Internetne tehnologije

Nadzorovanje omrežij

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

Univerza v Mariboru
Fakulteta za elektrotehniko, računalništvo in informatiko
Inštitut za Telematiko

Maribor 9. april 2009

Vsebina

Povzetek

Že danes je življenjskega pomena nadzor in upravljanje komunikacijskih omrežij, tako pri privatnih kot javnih komunikacijskih omrežjih, s ciljem zagotoviti kakovost njihovih storitev. Med njimi postaja varnost osrednjega pomena.

V prihodnosti se pričakuje razslojevanje poslovnih uporabnikov komunikacij predvsem v smislu upravljanja in vzdrževanja omrežij. Le nekaj največjih korporacij in ustanov z najvišjimi zahtevami po varnosti in zanesljivosti bo ohranilo svoja omrežja. Ostala, predvsem mala in srednja podjetja, pa bodo najemala celovite storitve pri raznih ponudnikih komunikacijskih storitev.

Tako bomo imeli dve veliki družini komunikacijskih omrežij. Prva, v lasti velikih podjetij kot so bančni sistemi in druga podjetja ali ustanove z zelo občutljivimi podatki, bodo imela mnogo bolj specializirano varnostno politiko in upravljanje omrežij. Druga omrežja, v lasti raznih ponudnikov komunikacijskih storitev pa bodo razvijala splošno varnostno politiko in potrebe posameznih uporabnikov reševale skozi politiko sporazumov o nivoju storitev.

Uporabljane kratice

ISO	International Standard Organization
MIB	Management Information Base
NMS	Network Management System
OSI	Open System Interconnection
PDU	Protocol Data Unit
RMON	Remote Monitoring
RFC	Request For Comments
SLA	Service Leve Agreement
SMI	Structure Management Information
SNMP	Simple Network Management Protocol

Nadzor omrežij

- Obstaja več razlag, kaj je nadzor komunikacijskih omrežij:
  - spremljanje vseh aktivnosti, sprememb in stanj v nekem omrežju, ki ga izvajamo s pomočjo posebnih analitičnih orodij
  - avtomatski zajemom in obdelavo podatkov z namenom sprotnega izrisovanja topologije in prometa preko omrežja

ISO model nadzora komunikacijskih omrežij:

Nadzor komunikacijskega omrežja je storitev, ki zajema širok nabor orodij ter postopkov, ki nadzornemu osebju omogoča nadzor nad dogodki in stanji omrežja ter olajša vzdrževanje delovanja omrežja.

sodobni nadzor komunikacijskih omrežij:

Nadzor komunikacijskega omrežja je sestavni del poslovne politike lastnika in/ali ponudnika storitev omrežja, ki zajema tako organizacijske kot tehnične ukrepe zagotavljanja kakovosti storitev in varnosti.

Področja delovanja nadzornega sistema

- **Nadzor napak** (Fault management) zaznava, locira ter odpravlja napake v delovanju komunikacijskega omrežja.
- **Nadzor nastavitev** (Configuration management) nadzira nastavitev celotnega omrežja. Zajema nadzor nad nastavitvenimi datotekami, programsko in strojno opremo.
- **Nadzor zmogljivosti** (Performance management) meri in nadzoruje zmogljivosti omrežja v različnih pogledih (prenosne kapacitete, njihovo zasedenost, latenco, odzivne čase, . . .).
- **Nadzor varnostnih parametrov** (Security management) zagotavlja pooblaščencem zaščiten dostop do omrežnih virov, vrši centralno zbiranje in nadzor varnostno sumljivih dogodkov.
- **Nadzor uporabe omrežnih virov** (Accounting) zbira informacije o uporabi omrežnih virov.

Nadzor napak

Centralni nadzor napak:

Namen nadzora nad napakami je odkrivanje in lociranje napak, njihovo beleženje, obveščanje uporabnikov in – če je mogoče – njihovo odpravljanje.

- Nadzor napak sestavlja več mehanizmov, vsak za svojo nalogo, ki pa skupaj omogočajo:
  - Raziskovanje omrežja (network discovery), ki najprej odkriva naprave v omrežju, nato pa iz MIB ugotavlja tip naprave.
  - Preslikava omrežnih naprav v topološko shemo, v kateri vsaki napravi natančno določi topološko mesto in s tem določi njene učinke na podatkovne poti oziroma druge naprave v omrežju.
  - Sprejem in obdelava dogodkov vseh spremljanj omrežja skladno z dogodkovnim modelom.
  - Zajem podatkov o zmogljivosti ter njihov prikaz za naknadno analizo morebitnega preventivnega ukrepanja.
- Primeri sistemov za nadzor napak: HP Open View, . . .

