Internetne tehnologije

Varnost omrežij

Žarko Čučej
e-naslov: zarko.cucej@uni-mb.si

Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko

Maribor 9. april 2009

Vsebina

1. **Uvod**
2. **Pomembnost varnosti**
3. **Napadi na varnost**
   - Neavtorizirani dostopi
   - Virusi, črvi in trojanski konji
   - Ponarejanje naslova IP
   - Zavračanje storitev
4. **Varnostna politika**
   - Večnivojska obramba
   - Varnostna orodja
5. **Zaključek**
   - Vprašanja
   - Slovarček
   - Literatura

Zakaj je pomembna varnost Interneta?

Internet se je iz preprostega sistema za prenos datotek razvil v sofisticirani sistem, ki ga uporabljamo na primer pri nakupih avtomobilov, izpolnjevanju receptov, vlogah za bančna posojila, plačilo računov itd, na kratko, postaja ena najpomembnejših infrastruktur tudi za poslovanje.

Podjetja so kmalu spoznala, da za poslovanje preko Interneta morajo zagotoviti varnost svojega omrežja in varnost komunikacije preko Interneta, da jim bodo stranke zaupale.

Tudi vlade so kmalu spoznale, da morajo svojim državljanom zagotoviti zasebnost tudi pri uporabi sodobnih informacijsko komunikacijskih tehnologij, predvsem pri uporabi njihovih osebnih podatkov, s katerimi razpolagajo in jih uporabljajo institucije kot so banke, bolnice, zavarovalnice itd.

Uporabljane kratice

APP	Allowed Public Policy
AUP	Acceptable Use Policy
DNS	Domain Name Server
DoS	Denial of Service
ECP	Extranet Connection Policy
EIP	E-mail and Internet Policy
EU	Europe Union
FTP	File Transport Protocol
HIPPA	Health Information Privacy Protection Act
HTTP	Hyper Text Transport Protocol

Uporabljane kratice (2)

ICMP	Internet Command Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	IP Security
MIB	Management Information Base
RAP	Remote-user Access Policy
RFC	Request For Comments
SNMP	Simple Network Management Protocol
TCP	Transport Control Protocol
UDP	User Defined Protocol

Zakaj je pomembna varnost omrežij?

- Varnost omrežij je nesporno odvisna od:
  - nagle rasti uporabe Interneta v poslovne namene
  - vse večje dostopnosti in zmogljivosti Interneta
  - zakonodaje
- Vse več podjetij posluje preko Interneta, zato zahtevajo jamstva za zasebnost strank in varnost svojih podatkov.
- Vse večje zmogljivost Interneta vzpodbuja nove oblike dela, na primer daljinsko delo od doma.

> omrežja podjetij se širijo izven “tovarniškega dvorišča”

- Vlade so kmalu spoznale, da je za poslovno rabo kot tudi za državno infrastrukturo nujna varnost Interneta in varnost informacijskih sistemov dosegljivih preko Interneta:
  - Health Information Privacy Protection Act (HIPPA),
  - EU Directive on Data Protection

Napadi na varnost

- Z evolucijo računalniških omrežij v novo tehnološko osnovo vsakodnevnega življenja so se ta izpostavila vsakodnevnim grožnjam in napadom.
- Napadi se pojavljajo različnih oblikah in izkoriščajo različne slabosti omrežja
- Vsak dan se odkrivajo nove slabosti in nove vrste napadov.
- V splošnem napade lahko delimo na:
  - neavtorizirani dostopi ki nastajajo zaradi nedovoljene uporabe omrežij, šibke avtentikacije in šibkih gesel
  - viruse, črve in trojanske konje
  - sleparjenje
  - zavračanje dostopa

Neavtorizirani dostopi

Nedovoljena uporaba

Pogosti primer nedovoljene uporabe omrežja je igranje omrežnih igric na omrežju podjetja. Mnogo nevarnejša pa so tekmovanja hekerjev (hackers) v vdiranju v tuje računalnike ali informacijske sisteme s ali brez pridobitniških ciljev.

