poročilo

DELAVNICA *TEMELJI VARNOSTI OMREŽJA*

Delavnica je potekala 27. oktobra 2009 na Agenciji POTI v Ljubljani. Vodil jo je Janko Kersnik, certificiran predavatelj za varnostne rešitve Juniper Networks, pred tem pa je delovne izkušnje pridobival pri Akademski in raziskovalni mreži Slovenije ARNES.

Delavnica je imela naslednje vsebinske sklope:

- Uvod v temelje varnosti omrežja.
- Vrste napadov in groženj.
- Kako se zaščitimo (gradniki zaščite).
- Varovanje dostopa do informacij.
- Požarni zid.
- Sistemi za detekcijo ter sistemi za detekcijo in preprečevanje napadov.
- Kriptografija.
- Navidezna privatna omrežja.
- Reaktivna in proaktivna varnost.

UVOD V TEMELJE VARNOSTI OMREŽJA

Poskušali smo odgovoriti na vprašanje: Kaj pomeni varnost omrežja? Prišli smo do zaključka, da varnost omrežja pomeni:

- zaščito omrežja in storitev pred nepooblaščenim spreminjanjem, uničenjem ali razkritjem,
- zagotavljanje pravilnega delovanja omrežja,
- preprečevanje stranskih učinkov in zagotavljanje integritete podatkov.

Zaščito omrežja izvedemo s pomočjo varnostnih naprav, varnostne politike in procesov. Varnostne naprave in procesi uveljavljajo varnostno politiko.

VRSTE NAPADOV IN GROŽENJ

Grožnje delimo na:

- strukturirane – napad je organiziran na točno določeno tarčo,
- nestrukturirane – napad ni organiziran in ni usmerjen na točno določeno tarčo, določenega gostitelja, omrežja ali organizacijo.

Vsiljivce delimo na:

- bolj izkušene, ki so običajno del strukturirane grožnje (angl. *cracker*),
- vpletene v strukturirane in nestrukturirane napade (angl. *hacker*),
- začetnike, ki uporabljajo skripte za preverjanje omrežja in izvajanje napadov (angl. *script kiddie*).

Napade delimo na:

- poizvedovalne napade – njihov cilj je zbrati čim več podatkov o sistemu ali omrežju,
- napade s poskusom dostopa – njihov glavni cilj je izrabiti ranljivost in pridobiti dostop do sistema oziroma omrežja.
- napade z zavrnitvijo storitve oziroma napade DoS – njihov glavni namen je, da onemogočijo delovanje računalnika ali omrežja.

GRADNIKI ZAŠČITE

Varnostna politika je središče celotne izvedbe zaščite. Določa, kdo lahko dela v omrežju in kaj, kako so sistemi zaščiteni in kdo je odgovoren za posamezno funkcijo.

S postopki a**vtentikacije**, **avtorizacije** in **beleženja** se samo pooblaščenim uporabnikom zagotavlja dostop do omrežnih virov, hkrati pa omogoča beleženje informacij o dostopu.

Segmentacija omrežja omogoča ločevanje virov glede na vrednost in tip. Poskrbi za večnivojsko zaščito bolj pomembnih sredstev. Vključuje tudi uporabo naslavljanja NAT/PAT po RFC 1918.

Dinamična primarna zaščita zahteva uporabo usmerjevalnikov in požarnih zidov ter sistemov IDP.[1] Ta kombinacija omogoča primarno zaščito, saj zaznava in odgovarja na napade.

Navidezna zasebna mreža – VPN (*angl. virtual private network*) zagotavlja varno povezavo med lokacijami in omrežnimi segmenti.

Zaščita odjemalcev je zadnja linija obrambe. Če napadalcu uspe priti do tarče, mu napad prepreči zaščita na odjemalcu. Zaščita prepreči neznan napad, saj reagira na vsako aktivnost, ki odstopa od normalnega delovanja.

Učinkovito nadziranje za spremljanje podatkov, ki jih posredujejo omrežne naprave (z njimi zaznamo napad na omrežje).

