST RAČUNARSKIH MREŽA

TLS (Transport Layer Security),

Osnovni zadatak TLS protokola je obezbeđivanje privatnosti i integriteta podataka u okviru komunikacije između dve aplikacije. Sam TLS protokol sastoji se od dva sloja:

1. TLS Record protokola
2. TLS Handshake protola

Kao osnovni ciljevi pri dizajniranju ovog protokola postavljeni su:

- ✓ Bezbednost
- ✓ Interoperabilnost
- ✓ Proširivost
- ✓ Relativna efikasnost

BEZBEDNOST RAČUNARSKIH MREŽA

VPN

Virtual Private Network,

Virtuelna privatna mreža je privatna komunikaciona mreža koja se koristi za komunikaciju u okviru javne mreže. VPN mreža ili „privatna mreža“, kako je neki nazivaju, predstavlja jedno od rešenja kako da povećate ličnu sigurnost i anonimnost na internetu.

VPN mrežu možemo posmatrati kao jednu vrstu tunela koja se kreira u već postojećoj mreži, tj. virtuelno se kreira prostor koji je obložen kriptovanim zidovima.

Unutar tog tunela odvija se mrežni saobraćaj dok je pristup tom tunelu dozvoljen samo određenim osobama.

BEZBEDNOST RAČUNARSKIH MREŽA

Kerberos

Kerberos je autentifikacioni protokol razvijen u MIT-u (*Massachusetts Institute of Technology*). Naziv je dobio po troglavom psu, čuvaru podzemnog sveta, iz Grčke mitologije. Ovaj protokol se temelji na simetričnom *Needham–Schroeder* protokolu

U njemu se koristi pouzdana treća strana - centar za distribuciju ključeva (Key Distribution Center, KDC) - koji je logički podeljen na (Authentication Server, AS) i (Ticket Granting Server, TGS).

Ulogu KDC servera može obavljati više servera kako bi se izbegao prestanak rada usled otkaza glavnog (*master*) računara

BEZBEDNOST RAČUNARSKIH MREŽA

Firewall

Firewall sistemi nove generacije (NGFW) nude veću funkcionalnost od tradicionalnih. Oni omogućavaju filtriranje korisničkog saobraćaja na nivou URL-a ili aplikacije, što otvara mogućnost blokiranja aplikacija koje spadaju u kategoriju potencijalno malicioznih, kakve su npr. Tor ili Torrent. Uz to, mnoga NGFW rešenja podržavaju i naprednu antimalver zaštitu, zaustavljajući distribuciju malicioznog fajla na nivou mreže. Neki pd preimera:

- ✓ Check Point je jedan od lidera u oblasti mrežnih firewall
- ✓ Cisco Firepower NGFW je prvi potpuno integrisani firewall naredne generacije fokusiran na pretnje.

BEZBEDNOST RAČUNARSKIH MREŽA

Ako se govori o poslovnim informacionim sistemima može se reci da su računarske konfiguracije su veoma različite,te se u jednom poslovnom sistemu mogu koristiti:

1. Veliki računari za centralnu obradu ;
2. Manji računari za decentralizovano prikupljanje i obradu podataka ;
3. Personalni računari za automatizaciju kancelarijskog poslovanja

BEZBEDNOST RAČUNARSKIH MREŽA

Virus je program ili kod koji se sam replicira u drugim datotekama s kojima dolazi u kontakt.
Računarski virus se obično sastoji od dva dela.

- ✓ Samokopirajući kod koji omogućava razmnožavanje virusa
- ✓ Korisna informacija koja može biti bezopasna ili opasna

NekevVrste računarskih virusa

- ✓ boot sektor virusi – napadaju Master boot sektor
- ✓ zaraze izvršne datoteke dodavanjem svog sadržaja u strukturu programa
- ✓ svestrani virusi – napadaju boot sektore i izvršne programe

virusi pratioci – stvori .com datoteku koristeći ime već postojećeg .exe programa i ugradi u nju svoj kod

BEZBEDNOST RAČUNARSKIH MREŽA

Neke Vrste računarskih virusa

- ✓ link virusi
- ✓ makro virusi – imaju mogućnost da sami sebe kopiraju, brišu i menjaju dokumente
- ✓ Exe-virus

Spyware je široka kategorija malicioznog software-a sa namenom da presretne ili preuzme delimično kontrolu rada na računaru bez znanja ili dozvole korisnika

CRVI

Računalni crvi su računalni programi koji umnožavaju sami sebe

Crv –može oštetiti podatke

Mailer i mass-mailer – sami se šalju e-mailom

Kombinacija karakteristike, spywara, virusa, crva i trojanskih konja

BEZBEDNOST RAČUNARSKIH MREŽA

HAKERI

Prvobitna definicija hakera kaže da je haker entuzijasta za računare, bilo da je u pitanju programiranje ili interes za način njegovog funkcionisanja (hardver).