Šibka avtentikacija:

O njej govorimo, ko sistemi ne zahtevajo identifikacije uporabnikov ali katerekoli entitete oziroma avtentikacijski mehanizem ne zagotavlja nobenega varnostnega učinka.

Opozorilo: Mnogo sistemov ima vgrajene stroge sisteme avtentikacije, vendar se ti (iz razno raznih razlogov . . .) ne uporabljajo

Neavtorizirani dostopi (2)

Gesla:

Običajno so prva obrambna linija pred napadi. Uporabljajo se za avtentikacijo in avtorizacijo uporabnikov. zato je pomembno, da gesla ni možno enostavno odkriti.

Pri pošiljanju gesel se uporablja enkripcijske algoritme. Tudi tako zaščitena gesla, če so gesla šibka, se da enostavno zlomiti s posebnimi orodji (password cracking tools). Orodja za lomljenje gesel delujejo na dva načina:

- z golo silo,
  kjer se preverja vse možne kombinacije črk, številk in specialnih znakov, dokler rezultat ni enak kot je v hašeju gesla
- s slovarjem,
  kjer se preverja seznam verjetnih gesel

Neavtorizirani dostopi (3)

Vohljači (sniffers):

To so programi, v žargonu jih imenujemo sniferji, ki pregledujejo vsebine paketov, ki potujejo po prenosnem mediju, na katerega so priključeni gostitelji sniferjev.

Drugače se porabljajo jih pri analizi prometa, hekerji pa z njimi skušajo iz paketov izvleči občutljive informacije, kot so gesla, s katerimi kasneje uporabljajo za nedovoljen dostop do informacijskih virov. Sniferji običajno lovijo pakete, ki so povezani s protokoli in aplikacijami, ki za uporabo zahtevajo geslo (na primer Telnet, HTTP, POP itd).

Aplikacijska plast:

Napadi na aplikacijski plasti skušajo zasesti zmogljivosti napadenega sistema s praznim delom. Za to izkoriščajo slabosti namestitve aplikacijskih programov, ki jim je skupna slabost prekoračitev vmesnega pomnilnika.

Virusi, črvi in trojanski konji

Virusi:

Virusi so skriti računalniški programi z zlobnimi nameni. Običajno se širijo z vstavljanjem svoje kopije v druge programe.

Njihova običajna pot širjenja so priponke k elektronski pošti, na primer slike, dokumenti iz obdelave tekstov, in razpredelnice. Virusi, vgrajeni v te priponke, okužijo sistem, ko uporabnik aktivira priponke.

Primeri virusov so Melissa, BugBear in Klez.

Črvi:

Črvi so neodvisno delujoči računalniški programi, ki se lahko samostojno širijo po omrežju. Destruktivno zasedajo gostiteljeve procesne zmogljivosti.

Mnogi menijo, da so črvi podzvrst virusov. Ponudniki protivirusnih programov vključujejo črve v svoje podatkovne baze.

Primeri črvov so Nimda, CodeRed, Slapper in Slammer.

Virusi, črvi in trojanski konji (2)

Trojanski konji:

Trojanski konji so navidezno koristni računalniški programi, v resnici pa vsebujejo skrite zlonamerne funkcije, ki ogrožajo varnostne mehanizme. Pri tem izkoriščajo avtentikacije sistemske entitete, ki oživi ta program.

Sleparjenje: ponarejanje naslovov IP

- Napade s ponarejanjem naslova IP izvajajo hekerji
- Hekerji se lahko nahajajo v omrežju, katerega napadajo, običajno pa imajo le zunanji dostop do omrežja
- S ponarejanjem naslova IP želijo prevzeti identiteto zaupanja vrednega računalnika.
- Napad se lahko izvede na dva načina:
  - z uporabo naslova IP ki je znotraj območja naslovov, ki jim zaupamo
  - z uporabo IP naslova izven območja naslovov omrežja, ki pa so avtorizirani, da jih lahko uporabljajo določeni resursi v omrežju

Pozor! Napad s ponarejanjem naslova IP je običajno začetek drugih napadov na omrežje oziroma informacijske vire na njem.