Nadzor nastavitev

- Nadzor nastavitev uporabljam pri:
  - nadzor strojne opreme (Inventory Management),
  - nadzoru programske opreme (Software Management), uporablja se predvsem pri operacijskih sistemih
  - nadzoru nastavitev (Configuration File Management)

- Nadzor nastavitev omogoča:
  - Centralizirano distribucijo programske opreme naprav
  - Centralni arhiv za vse nastavitve v vseh napravah
  - Centralizirano upravljanje in nameščanje nastavitvenih datotek
  - Centralizirano spremljanje nastavitve strojne opreme v vseh napravah

Nadzor zmogljivosti

- Nadzor zmogljivosti spremlja vse vidike kapacitete, obremenitve, sposobnosti in razpoložljivih virov v omrežju.
- Izvaja se na dva načina:
  - **sprotno spremljanje**, ki dejansko zajema informacije o prometu v zelo kratkih časovnih intervalih
  - **statistično spremljanje**, kjer informacije iz sprotnega spremljanja vrednotimo v daljših časovnih intervalih
- Informacije se lahko zbirajo s protokoloma SNMP in RMON, obdelujejo, vrednotijo in prikazujejo pa s posebnimi orodji:
  - **sprotno spremljanje**:
    Info Vista, SAS IT service Vision, Fluke Network Monitor
  - **statistično spremljanje**: Fluke Protocol Analyzer
- Z nadzorom zmogljivosti lahko nadzorujemo tudi izpolnjevanje SLA parametrov.

Analiza zmogljivosti in povratni inženiring

- Celoviti vpogled v dogajanje in stanje v omrežju dajo profili prometnih tokov uporabnikov ali aplikacij.
- Profil prometnega toka določajo njegove statistične značilnosti.
- Le analiza prepleta aplikacijskih in uporabnikiških profilov prometnih tokov da poglobljeno sliko dogajanja v omrežju.
- Rezultate analiza uporabljamo pri povratnem inženiringu, ta lahko obsega:
  - nove nastavitve omrežnih naprav (stikal, usmerjevalnikov . . .)
  - novo politiko pri sklepanju SLA
  - dogradnja zaščitnih ukrepov pred neželenim prometom
  - . . .
- Sprotno spremljanje prometnih tokov in s tem določanja njihovih profilov omogočata RMON in NetFlow.

Dogovor o kakovosti storitev

Pogodba o nivoju storitev (SLA):

Pogodba o nivoju storitev (Service Level Agreement: SLA) je sklenjen dogovor med ponudnikom in uporabnikom (telekomunikacijskih) storitev, ki količinsko določa parametre omrežnih zmogljivosti.

SLA natančno določa vse parametre in njihove mejne vrednosti, s katerimi lahko merimo izpolnjevanje dogovorjenih mrežnih zmogljivost, ter način spremljanja oziroma merjenja teh parametrov.

- Parametri zmogljivosti omrežja po plasteh ISO/OSI modela:
  - L2: bitna hitrost na izhodnem in/ali vhodnem kanalu, število napak na posameznem kanalu, zakasnitev pri prenosu, ...
  - L3: bitna hitrost, zmogljivost posredovanja IP paketov, velikost MTU, velikost izhodnih pomnilnikov, število čakalnih vrst, latenca, zakasnitev, drhtenje, ...
  - L4: zmogljivosti, ki so odvisne od protokola

Dogovor o kakovosti storitev (2)

- SLA pridobi na pomenu, ko poleg zmogljivosti komunikacije zahtevamo še kakovost storitev ponudnika in/ali omrežja.

Kakovost storitev:

Kakovost je skupnost lastnosti in karakteristik izdelka ali storitev, ki se nanaša na njihovo zmožnost zadostiti zapisanim potrebam.

British Standard

- **Splošne parametri kakovosti**: zanesljivost delovanja v MTBF, čas med odkritjem in odpravi napake, odzivni čas servisa itd.
- **Razredi kakovosti storitev:** zlati, srebrni, . . . razred.

SLA in varnost:

Danes postaja varnost pomembna atribut pri merjenju kakovosti storitve ponudnika oziroma njegove omrežja.

Nadzor varnosti

Varnost omrežij:

Vsaka varnost komunikacijskih omrežij in informacijskih sistemov (IS) se prične z varnostno politiko, nadzorni sistemi jo lahko le izvajajo.

Sistemi za varnostni nadzor:

- Sistemi za varnostni nadzor omrežja primarno skrbijo za avtentikacija (authentication), avtorizacijo (authorization) beleženje uporabe virov (accounting). Zato mnogokrat te varnostne sisteme imenujemo sistemi AAA oziroma sistemi A^3
- Varnostni nadzor je – iz vidika komunikacijskega omrežja – ločen od zaščite omrežja ali IS pred vdori iz drugih omrežij.
- Varnostni nadzor nima nič skupnega z nadzornimi sistemi, ki skrbijo za delovanje zaščitnih sistemov.

