Securing the network and information

Markus Peuhkuri

2001-03-15

Luennon aiheet

- Yleistä tietoturvasta
- Operaattorin turvallisuus
- Asiakkaan turvallisuus

Kirjasta kappale

- 9 Security (ss. 349–368)

Mitä tietoturva on?

Luottamuksellisuus tieto on vain oikeiden tahojen käytettävissä

Tunnistettavuus tiedon lähde tai kommunikoiva osapuoli tunnetaan

Tiedon eheys tietoa ei ole muutettu tunnistetun tahon jälkeen

Kiistämättömyys tiedon lähde tai osapuoli ei voi kiistää omaa osuuttaan

Tiedon saatavuus tieto on käytettävissä tietyllä hetkellä

Miten suuri turva tarvitaan

- Täydellistä turvaa ei ole
  ⇒ investointi turvallisuuteen kannattaa jos

$$kulut_{turvaus} < \sum P('riski'_i) kulut_{vahinko} \tag{1}$$

- Käytännössä
  1. minimoidaan riskit
  2. noudatetaan hallintarutiineja
  3. seurataan kehitystä

Eräs tapa nostaa turvallisuutta

Iso paha Internet

- Televerkko
  - operoitu
  - yhteyksien kirjaus
  - muutamia, “luotettuja” osapuolia
  - hallinta- ja käyttäjäliikenne eriytetty
  - äly verkkolaitteissa
- Internet
  - miljoonia liityntäpisteitä
  - ei (aina) yhteyksien kirjausta
    ⇒ jäljittäminen vaikeaa
  - in-band hallinta
  - äly päätelaitteissa

Ongelmakohdat

- Operointi perustuu keskinäiseen luottamukseen

  DNS paikalliset valtuutukset
  ⇒ mahdotonta varmistua oikeellisuudesta[1]

  reititys sisältää tiedon vaihtoa verkon rakenteesta ja vertaissuhteista
  ⇒ liikennevirtojen muuttaminen mahdollista

- Hyödyt suuremmat kuin riskit
  ⇒ tilanne voi muuttua Internetin merkityksen kasvaessa

Panostukset turvallisuuteen

- Toiminta keskittynyt *suoria tuloja* tuovaan toimintaan
- Turvallisuudesta ei välitöntä tuloa
  ⇒ lasku laiminlyönnistä tullee “joskus”
- Oikea tasapaino ja prioriteetti turvapanostuksiin

Mitä kyselyt kertovat

Computer Security Institute & FBI: 538 yritystä, viranomaista, yhteisöä ja yliopistoa (USA)

- 85 %:lla vastaajista tietoturvatapauksia
- 64 %:lla taloudellisia menetyksiä
- Menetykset keskimäärin yli USD 500 000
- Suurimmat menetykset salaisesta tiedosta ja taloudellisista huijauksista (> USD 4 000 000 keskimäärin)
- 70 % hyökkäyksistä internetistä, 30 % sisäisistä järjestelmistä
- Järjestelmiin tunkeuduttu 40 % organisaatioissa
- 38 % DoS-hyökkäyksen kohteena
- 91 %:lla työntekijöitä “väärää sisältöä” hankkimassa
- 94 % tietokoneviruksia

[1] DNSSEC `http://www.ietf.org/html.charters/dnsext-charter.html` tuo apua

- 33 % luvatonta käyttöä
- 37 % *ei tiennyt* onko ollut luvatonta käyttöä
- 79 % enemmän kuin 2 tapausta, 58 % enemmän kuin 10
- 90 % hyökkäyksistä vandalismia
- 13 % hyökkäyksissä tapahtumatietojen varastamista
- 8 % hyökkäyksissä talousrikoksia

http://www.gocsi.com/prelea_000321.htm

Prioriteetit turvallisuudessa

Palvelun eheys peruskriteeri

- verkkolaitteet (reitittimet, kytkimet, liityntäpalvelimet)
- palvelinlaitteet (nimipalvelu, web, posti, käteispalvelin)
- tiedostot

Asiakasturvallisuus riippuu ISP:n turvallisuudesta

- vaikuttaa myös ISP:n turvallisuuteen
- "murrettu" asiakas voi aiheuttaa ISP:lle vahinkoa
- esim. VPN- ja autentikointipalvelut, nimipalvelu

Tapahtumiin reagointi oltava suunniteltua

- hyökkäysten havainnointi
- hyökkääjien seuranta yhteistyössä

Viranomaisvaatimukset ovat minimi

- vaatimukset operoinnille
- avustus rikosten selvittämisessä

Mitä Suomen viranomaiset sanovat?