Zavračanje storitev

- Napad z zavračanjem storitev (DoS) je med najbolj zastrašujočimi napadi saj povzročijo zastoj sistemov in s tem izgubo zaslužka.
- Cilj napada DoS je prekiniti ali omejiti legitimnega uporabnika pri dostopu do njegovih resursov.
- Preprosta oblika napada DoS je množičen napad na izbrani vir z gesli, ki blokira dostop uporabniku. To se zlahka naredi pri enem gostitelju napada. Napadi DoS se običajno naredijo iz ponarejenega naslova IP
- Bolj zahrbtna oblika DoS je napad iz množice gostiteljev, ki jih koordinira gospodar. Ta napad omogoča pošiljanje mnogo večjega števila paketov.

Varnostna politika

Varnostna politika:

Z varnostno politiko podjetja ali ustanove določajo cilje in sredstva pri varovanju svojih omrežij. Običajno se sestoji iz:

- **pravilnika za dodeljevanje uporabnih dovoljenj**
- **pravilnika za gesla**
- **pravilnika za uporabo elektronske pošte in Interneta**
- **pravilnika ukrepov in procedur odzivov ob incidentih**
- **pravilnika o izvedbi daljinskega dostopa**
- **pravilnika o priključevanju tujih omrežij**
- **pravilnika o dodeljevanja javnega dostopa**

Varnostna politika (2)

pravilnik za dodeljevanje uporabnih dovoljenj (AUP)

AUP (Acceptable Use Policy) določa, kaj je uporabniku dovoljeno početi na omrežju. Določa kateri uporabnik lahko ali ne sme do omrežja. Prav tako določa odgovornost avtoriziranega uporabnika. Na primer AUP lahko določa, da mora uporabnik zagotoviti, da bo anti virusni program pregledal njegov vir enkrat na dan.

pravilnik za gesla

Pravilnik določa, kako izbrati varno geslo, kako pogosto se morajo gesla spremeniti, kako gesla shraniti in kdo ima dostop do gesel. Na primer gesla usmerjevalnikov morajo imeti vsaj 10 znakov, menjavati se morajo vsakih 60 dni ali takoj, ko administrator zapusti podjetje/ustanovo.

Varnostna politika (3)

pravilnik za uporabo elektronske pošte in Interneta (EIP)

EIP (E-mail and Internet Policy) določa, kateri uporabnik imajo dostop elektronske pošte in Interneta. Na primer, IEP določa, da se lahko elektronska pošta uporablja le za poslovne namene, Interneta pa le za dostop do domačih strani, za katere se oceni, da so pomembne za delo uporabnika.

pravilnik ukrepov in procedur odzivov ob incidentih

Pravilnik določa, kako osebje, ki skrbi za varnost omrežja, ukrepa ob varnostnih incidentih, kot so izbruh virusov ali poskusov vdora. Pri odzivih na vdore pa določa kako in koga obvestiti o odkritem vdoru.

Varnostna politika (4)

pravilnik o izvedbi daljinskega dostopa (RAP)

RAP (Remote user Access Policy) določa postopek dostopa do omrežja podjetja iz tujih, javnih omrežij. Na primer, za dostop od doma moramo uporabiti navidezno zasebno omrežje in enkratno geslo.

pravilnik o priključevanju tujih omrežij (ECP)