Danas hakerima smatramo osobe koje pokušavaju da pristupe tuđem računaru bez dozvole (s nečasnim namerama) ili osobe koje se protiv njih bore. Međutim, postoji daleko širi spektar motiva koji pokreću hakere.

Neki hakeri prave različite alate i aplikacije za bezbednost korisnika na internetu, dok drugi neumorno traže i prijavljuju otkrivene ranjivosti i malver. U početku su većinu hakera pokretali radoznalost i potreba za učenjem i izazovima. Uglavnom nisu postojale maliciozne namere

BEZBEDNOST RAČUNARSKIH MREŽA

Script Kiddies (Skids) su hakeri sa niskim nivoom poznavanja materije. Najčešće koriste kod koji je napisao neko drugi i preferiraju alate koji se lako koriste. Uglavnom se zadržavaju na tehnikama kao što je doxing i izvođenje DDoS napada.

Green Hat hakeri su takođe početnici, ali za razliku od Skidsa, imaju ambicije da prošire svoja znanja i veštine. Radoznalost ih motiviše da provode sate i sate učeći, vežbajući i unapređujući svoje veštine.

Blue Hat hakeri su osvetoljubivi skids hakeri kojima je cilj da se osvete svojim neprijateljima.

(Black Hat) U pitanju su hakeri čiji su motivi finansijske prirode.

BEZBEDNOST RAČUNARSKIH MREŽA

White Hat

Svoje veštine koriste da pomognu pojedincima, kompanijama i državnim organima. Između ostalog, oni se bore protiv malicioznih hakera, otkrivaju ranjivosti kojima je potrebna zakrpa, otkrivaju novi malver, pomažu da se zaštite računarske mreže, edukuju korisnike o bezbednosti na internetu itd.

Gray Hat

Nisu nužno ni dobri ni loši, niti su motivisani zaradom.

Haktivisti

U pitanju su hakeri koji se zalažu za određeno pitanje, ideju, cilj. Njih motiviše potreba da isprave ono što smatraju da je pogrešno.

BEZBEDNOST RAČUNARSKIH MREŽA

DOXING

Reč "doxing" ili "doxxing" je nastao iz "dokumenata" ili "odbacivanja dokumenata", koji su krajem vremena skratili na "dox". Doxing se odnosi na praksu pretraživanja, deljenja i objavljivanja ličnih podataka ljudi na Vebu na veb lokaciji, forumu ili drugim javno dostupnim mestima. Ovo bi moglo uključivati puna imena, kućne adrese, radne adrese, telefonske brojeve (i lične i profesionalne), slike, rođake, korisnička imena, sve što su objavili na mreži (čak i stvari koje su nekada bile smatrane privatnim) itd.

BEZBEDNOST RAČUNARSKIH MREŽA

Sposobnost da bude potpuno anoniman na mreži je jedna od ključnih prednosti Interneta, ali ova korist može biti iskorišćena od strane drugih ljudi, posebno pošto postoji ogromna količina informacija koje su dostupne besplatno svima koji imaju vremena, motivacije i interesa da sastave tragove i oduzmu tu anonimnost. Pored imena, adrese i brojeva telefona, pokušaji doxinga mogu takođe otkriti detalje mreže, informacije o e-pošti , organizacione strukture i druge skrivene podatke - bilo šta od neugodnih fotografija do .....

BEZBEDNOST RAČUNARSKIH MREŽA

DOS (Denial of Service Attack)

DDoS (Distributed Denial of Service)

DOS (Denial of Service Attack) ima vrlo jednostavan cilj – sprečavanje da bilo ko priđe odgovarajućem resursu (bilo da je u pitanju web sajt ili drugi servis koji postoji na serveru), a taj cilj se ostvaruje slanjem ogromne količine zahteva ka serveru ili nekom resursu koja je veća od raspoložive moći za procesiranjem tih zahteva.

DDoS napad (Distributed Denial of Service) je samo napredniji tip DOS napada u kojem saobraćaj stiže sa mnogo različitih lokacija u svetu, što značajno može da otežа odbranu celog sistema

BEZBEDNOST RAČUNARSKIH MREŽA

DDoS

Distributed Denial of Service

DDoS napadi se prvi put pojavljuju početkom ovog veka, iz godine u godinu sve ih je više, sve su obimniji i intenzivniji. Teško ih je sprečiti, preživeli su test vremena, jeftino se mogu iznajmiti i mogu imati dugoročne i razorne posledice.
Moderni DDoS napadi generišu ogromne količine saobraćaja pomoću botova (botnet). Botovi predstavljaju mrežu računara koji su zaraženi malicioznim softverom zbog čega haker ima kontrolu nad njima sa udaljene lokacije.
Postoji veliki broj tehnika koje se mogu koristiti prilikom DDoS napada.
alati poput MyDoom i Slowloris su često prikačeni uz malware koji se distribuira po računarima korisnika

BEZBEDNOST RAČUNARSKIH MREŽA

Fišing (phishing)

Fišing (phishing) je vrsta napada na internetu kada se napadači kori-ste postojećim internet servisima da namame i prevare korisnike da otkri-ju osetljive informacije (korisnička imena, lozinke, podatke sa kreditnih kartica...) koje mogu biti iskorišćene u kriminalne svrhe.