THK 47/1999 M Teleyritysten tietoturvasta

- perustuu lakiin *yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta* (565/1999)
- THK voi puuttua yrityksen toimintaan (uhkasakko tai toiminnan keskeytys)
- Sakkoa laiminlyönneistä

THK 48/1999 M Teleyritysten ja televerkkojen fyysinen suojaus

- murto-, palo- ja vesisuojaus

THK 30 A/1997 M Televerkkojen tehonsyötöstä

- sähkön syötöstä sähkökatkon aikana
- eri tärkeysvaatimuksia tilaajamäärän perusteella
- akusto vähintään 3 h
- varavoiman liitosmahdollisuus

THK 47/1999 M Teleyritysten tietoturvasta

Toiminnan tietoturvallisuus: dokumentoinnin vaatimus

- *kirjalliset* ohjeet
- tietoturvan *tasoa seurattava*, myös *alihankkijoiden*
- laitteistot ja tiedostot on *suojattava luvatonta* pääsyä ja käyttöä vastaan.
- järjestelmien *käyttäjät ja oikeudet* kirjattava rekisteriin
- *valvottava*, että tietoturvaan vaikuttavat tapahtumat *havaitaan*
- muutokset järjestelmään kyettävä *jäljittämään*

Tietoliikenneturvallisuus: verkkoturvallisuus

- viestien ja tunnistetietojen *paljastumattomuus*
- viestien ja tunnistetietojen *muuttamattomuus*
- käyttäjän ja yrityksen väliset todentamis-, *pääsynvalvonta-* ja kiistämättömyysmenettelyt
- hallinta-, reititys-, veloitus-, loki- ja käyttäjätietojen *suojaus* asiattomilta

Laitteisto- ja ohjelmistoturvallisuus: järjestelmien valinta

- käytettävien järjestelmien *tietoturvallisuusriski on pieni*
- tärkeiden ohjelmistojen *varmuuskopiointi* ja *säilytys*

Tietoaineistoturvallisuus: tiedon turvaus

- tietoaineistojensa turvallinen käsittely *hyvän tietojenkäsittelytavan* mukaisesti
- määriteltävä *suojattavat* tietoaineistot
- tietoaineistojen *varmuuskopiointi* ja *turvallinen säilytys*

THK 48/1999 M: Teleyritysten ja televerkkojen fyysinen suojaus

Erittäin tärkeä tila suuri määrä liikennettä, laitteiden korvaus vaikeaa tai vaikuttaa suureen alueeseen

- verkkojen yhdysliikennepiste
- teleliikennealuetason laitteet
- valtakunnallisen verkonhallinnan laitteita

Tärkeä tila vika häiritsee yli 5000 tilaajan liikennettä

- verkon tärkeä solmupiste
- palvelinhotelli
- verkonhallinnan laitteita

Luokitus koskee myös *toimisto-* ja *asiakaspalvelutiloja* jos näissä olevista laitteista on pääsy asiakas- tai hallintajärjestelmiin

Vaatimukset tiloille

Perusvaatimukset kaikille tiloille

- asiattomien pääsy estetty (murtosuojaus, lukot, ovirakenteet)
- tilat jaettu käyttötarkoituksen mukaan
- seinä-, katto- ja lattiarakenteet vahvoja
- vesivahingot estettävä
- henkilökunta tunnistettava
- vierailijoita ja asiakkaita valvottava