Korelacija in iskanje trendov omogoča učinkovito upravljanje z velikimi količinami podatkov, ki jih posredujejo omrežne naprave. Obstaja tudi možnost korelacije podatkov iz različnih vrst naprav (kot npr. požarne pregrade in sistem IDP), saj lahko dobimo celovito sliko napada.

Učinkoviti varnostni proces je nenehen proces, ki zahteva stalne izboljšave, večjo natančnost in vedno boljše razumevanje okolice.

VAROVANJE DOSTOPA DO INFORMACIJ

Preverjanje identitete uporabnika je v elektronskem poslovanju ključnega pomena. Za zagotavljanje nemotenega poslovanja mora podjetje zagotoviti dostop do pomembnih podatkov in aplikacij različnim notranjim in zunanjim uporabnikom. Brez zanesljive avtentikacije uporabnikov so ključne informacije podjetja izpostavljene poneverbi, kraji in neupravičeni uporabi.

Statistika kaže, da 45 % vseh varnostnih vdorov povzročijo nezadovoljni ali zlonamerni zaposleni (vir: CSI/FBI 2003), 70 % vseh nepooblaščenih dostopov do informacijskih sistemov storijo zaposleni; od tega je 95 % vdorov povezanih z velikimi finančnimi izgubami (vir: Gartner).

Prav tako je treba sistem zaščititi pred osebami, ki fizično vstopajo v zgradbo (pogodbeni, servisni, storitveni delavci in gostje, vključno s ponudniki, strankami in partnerji) – vsak od njih lahko odkrije geslo za dostop do ključnih informacij.

POŽARNI ZID

Požarni zid je sistem za kontrolo dostopa med dvema omrežjema. Požarni zid je odporen na napade in je edina prehodna točka med dvema omrežjema (celoten promet gre skozi njo).

Uveljavlja kontrolo dostopa na različnih nivojih:

- kontrolo povezljivosti – omejuje, kdo se lahko poveže,
- kontrolo protokola – omejuje, kaj lahko uporabnik počne znotraj aplikacije,
- kontrolo podatkov – omejuje, kateri podatki se lahko izmenjujejo.

Požarni zid mora biti edina prehodna točka med dvema omrežjema, tako se prepreči uporaba t. i. stranskih vrat (angl. *backdoor*), pri katerih se skuša zaobiti požarni zid in prekršiti omrežna politika dostopa.

Politika omrežnega dostopa določa, katere omrežne povezave so dovoljene glede na varnostno politiko organizacije. Zajeti so različni aspekti komunikacije:

- omrežne seje med odjemalci in strežniki,
- aplikacije, ki uporabljajo omrežne seje,
- podatki, ki se prenašajo znotraj aplikacijskih sej.

SISTEMI ZA DETEKCIJO IN SISTEMI ZA PREPREČEVANJE VDOROV

Napadi se dogajajo na različnih nivojih. Nekateri na omrežnem nivoju, drugi na aplikacijskem nivoju, medtem ko obstajajo tudi hibridni napadi. Za zaščito pred njimi potrebujemo sistem, ki bo razumel in prepoznal napade na vseh nivojih.

Za znane napade obstajajo vzorci, ki jih lahko razpoznamo s pomočjo podpisov. Toda napad, ki bo odstopal od vzorca, bo še vedno uspešno prebil obrambo.

S pomočjo mehanizma anomalije protokolov lahko razpoznamo tudi nove napade ali pa napade brez vzorcev. Tu gre za primerjavo prometa s protokolom in ugotavljanja kakršnegakoli odstopanja:

- IDS (Intrusion Detection System) je sistem za detekcijo napadov in je sposoben zaznati napad, ni pa ga zmožen preprečiti.
- IPS (Intrusion Prevent System) je sistem za detekcijo in preprečevanje napadov in je sposoben zaznati napad ter ga po potrebi tudi preprečiti.
- IDS sistem, ki ima sposobnost posredovanja signalizacije požarnemu zidu, se lahko zelo hitro sprevrže v sistem, ki ga napadalci uporabijo za DoS napade.