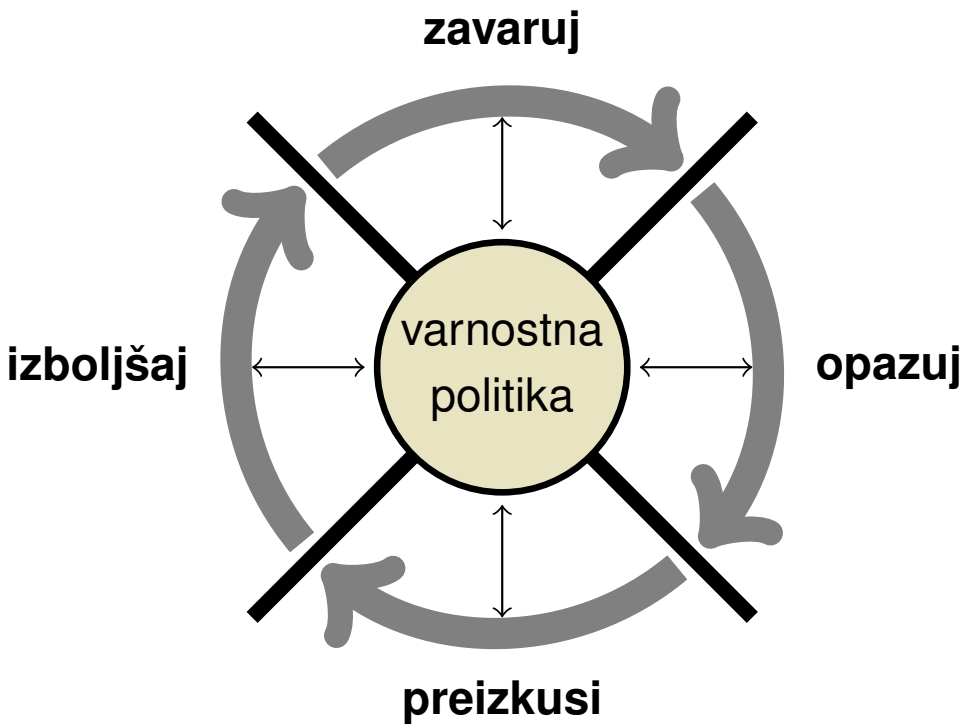
ECP (Extranet Connection Policy) določa pravila kako se lahko poslovni partner poveže na omrežje podjetja. Na primer, partner se lahko poveže le z domačo stranjo podjetja in to preko tunela VPN.

pravilnik o dodeljevanja javnega dostopa (APP)

APP (Allowed Public service Policy) določa katere storitve omrežja so na voljo Internetu. Na primer, FTP, SMTP, HTTP in DNS. APP lahko določi, da ima DNS dostop le do korena strežnika DNS.

Varnostni cikli

- varnost je ciklični proces (slika 2), ki ga je potrebno neprestano izboljševati:



Slika: Kolo varnosti.

Varnostni cikli (2)

korak 1 Zavaruj omrežje skladno z varnostnim pravilnikom. Na primer, dostop do vseh usmerjevalnikov in stikal v omrežju naj bo mogoč le z avtentikacijo.

korak 2 Opazuj omrežje. Na primer s programom, ki detektira vdor (Intrusion Detection System: IDS), opazuj promet skozi požarni zid.

korak 3 Preizkusi varnost. Periodično preveri varnost omrežja in odkrivaj ranljivost. Ta postopek običajno zahteva najem zunanjih svetovalcev, ki s pregledovalniki ranljivosti iščejo ranljivost omrežja in ugotavljajo učinkovitost uvedenih varnostnih ukrepov. Popularni pregledovalnik je Nmap (network mapper).

korak 4 Izboljšaj varnost. Na osnovi ugotovitev iz testiranja izboljšaj varnostne ukrepe. Na primer, če se v koraku preizkušanja odkrije, da je ranljiv program web strežnika, tega dogradi s popravki kot priporoča prodajalec programa.