Tärkeiden tilojen lisävaatimukset

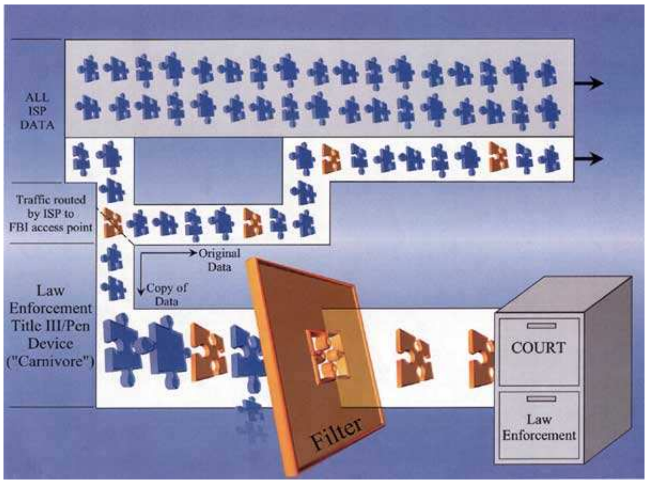
- kiviaineiset katto- ja seinärakenteet
- palamattomat sisämateriaalit
- tallentava, yksilöivä kulunvalvontajärjestelmä
- automaattinen paloilmoitusjärjestelmä

Erittäin tärkeiden tilojen lisävaatimukset

- rakenteellisesti kevyt väestönsuoja
- "järeän" murtoyrityksen kestävä
- kaksoislukitus
- ulkopuolisesta sähköstä riippumaton vuotovedenpoisto
- tallentava videovalvonta
- rikos- ja lämpötilailmoitusjärjestelmä

Carnivore

- FBI:n salakuuntelulaite
- Liitetään operaattorin verkkon
- Suodatus aktivoidaan oikeuden päätöksellä



`http://www.fbi.gov/programs/carnivore/carnivore.`

Turvaongelmat

Protokollaongelmat protokollien suunnittelussa ei riittävää painoa turvaominaisuuksiin

- IP-lähdereititys
- FTP-protokolla

Ohjelmistovirheet syötteen olettaminen

- ohjelmointivirheet (puskureiden ylivuodot yms.)
- virheellinen toteutus protokollasta (esim. ICMP redirect)
- mitään *ei pidä olettaa* käyttäjältä tai verkosta tulevasta datasta

Konfigurointivirheet oletuskonfiguraatio pielessä

- ominaisuudet tärkeämpiä kuin turvallisuus
  ⇒ oletusasetukset liian sallivia

Palvelunestohyökkäys

- Helpoin hyökkäys
- Helppo naamioitua väärentämällä osoite

Smurf useat laitteet vastaavat levitysosoiteeseen lähetettyyn ICMP Echo Request-viestiin

Jos aliverkko on 10.50.1.0/24, saadaan osoitteeseen 10.50.1.255 lähetettyyn viestiin jopa 254 vastausta
$\Rightarrow$ liikenteen lisäys 254-kertaiseksi

- väärentämällä lähetysosoite, voidaan vastaus kohdistaa haluttuun koneeseen
- estetään konfiguroimalla reititin olemaan välittämättä suunnattuja levitysviestejä [8]

TCP SYN flood (myös NAPTHA)

- järjestelmän tietorakenteiden täyttäminen
- suuri määrä puoliavonaisia TCP-yhteyksiä
  $\Rightarrow$ "oikeita" yhteyksiä ei voida hyväksyä

DDoS (hajautettu DoS)

- murrettuja[2] tietokoneita käytetään orjina
- suuri määrä dataa lähetetään tiettyyn kohteeseen

ISP:n turvalista[7]

- Turvallisuusryhmä CSIRT (Computer Security Incident Response Team) [2]
- Kommunikointi asiakkaalle ja toisille ISP:lle
  - sähköpostitunnukset `security`, `abuse` ja `noc@isp.example` [3]
  - yhteystiedot whois- ja reititystietokannoissa [1] ajantasaiset
  - tietojen vaihto asiakkaiden, toisten ISP:den, CSIRT:n, viranomaisten, lehdistön ja yleisön kanssa *suunnitellusti* ja *turvallisesti*
  - tiedotus turvaongelmista
- Hyväksyttävän käytön politiikka: *sopimusehdoissa* oltava mahdollisuus puuttua asiaan
  - palvelun väärinkäyttö
  - ISP:n tai kolmannen osapuolen häiritseminen
  - murtautuminen toisiin koneisiin
  - datan muuttaminen
  - häiriköiminen

  Suomen *lainsäädäntö* mahdollistaa puuttumisen ilman sopimustakin vakaviin ongelmiin!