Napadači (fišeri) obično izvršavaju fišing napade koristeći falsifikova-ne e-mejlove tako da izgleda da ih šalje određena institucija sa kojom žr-tva ima kontakt (npr. banka, osiguravajuća kuća i slično).

Pored elektronske pošte, fišeri koriste i druge servise na internetu kao što su razni Messenger, Skype, Google Talk, društvene mreže (Facebook, Twitter, Instragam, ...)

BEZBEDNOST RAČUNARSKIH MREŽA

Botovi -bots

Botovi (engl.bots, skraćenica od robots) su programi (obično izvršni fajlovi) koji su instalirani na računar s ciljem da automatski pokrenu set funkcija i dopuste neovlašćenim korisnicima da dobiju daljinsku kontrolu pomoću komunikacionog kanala.

Ti zaraženi računari se nazivaju zombiji (zombies) ili botovi (bots), a mogu se nalaziti svuda širom sveta

Botnetovi su koordinirane grupe od nekoliko (desetina, stotina ili hiljada) personalnih računara ili čak novih smar telefona pri čemu su svi zaraženi istim malicioznim programom.

BEZBEDNOST RAČUNARSKIH MREŽA

Spem (spam)

Spem (spam) je neželjena elektronska pošta, odnosno pošta koju korisnik nije tražio niti je dao saglasnost pošiljaocu da šalje takve poruke na njegovu adresu. Najčešće su to reklamne poruke ili ponude, ali mogu biti i poruke s ciljem ubacivanja malicioznog softvera u željeni računar. To je oblik elektronske pošte koji pokušava da sakrije e-mail adresu pošiljaoca s ciljem onemogućavanja njegovog praćenja ili koji se koristi obmanjivanjem prilikom ispisa u polje „predmet (subject)“, s namenom da natera primaoca da otvori primljenu poštu

BEZBEDNOST RAČUNARSKIH MREŽA

Spem (spam)

Tokom poslednje decenije, korišćenje i slanje spam poruka se raširilo. U početku, spam se slao direktno korisnicima kompjutera i bilo ga je lako blokirati, ali u godinama koje su usledile, brzo širenje interneta je omogućilo spamerima da jeftino i brzo šalju masovnu poštu, i to onda kada su otkrili da modemima individualnih korisnika može pristupiti bilo ko, sa bilo kog mesta u svetu, zbog toga što oni uopšte nisu bili zaštićeni. Drugim rečima, internet konekcije korisnika koji ništa ne sumnjaju mogu biti iskorišćene za spamovanje znatno većeg obima.

PREPORUKA:

Nikada ne objavljujte svoju privatnu adresu na mestima koja su svima dostupna.

- ✓ Greylisting metoda - Metoda "sive liste" (engl. graylisting) je zamišljena kao antispam metoda
- ✓ Bajesova tehnika filtriranja spama

BEZBEDNOST RAČUNARSKIH MREŽA

Bezicni uredjaji

Da bi klijent, dobio pristup mreži, mora prvo proći proces autentifikacije.

Autentifikacija otvorenog sistema

Autentifikacija zasnovana na deljenoj tajni (Shared Key Authentication)

WEP (Wired Equivalent Privacy) je definisan u standardu 802.11

- ✓ Integritet poruka
- ✓ Šifrovanje
- ✓ Sigurnosni propusti u WEP standardu

Napad obrtanjem bitova

BEZBEDNOST RAČUNARSKIH MREŽA

Bezicni uredjaji

Svi kriptografski protokoli bežičnih uređaja u osnovi koriste RC4 kriptografski algoritam. RC4 je šifra koja pripada grupi sekvencijalnih šifara. Sam algoritam je zasnovan na promenljivim tabelama ili samo modifikujućim tabelama.