Večnivojska obramba

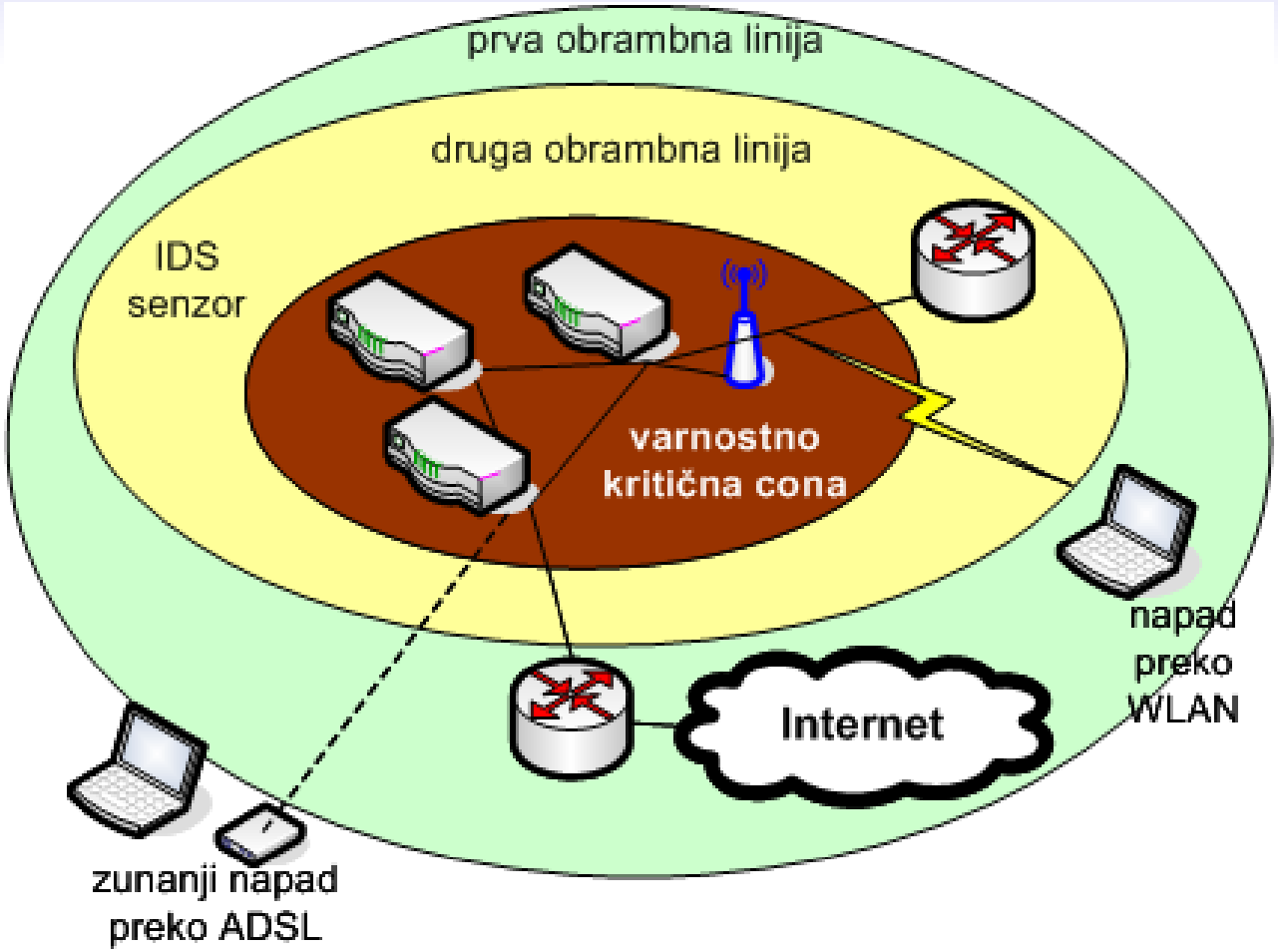
- sodobni varnostni sistemi so večnivojski obrambni sistemi
- pri njej omrežje razdelimo na več koncentrično nameščenih con tako, da središčna cona zajema varnostno najbolj kritične resurse omrežja
- varnostni ukrepi v vsaki coni dopolnjujejo predhodne zunanje varnostne cone (slika 2), na primer:

  prva obrambna linija:
  : usmerjevalniki s filtrskimi požarnimi zidovi

  druga obrambna linija:
  : specializirani požarni zidovi in senzorji vdora

  tretja obrambna linija:
  : senzorji vdora

Večnivojska obramba (2)



Slika: Varnostne cone v večnivojskem varovanju omrežja.