  - Rikoslain 38 luku, tieto- ja viestintärikoksista.
  - Vi 121, laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta.
  - Vi 121a, asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta.
- Verkon suojaaminen ja konfigurointi
  - reititystietokannoissa [1] ja protokollissa [6] tulee käyttää autentikointia
  - reititystietojen suodatus ja vaimennus
  - lähdeosoitteen suodatus (ingress)[4]
    * vain osoitteet, joihin on *reitti* toiseen suuntaan, sallitaan. Eräissä reitittimissä yksi komento.

[2] Joko "perinteisesti" ohjelmistovirheellä tai troijan hevosella tai viruksella.

    * ongelmia *Mobile-IP*:n kanssa
    * myös asiakkaan suuntaan (egress)
      ⇒ estää tekeytymisen asiakkaan verkossa olevaksi koneeksi
  - suunnattujen levitysviestien esto [8]

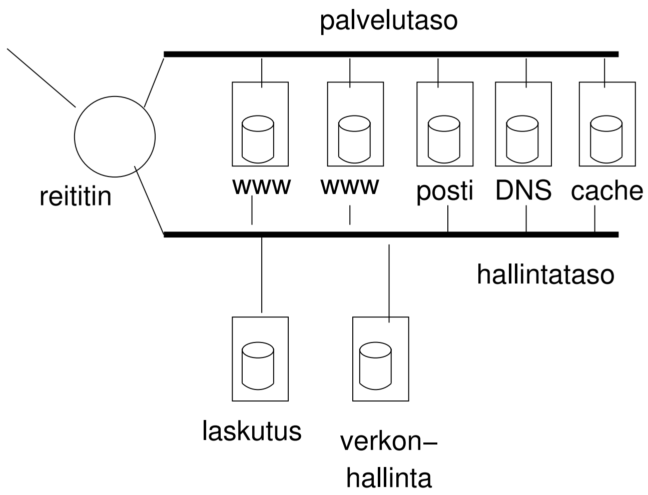
- Palvelinjärjestelmät
  - erilliset laitteet eri palveluille
  - vain asiaan kuuluville ylläpitohenkilöille pääsy järjestelmiin
  - vain palveluihin pääsy ISP:n verkon ulkopuolelta, ei hallintayhteyksille
  - palvelin- ja välitysverkkojen eriyttäminen vaikeuttaa salakuuntelua
  - postijärjestelmien suojaaminen

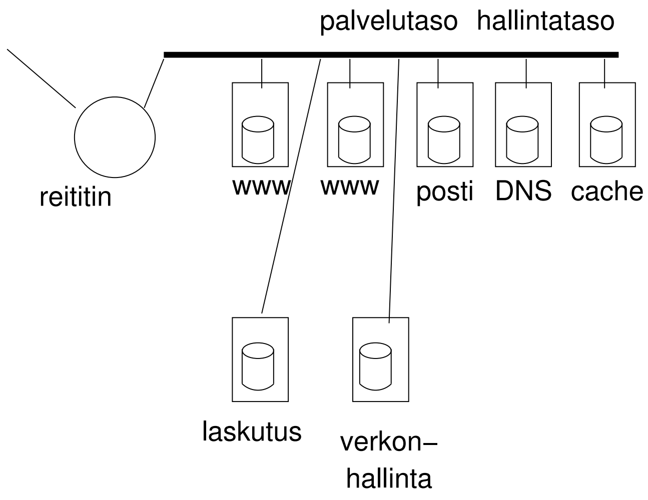
Palvelimien suojaaminen

- Kriittiset palvelimet
  - nimipalvelu (DNS)
  - autentikointi (RADIUS)
- Tärkeää tietoa sisältävät
  - laskutus
  - verkonhallinta
- Suuri liikennemäärä
  - sähköpostipalvelin (SMTP)
  - uutisryhmäpalvelin (NNTP)
  - WWW-käteispalvelin
- “Ohjelmoitavat” palvelimet
  - WWW-palvelimet
  - unix-palvelimet “shell”