- ✓ Wired EquivalentPrivacy (WEP) je algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža .
- ✓ WPA2 protokol (engl. *Wi-FiProtected Access*) je protokol za sigurnu komunikaciju IEEE
- ✓ TKIP protokol radi sa postojećim hardverom koji podržava RC4. Rešava sve sigurnosne probleme sa WEP protokolom, tako što povećava inicijalni vektor na 48 bita da bi se izbeglo ponavljanje istog inicijalnog vektora.
- ✓ EAP (eng. *Extensible Aithentication Protocol*), proširiv protokol za autentivikaciju,

BEZBEDNOST RAČUNARSKIH MREŽA

Sigurnost e-commerce sistema

- Autentifikacija korisnika
- Autorizacija
- Zaštita tajnosti
- Infrastruktura javnih ključeva
- Sertifikati

BEZBEDNOST RAČUNARSKIH MREŽA

- **Digitalni potpisi**
- Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da obezbedi garantovanje identiteta pošiljaoca poruke. Pomoću svog potpisa korisnik ovlašćuje neku radnju i preuzima odgovornost za nju.
- Digitalni potpis je digitalna verzija ručnog potpisa (ne skenirana) i uz odgovarajuće zakone dokument sa digitalnim potpisom, prenesen preko Interneta je jednako validan kao i dokument ručno potpisan. Sama metoda autentifikacije se zasniva na asinhronom (de)šifrovanju podataka **javnim ključem** i **tajnim ključem**.

BEZBEDNOST RAČUNARSKIH MREŽA

ANTIVIRUSNI PROGRAMI

Postoji širok izbor antivirusni programa koje možete da izaberete. Dosta njih dolazi sa besplatnom uslugom a mnogi se i plaćaju i dolaze sa neverovatnim alatkama.

Antivirus program ili antivirus je računarski program koji se koristi za zaštitu, identifikaciju i uklanjanje računarskih virusa i ostalih malicioznih softvera (малware), koji mogu da oštete računarski sistem.

Kad je prvi put napravljen anti virus program?

Prvi virus koji je zarazio PC računar, otkriven je 1986. godine.
Prvo uklanjanje jednog računarskog virusa izvršeno je 1987. godine Bernt Fiks, a radilo se o jednom od prvih virusa— pod imenom Viena.

BEZBEDNOST RAČUNARSKIH MREŽA

ANTIVIRUSNI PROGRAMI

Šta je bitno kod izbora antivirus programa?

- ✓ · Nivo zaštite
- ✓ · Efikasnost (efikasan i brz rada ovog softvera)
- ✓ · Lakoća instalacije i podešavanja (laka i jednostavna)
- ✓ · Jednostavnost (jednostavni za upotrebu i ne iziskuje konstantno odrzavanje)
- ✓ · Ažuriranje antivirusa (mogućnost automatskog ažuriranja)
- ✓ · Podrška (preko interneta ili telefona)

BEZBEDNOST RAČUNARSKIH MREŽA

ANTIVIRUSNI PROGRAMI

U nastavku su dati nazivih nekih antivirusnih programa koji se koriste

- ✓ **Avast**
- ✓ **MC AFEE**
- ✓ **NORTON ANTIVIRUS**
- ✓ **AVG Anti-virus**
- ✓ **Avira AntiVir Personal Edition**
- ✓ **Panda Cloud Antivirus**
- ✓ **Bitdefender Free Edition**
- ✓ **Kaspersky**
- ✓ **NOD32**
- ✓ **Trend Micro HouseCall**
- ✓ **BitDefender Online Scanner**
- ✓ **ESET Online Scanner, ...**

BEZBEDNOST RAČUNARSKIH MREŽA

ANTIVIRUSNI PROGRAMI

1. Obavezno instalirati neki od antivirusnih alata!
2. Redovno ažurirati antivirusne programe
3. Podesiti antivirusni softver da automatski skenira sve datoteke.
4. Skenirati sve datoteke koje dolaze sa Interneta
5. Povremeno skenirati ceo hard disk.
6. Skenirati hard disk nakon instalacije softvera
7. **Skenirati USB**

BEZBEDNOST RAČUNARSKIH MREŽA

ANTIVIRUSNI PROGRAMI

- ✓ **Administracija same računarske mreže (prava i privilegije korišćenja)**
- ✓ **Sigurnost baza podataka**
- ✓ **Sistemske privilegije**
- ✓ **Korišćenje rola**
- ✓ **Virtual Private Databases**

BEZBEDNOST RAČUNARSKIH MREŽA

Treba imati u vidu činjenicu da je nemoguće ostvariti apsolutnu zaštitu.

Postoje i problemi u sigurnosnim aspektima programiranja, gde greške programera dovode do toga da je programaski kod bude nesiguran i otvara aspekte problema sigurnosti računarskih mrežnih sistema.

Pored nužnosti poznavanja pretnji na internetu nužno je stalno razvijati nove mehanizme zaštite u skladu sa bezbednosnim problemima koji nastaju. Najslabija karika svakog računarskog sistema može da bude i ljudski faktor i njemu se mora posvetiti naročita pažnja.