Zmanjševanje nevarnosti napadov

- vseh napadov na varnost omrežja in v njem prisotnih virov informacij ne moremo odstraniti
- kot sestavni del varnostne politike izdelamo oceno tveganja in škode, ki lahko nastane, za vsak element omrežja:

Tabela: Primer tabele z oceno tveganja. K: kritično, slabosti moramo odpraviti takoj, R: rizično, slabosti moramo odpraviti v določenem roku, MR: manj rizično

↓ škoda \ verjetnost napada →	1	2	3	4	5
1	MR	MR	MR	MR	R
2	MR	MR	R	R	R
3	MR	R	R	R	K
4	MR	R	R	K	K
5	R	R	M	K	K

algoritem:

$$x = \left[\text{škoda}\right] \times \left[\begin{matrix}\text{verjetnost}\\ \text{napada}\end{matrix}\right]$$

$$x = MR \quad x < 5$$
$$x = R \quad 5 < x < 15$$
$$x = K \quad x > 15$$

Zmanjševanje nevarnosti napadov (2)

- priporočene metode zmanjševanja uspešnosti napadov:

neavtorizirani dostop:

Nevarnost zmanjšamo z nadzorom dostopa. Določimo, kateri promet lahko vstopa v varovano omrežje in kateri ima dovoljenje za izhod iz omrežja.

šibka avtentikacija:

Moč avtentikacije lahko povečamo z uporabo gesel na vsaki napravi v omrežju. V omrežjih, kjer se zahteva stroga avtentikacija, uporabimo avtentikacijske postopke kot so enkratna gesla ali bio-metrične metode.

šibka gesla:

Moč gesel lahko povečamo s sistemom, ki na primer od uporabnikov zahteva gesla s 7 – 14 znaki in z veljavnostjo le treh mesecev, da gesla ne sestavljajo iz znanih besed ali ponovno uporabljajo.

Zmanjševanje nevarnosti napadov (3)

“sniferji” paketov:

Vse tekstovne podatke se iz omrežja da enostavno dobiti s “sniferji”, to je programi, ki vohljajo za prometom na omrežju. Nevarnost napada z njimi lahko zmanjšamo z naslednjimi ukrepi:

- stroga avtentikacija: Z uporabo enkratnega gesla se izniči uporabnost zajetega gesla, saj veljale za eno uporabo
- stikala: Uporaba stikal namesto zvezdišč v omrežju omeji širjenje prometnih tokov po omrežju na direktne poti med uporabniki. S tem se zmanjša možnost vohljanja za vsemi paketi.
- kriptografija: V omrežjih, kjer se zahteva najmočnejša zaščita pred napadi, uporabimo kriptografijo, na primer z uporabo prenosa z IPsec (IP Security)

Zmanjševanje nevarnosti napadov (4)

napadi v aplikacijski plasti:

Napade na aplikacijski plast ni mogoče povsem odstraniti. Vsak dan se odkrivajo nove ranljive točke. V splošnem lahko z njimi povezane nevarnosti zmanjšamo z:

- s stalnim spremljanjem obvestil o varnostni problematiki programske opreme, ki se uporablja. Na primer z vključitvijo na poštni seznam foruma proizvajalca opreme o varnosti
- rednim dograjevanjem varnostnih popravkov v nameščeni programski opremi, na primer, SP2 in SP 3 pri operacijskih sistemih Windows XP
- uporabo detektorjev vdora (IDS) v omrežju in na računalnikih

Zmanjševanje nevarnosti napadov (5)

virusi, črvi in trojanski konji:

Pred to nadlogo in nevarnostjo se varujemo s protivirusnimi programi. Pri kritičnih aplikacijah namestimo tudi lokalne požarne zidove in detektorje vdorov.

zavajanje z naslovi IP:

Za zaščito pred sleparskimi naslovi RFC 2827 priporoča uporabo vhodnih in izhodnih filtrov. Pri njih dobro upoštevati tudi RFC 1918.

zavračanje dostopa:

Pri zmanjševanju nevarnosti zavračanja dostopa je poleg filtriranja naslovov dobro v dogovoru z Internetnim ponudnikom omejiti količino prometa. To omejitev namestimo tudi na robnem usmerjevalniku, preko katerega smo povezani na zunanje omrežje. Na izbrane gostitelje namestimo zaščitni program, ki omejuje število dovoljenih dostopov (programi anti-DoS).