Hallinnan ja palvelun eriyttäminen

- Liikenne ja hallinta eri verkoissa
  ⇒ paremmat mahdollisuudet rajoittaa ja seurata liikennettä





Suojautuminen

- *Mitä* suojataan?
- *Miltä* suojaudutaan?
- Uhkan *todennäköisyys*
- Toteuta *kustannustehokkaat* suojaukset
- Uudelleenarvioi *säännöllisesti*

Hyviä lähteitä esim. [5] ja `http://www.cert.org`

Haittaohjelmat

Virus leviää toisten ohjelmien tai dokumenttien välityksellä

- tuhoaa tiedostoja, jopa laitteistoja
- muuntaa tiedostoja
- heikentää suorituskykyä

Mato leviää itsenäisesti järjestelmästä toiseen verkon yli

- voi heikentää myös verkon suorituskykyä

Troijan hevonen näennäisesti hyödyllinen ohjelma tai dokumentti jolla on salainen toimintatapa

- voi esimerkiksi mahdollistaa murtautumisen koneeseen

Palomuurit

- Palomuuri eroittaa kaksi *eri turvapolitiikkaa* noudattavaa aluetta
  - yrityksen sisäinen verkko vs. Internet
  - myös yrityksen sisäisessä verkossa esim. osastojen välillä
- Yksikerroksinen palomuuri
  - yksi kone kahden verkon välissä
  - yksinkertainen konfigurointi, virheet vakavia
- Monikerroksinen palomuuri
  - palomuuritoiminnallisuus hajautettu useiden laitteiden välille
  - neutraaliverkko (DMZ) erotettavien verkkojen välillä

Toimintaperiaatteet

Pakettisuodatus päätös paketin kenttien perusteella

- tilaton
  ⇒ suorituskykyinen
- määrittely vaatii protokollatietämystä

	tietokone	reititin
+	laajennettava toiminnallisuus	suorituskykyinen, suuri määrä verkkoliitäntöjä
-	käyttöjärjestelmän heikkoudet	suurempi muistintarve, optimoitu reititykseen

Sovellusyhdyskäytävät luo uuden "yhteyden"

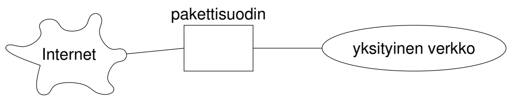
- läpinäkyvä (ei näy asiakaskoneelle) vs. konfiguroitava
- yhteyden puolitus
- vaatii suorituskykyä
- mahdollisuus analysoida dataa, esim. virustarkistus

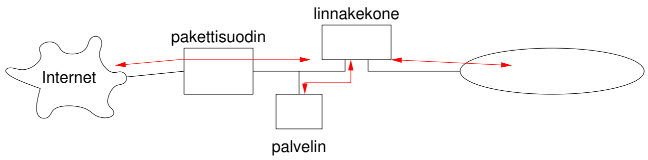
Tilallinen tutkimus (dynaaminen pakettisuodatus)

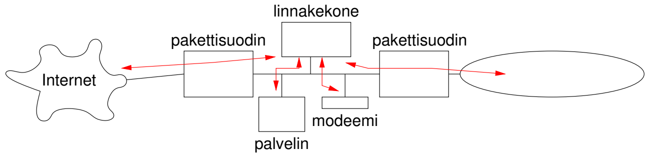
- mahdollistaa tarkemman analysoinnin kuin pakettisuodatus
- suuret datamäärät mahdollista "laskea läpi"