KRIPTOGRAFIJA

Kriptografija je veda o pisanju in branju kodiranih sporočil. Osnovni elementi, na katerih temeljijo varnostni principi, so:

- *Zaupnost*. Podatkovna enkripcija ohranja podatke varne in skrite. Podatki se kriptirajo in dekriptirajo s pomočjo simetričnih in asimetričnih ključev. Podatkovna enkripcija je povraten proces.
- *Integriteta*. Zagotovilo, da se informacija ni

spremenila. Uporablja se hash funkcija. Enosmerni hashing algoritem – iz hash vrednosti ni možno določiti originalnih podatkov. (hash = zgoščena vrednost, digitalni prstni odtis)
- *Avtentikacija*. Za preverjanje, ali je informacija res prišla do pravega vira, se uporablja mehanizem HMAC (Heshing Message Authentication Code), ki preverja podatke v paketu in jim dodaja tajni ključ.

Enkripcija s simetričnimi ključi je najbolj enostavna oblika enkripcije z najmanj izgubami oz. dodatnega prometa. Ker se isti ključ uporablja za enkripcijo in tudi za dekripcijo, se imenuje simetrična enkripcija. To pomeni, da morata obe strani poznati in imeti isti ključ. Največjo težavo predstavlja upravljanje s ključi, saj je treba zagotoviti varen prenos ključa na drugo stran.

Pri asimetrični enkripciji se uporablja metoda para ključev, ki sta med seboj matematično povezana. Privatni ključ je varno spravljen in poznan samo lastniku. Javni ključ je javno objavljen in dosegljiv komurkoli. Podatke, ki so šifrirani s privatnim ključem, je možno dekriptirati samo z ustreznim javnim ključem. Ker so ključi med seboj matematično povezani, je skoraj nemogoče izpeljati en ključ s pomočjo drugega. Javni ključi se uporabljajo predvsem za avtentikacijo uporabnikov in naprav.

Proces zgoščevanja (angl. *hash*) preverja, da podatki niso bili spremenjeni. Proces zgoščevanja poteka v tem zaporedju:

- Pošiljatelj pošlje podatke preko zgoščevalnega procesa.
- Pošiljatelj pripne zgoščeno vrednost k podatkom in pošlje vse skupaj k prejemniku.
- Prejemnik loči podatke in zgoščeno vrednost.
- Prejemnih pošlje podatke preko zgoščevalnega procesa.
- Prejemnik primerja vrednost obeh zgoščevalnih procesov. Če se vrednosti ujemata, se podatki niso spremenili.

NAVIDEZNA PRIVATNA OMREŽJA

Omrežja VPN (predstavljajo sredstvo za varno komunikacijo med dvema lokacijama, ki sta povezani s pomočjo tunela IPsec, preko interneta kot javne infrastrukture. Tunel IPsec ima naslednje varnostne funkcije:

- zasebnost s pomočjo enkripcije,
- vsebinska celovitost s pomočjo avtentikacije,
- pošiljateljeva navzočnost.

REAKTIVNA IN PROAKTIVNA VARNOST

Z večanjem števila znanih groženj in ranljivosti raste tudi število varnostnih incidentov. Znane ranljivosti izrablja 99 % vdorov, za katere obstajajo protiukrepi (CERT), 90 % manj uspešni pa bodo napadi v podjetjih, ki bodo uporabljala sistem za nadzor ranljivosti omrežja in upravljanje z ranljivostjo (Gartner).

Reaktivna varnost je učinkovita v primeru napada ali izgube. Proaktivna varnost ublaži izpostavljenost pred izrabljanjem. Pravilno konfigurirani in posodobljeni sistemi so imuni na napade.

Opomba

1 IDP sistem (Intrusion Detection Prevention) je sistem za detekcijo in preprečevanje napadov.

Boštjan Krajnc, Matjaž Cigrovski, Boštjan Batič