Varnostna orodja

- Mnogo varnostnih problemov nastaja zato, ker se v omrežje brez dovoljenja vključujejo nove naprave ali storitve.
- Pri nadzoru varnosti si sistemski administratorji pomagajo z različnimi orodji, s katerimi ugotavljajo prisotnost naprav v omrežju, kateri servisi so na voljo, kje je sistem ranljiv itd.

pregledovalnik naprav (port-scanning tools):

- Program s pošiljanjem paketov ICMP z zahtevo odziva naprav – **ping sweeping** – v omrežje odkriva prisotne naprave.
- Odkritim napravam pošlje paket TCP z zahtevo za povezavo. Z njim določi, ali naprava nudi storitve TCP kot so HTTP, FTP in Telnet.
- Odkritim napravam še pošlje paket UDP, da ugotovi, ali naprava nudi storitve UDP kot so DNS in SNMP.

Varnostna orodja (2)

varnostni pregledovalnik (security scanner):

Pregledovalniki varnosti omrežja se uporabljajo za ugotavljanje, ali so storitve omrežja ranljive. Vsebujejo podatkovno bazo, v kateri so vpisane vse znane ranljive točke. Njihove podatke primerja s podatki v nadzorovanem omrežju:

- Preverja verzijo operacijskega sistema – **fingerprinting**.
- Preverja verzijo programske opreme.
- Simulira napade. Na primer, strežniku pošlje dolg URL in preveri, ali mu odgovori s specifičnim odzivom.

- Obstaja še mnogo drugih orodij, s katerimi si lahko pomagamo pri vzdrževanju varnosti v omrežju.

Varnostna orodja (3)

John the Ripper:

To je odprto kodni program za razbijanje gesel. Z njim lahko odkrivamo šibka gesla. Več informacij je na www.openwall.com/john/

Nmap:

To je odprto kodni program za raziskovanje omrežja in varnostno prisluškovanje. Deluje na večini vrst računalnikov. Zanj je na voljo grafični uporabniški vmesnik GTH+. Več informacij najdemo na www.insecure.org.

Nessus:

To je brezplačno orodje za varnostno prisluškovanje. Več informacij je na www.nessus.org.

Varnostna orodja (4)

SomarSoft:

To je zbirka brezplačnih programov za pomoč sistemskim administratorjem pri uvajanju varnosti pri Microsoft Windows okolji:

- DumpEvt omogoča varnostno prisluškovanje operacijskim sistemom Windows NT in Windows 2000
- DumpEvt je program za Windows NT, ki izpisuje EventLog v obliki, ki je primerna za vpis v podatkovne baze
- DumpReg je program za Windows NT in Windows 95, ki izpisuje vsebino registrov. Olajša iskanje ključev in nizov.

Več informacij je na `www.somarsoft.com`

Povzetek

Danes Internet ni več sistem za prenos elektronske pošte in datotek ampak iz dneva v dan postaja vse bolj pomembna poslovna infrastruktura. V tej vlogi je varnost ključnega pomena. Uporabniki pričakujemo, da bodo naši podatki, ki jih izmenjujemo v poslovnih ali drugih transakcijah po internetu ostali zaupni.

Omrežja so danes izpostavljena številnim napadom in poskusov zlorab. Med napadi so najbolj pogosti neavtorizirani dostop, šibka (z lahkoto premagljiva) avtentikacija, gesla, vohljači naslovov IP, napadi na aplikacijski plast, virusi, črvi, trojanski konji sleparije z IP naslovi in napad z zavračanjem storitev.

Varnostna politika je določena s pravilnikom, ki določa varnostna pravila uporabe Interneta. Ta pravila lahko zelo posežejo med ustaljene navade zaposlenih v podjetju.

Povzetek (2)

Zaščita z večnivojsko obrambo temelji na oblikovanju več koncentričnih con zaščite omrežja. V vsakem območju varnostni ukrepi dopolnjuje varnostne ukrepe predhodne zunanje cone.