Monet tuotteet yhdistelmiä eri tekniikoista

Palomuuritopologiat







Palomuurin käyttöönotto

1. Valitse käytettävä topologia ja arkkitehtuuri: kompromissi
   - palvelun saatavuudesta (onko laite luotettava, tulisiko kahdentaa)
   - suorituskyvystä
   - turvallisuudesta
     – yksi vai kaksi palomuuria
     – eri valmistajien palomuurit
       ⇒ suuremmat hallintakulut, mutta pienempi riski ohjelmistovirheille
   - kuluista
2. Kasaa ja konfiguroi järjestelmä, järjestä tuki

- onko järjestelmä turvallinen myös käynnistyessään

3. Testaa järjestelmä testiverkossa
4. Ota käyttöön
   - ilmoita käyttäjille

Palvelimien suojaaminen

- Palvelimen turvariskit
  1. luottamuksellisuus: sekä palveluun että dataan
     - tiedosto- ja tietokantapalvelimet sisältävät yrityksen toiminnalle kriittistä dataa
     - autentikointipalvelimesta riippuu koko verkon turvallisuus
  2. eheys: tietoa ei muutettu
     - julkinen kuva, kirjanpito
  3. palvelun saatavuus: toipuminen ohjelmisto- ja laitteistovioista sekä turvavälikohtauksista
     - suoria menetyksiä kaupankäyntipalvelimien toimimattomuudesta
     - työvoimakuluja yrityksen sisäisten palvelujen toimimattomuudesta
  4. molemminpuolinen autentikointi

1. Huomioi turvallisuus käyttöönottosuunnitelmassa; määrittele
   - koneen tarkoitus; turvavaatimukset
   - tarjottavat palvelut
   - asennettavat ohjelmat
   - sallitut käyttäjät
   - käyttäjäryhmien oikeudet
   - autentikointimenetelmät: pyri käyttämään vahvoja menetelmiä
   - tietojen suojaus: käyttöjärjestelmän mekanismit tai salaus
   - tunkeutumisen havaitsemisstrategia
   - varmuuskopiointi- ja palautusmenetelmät
   - korvaus vikojen tai vaurioiden sattuessa
   - käyttöjärjestelmän ja sovellusten asetukset
   - liittyminen verkkoon
   - päivittäisen hallinnan menetelmät
   - käytöstä poistetun laitteiston käsittely, erityisesti massamuistit
   - määrittelyjen uusiminen
2. Liitä turvallisuusvaatimukset järjestelmän valintaan
   - toiminnalisten ja suorituskyvyn ohella
   - erityiset turvallisuusvaatimukset
   - selvitä tietoturvan taso
3. Pidä ohjelmistot ajantasaisina
   - seuraa *ajantasaisia* tietolähteitä päivityksistä ja turvaongelmista *säännönmukaisesti*
   - arvioi päivitystarve: eivät aina ongelmattomia
   - suunnittele päivitykset minimoiden häiriöt
   - päivitä uudet koneet välittömästi
   - päivitä tarkistussummat
4. Poista tarpeettomat palvelut

    - jokainen palvelu potentiaalinen turvariski
    - valitse turvallinen vaihtoehto (esim. ssh vs. rsh)
5. Määrittele käyttäjät ja oikeudet
    - poista tarpeettomat käyttäjät
    - tarkkaile salasanojen laatua
    - uudelleenautentikointi käyttämättömyyden jälkeen
6. Tapahtumien kirjaus
    - mitä tietoja tallennetaan
    - minne tallennetaan
    - miten tarkastetaan
    - tietojen varmuuskopiointi, salaus ja tuhoaminen
7. Tärkeiden tiedostojen varmuuskopiointi
    - säännöllinen varmuuskopiointi
    - riittävästi eri ikäisiä versioita
    - palautuksen onnistumisen tarkistaminen
8. Suojaa haittaohjelmilta
    - käyttäjäkoulutus, toimintatavat
    - ajantasaiset työkalut
9. Suojattu etähallinta
    - käytä suojattuja yhteyksiä ja vahvaa autentikointia
    - toimi minimaalisilla oikeuksilla
10. Suojaa kone ja yhteydet fyysisesti