AAA

- V sodobnih omrežjih se dostop do naprav v komunikacijskih omrežjih omejuje na pooblaščene osebe ali entitete.
- Osnova omejevanja je varnostna politika lastnika omrežja.

Varnostna politika:

- Osnova varnostne politike je jasno določitev pravic, ki jih ima posamezni uporabnik omrežnih storitev.
- Jasno morajo biti opredeljena dovoljenja uporabnikom in sistemom nadzora do dostopa do informacijskih virov in komunikacijskih naprav ter pravic poseganja v njihovo vsebino oziroma delovanje.
- Vsak dostop do virov ali naprav dovoliti sistem A^3.

AAA

- Avtentikacija entitet v omrežju ima isti cilj in pomen kot identifikacija ljudi v običajnem življenju – določiti identiteto posameznika.
- Za avtentikacijo se uporabljajo različni mehanizmi:
  - uporabniška imena in gesla,
  - enkratna gesla (sistemi OTP),
  - pametne kartice,
  - digitalna potrdila,
  - biometrični podatki
- Avtentikacija dobra takrat, ko združuje tri elemente:
  - nekaj kar si,
  - nekaj kar imaš
  - nekaj kar veš

  na primer: **prstni odtis + pametna kartica + geslo**.

AAA

- Avtorizacija je postopek, ki podrobno določi pravice pri uporabi omrežnih virov entiteti oziroma uporabniku, ki jih pridobi z uspešno avtentikacijo.
- Vsak dostop do omrežja in njegovih virov se zabeleži.
- Beleženje se uporablja za:
  - za izstavitve računa (na primer, za čas uporabe interneta),
  - za izdelavo statistik uporabe virov
  - zagotavljanja revizijskih sledi
  - beleženje navad uporabnikov za samodejno prilagajanje njegovim potrebam
  - ...

AAA

- Sistemi AAA se lahko lokalni ali centralni.
- Centralni sistemi AAA omogoča:
  - \+ enotno avtentikacijo, avtorizacijo in beleženje uporabe za vse omrežne vire.
  - \+ povečanje varnosti zaradi možnosti sledenja kraja izvajanja AAA (zelo pomembna storitev pri plačevanju s kreditnimi karticami)
  - − povečanje prometa v omrežju zaradi AAA
- Za izvajanje centralnega sistema AAA obstaja več komunikacijskih protokolov – RADIUS, TACAS in drugi, orientirani v računalniško tehnologijo.
- Primer centralnega sistema AAA je sistem Cisco ACS.

Protokoli za nadzor omrežij

- Večina komunikacijskih naprav podpira več omrežnih nadzornih protokolov:
  - Telnet – omogoča delo na oddaljeni napravi, oziroma njeno nastavljanje
  - SNMP – je osnovni protokol za upravljanje omrežij. SNMP sestavljajo upravljalski program v upravljalski postaji ter agent in baza upravljalskih informacij v upravljancu.
  - RMON je nadgradnja SNMP. Omogoča daljinsko zbiranje podatkov, ki jih zajema na primer računalniško podprti merilni sistem. Podatki so lahko skalarni ali organizirani v skupine ali polja.
  - Event log ni komunikacijski protokol, ampak omogoča beleženje vseh dogodkov na oddaljeni napravi.
- V zadnjem času se za daljinski nadzora vse več uporablja protokol http oziroma njegova varna izvedenka https.

Povzetek

Sistemi tehniškega nadzora (tele)komunikacijskih omrežij so danes predpogoj tekmovalnosti ponudnikov (tele)komunikacij na tržišču. Z njimi zmanjšajo stroške vzdrževanja, večajo zanesljivost delovanja in lahko jamčijo nivoje storitev uporabnikom, za katere so se obvezali pri sklenitvi pogodbe o nivoju storitev z uporabniki.

Področja uporabe nadzora komunikacij so nadzor napak, nastavitev, zmogljivosti, varnostnih parametrov in nadzor nad uporabo omrežnih virov.

Sistemi tehniškega nadzora komunikacijskih omrežij udejanjajo tudi varnostno politiko ponudnikov komunikacijskih storitev.

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;

Viri

- Cisco Systems, Inc: **Internetworking Technologies Handbook**. Fourth Edition, Cisco Systems™ 2004, ISBN 1-58705-119-2
- William Stallings: **Data and Computer Comunications**. Fifth editions, Prentice Hall, 1997, ISBN 0-13-571274-2
- Boštjan Lavuger: **Nadzor komunikacijskih omrežij**. Poročilo o individualnem raziskovalnem delu, UM-FERI 2006