Tehnike zmanjševanja nevarnosti so odvisne od izpostavljenosti napadom. Tako s pravili menjav in izbire gesla zmanjšujemo tveganje napada na gesla. Vhodno in izhodno filtriranje skladno z RFC 2827 zmanjša tveganje pri napadih s sleparskimi naslovi IP.

Administratorji omrežij lahko s stalno analizo dogajanj na omrežju mnogo prispevajo k varnosti omrežja. S programi za pregledovanje vrat (port scanners), ranljivosti (vulnerability scanners) in programi za odkrivanje gesel (password-cracking) lahko poiščejo varnostno šibke točke in z njihovo odpravo znatno izboljšajo varnost omrežja.

Vprašanja

1. Kateri faktorji vplivajo na pomembnost varnosti v omrežjih?
2. Kako varnostna politika vpliva na omrežja podjetij?
3. Navedite primer globoke obrambe pred napadi na omrežje!
4. Naštejte glavne vrste napadov na omrežje!
5. Kateri napad na omrežje skuša zasuti omrežje s poplavo neželenih paketov?
6. Katera vrsta napadov se vrši preko priponk k elektronski pošti?
7. Opišite kako ublažiti napad s sleparskim IP
8. Kako infrastruktura s stikali ublaži napad vohunjenja?
9. Katero varnostno orodje odkrije naprave in razpoložljive storitve na omrežju?
10. Katero orodje odkrije ranljivost omrežnih naprav?
11. Katero orodje odkriva šibkost gesel?

Slovar

avtentikacija (authentication) je proces, v katerem se potrjuje identiteta entitete.

detekcija vdora (intrusion detection) je varnostna storitev ki nadzira in analizira dogodke v sistemu s ciljem odkriti in v realnem času opozoriti na nedovoljen dostop do virov v sistemu.

enkratno geslo (one-time password: OTP) je preprosta avtentikacijska tehnika, v kateri se vsako geslo uporabi samo enkrat. Uporabna je

Internet Protocol Security (IPSec) je skupno ime za varnostno arhitekturo in zbirko protokolov, ki zagotavljajo varnost prometa na Internetu.

zahtevanje odzivov (ping sweep) je napad, v katerem se uporabi zahteva odziva (ping) pri protokolu ICMP pri množici IP naslovov s ciljem odkriti gostitelja, kateremu se lahko odkrije ranljivost

ranljivost (vulnerability) je razpoka ali šibka točka v načrtovanju sistema, njegovi izvedbi, delovanju ali upravljanju, ki se lahko izkoristi za nasilni vdor v varnostno politiko sistema.

Več informacij najdemo v . . .

- CERT: www.cert.org
- Cisco SAFE: www.cisco.com/go/safe
- Fact Sheet on EU Privacy Directive:
  www.dss.state.ct.us/digital/eupriv.html
- Helt Privacy Project:
  www.dss.state.ct.us/digital/eupriv.html
- RFC 1918 “Address Allocation for Prirvate Networks”
  www.ietf.org/rfc/rfc2118.txt
- RFC 2196 “Site Security Handbook”
  www.ietf.org/rfc/rfc2196.txt
- RFC 2827 “Netwotk Address Ingress Filtering”
  www.ietf.org/rfc/rfc2827.txt

Dodatno čtivo

- Dorothy E. Denning: **Information Warfare and security**, Addison-Wesley, 1999;
- Linda McCarthy: **Intranet Security: Stories from the Trenches**, Palo Alto, CA: SUN Microsystems Press, 1998;
- Marike Kaeo: **Designing Network Security**, Macmillan technical Publishing, 2000;
- William Stallings: **Data and Computer Comunications**. Fifth editions, Prentice Hall, 1997, ISBN 0-13-571274-2

Viri

- Cisco Systems, Inc: **Internetworking Technologies Handbook**. Fourth Edition, Cisco Systems™ 2004, ISBN 1-58705-119-2
- Boštjan Lavuger: **Nadzor komunikacijskih omrežij**. Poročilo o individualnem raziskovalnem delu, UM-FERI 2006