Julkisten web-palvelimien suojaus

- Perusteet samat kuin yleisesti palvelimella
- Web-palvelin näkyvä osa palveluita
- Pääsy palvelimelle kaikkialta

1. Sijoita palvelin DMZ-verkkoon
    - huomioi tarvittava liikenne hakemistoihin ja tietokantoihin
2. Määritä suojaukset
    - palvelinprosessi ei pysty muuttamaan dokumentteja
    - vain julkiset dokumentit saatavilla
    - määritä resussirajat DoS-hyökkäyksen estämiseksi
3. Määritä Web-palvelimen tarvitsemat tapahtumakirjaukset
4. Huomioi sovellusten turvallisuusvaikutukset
    - tarpeellisuus ja luotettavuus
    - minimoi kunkin sovelluksen oikeudet
5. Käytä autentikointia ja salausta tarvittaessa
    - autentikointia ei tulisi käyttää ilman salausta
6. Säilytä kopio palvelimesta turvallisessa paikassa
7. Suojaa palvelin yleisiltä hyökkäyksiltä
    - pidä ohjelmistot ajantasaisina
    - työskentele ISP:n kanssa DDoS-hyökkäysten torjumiseksi

Työasemien suojaaminen

1. Huomioi turvallisuus laitteiden käyttöönotossa
   - vrt. palvelin
   - usein oletusasetukset turvattomat
2. Suojaa haittaohjelmilta
   - tee suunnitelma suojaamiseksi, huomioi ohjelmistovalinnoissa
   - käytä ajantasaisia virustorjuntaohjelmia
   - kouluta käyttäjät tunnistamaan ja välttämään viruksia ja troijalaisia
3. Poista tarpeettomat palvelut
4. Voiko työasema vuotaa tietoja tietojärjestelmistä?
5. Luo testatut malliasennukset
6. Ilmoita hyväksyttävän käytön politiikka
   - osa yrityksen tietoturvaa
     ⇒ johdon oltava takana
     ⇒ työntekijöiden sitouduttava (oltava mukana määrittelyssä)
   - politiikkaa seurattava ja kehitettävä sekä noudattamista valvottava
     ⇒ dokumentointi tärkeää
   - tarjoa säännöllisesti muistutus

Alihankkijat ja turvallisuus

- Usein tietojärjestelmiä hankitaan alihankkijoilta
- Näillä pääsy (asennuksessa) tietojärjestelmiin
  ⇒ turvariski

1. Alihankkijan turvallisuuden oltava samalla tasolla
   - vaatimukset kirjattava sopimukseen
   - virus- ja troijalaisvapaa ohjelma
   - NDA
2. Ohjelmisto asennettu ja konfiguroitu oikein
3. Alihankkijan yhteydet turvattuja
   - vahva autentikointi
   - tiedon salaus
4. Alihankkijalle annetut oikeudet kontrolloitava ja dokumentoitava
5. Tarkkaile yllättäviä muutoksia järjestelmään
6. Tarkkaile tapahtumakirjauksia
7. Arvioi alihankkijan suoriutuminen
   - seurataan alihankkijan turvallisuutta
8. Poista alihankkijan pääsy järjestelmään heti kun mahdollista

Kuinka havaita tunkeutuminen

- Järjestelmän tulisi olla instrumentoitu siten, että tunkeutuminen havaitaan

  verkon suorituskyky liikenteen määrä, ominaisuudet ja jakauma, virheiden määrä

  verkkoliikenne yhteyspyynnöt, laitejakauma, yhteyksien kestoajat, skannaukset, verkkoliitäntöjen tilat

  järjestelmien suorituskyky resussien käyttö (CPU, muisti, levy), virheiden määrä

  järjestelmät oikeuksia vaatineita toimia, epäonnistuneita sisäänkirjautumisia, uusia palveluita

  prosessien suorituskyky prosessin käyttämät resussit, eniten resusseja käyttävät prosessit

  prosessit käyttäjät verrattuna "normaaliin", auki olevat tiedostot

  tiedostot tarkisteet tiedostoista, lista oikeuksista, muutosajankohdat, oudot tiedostojen sijainnit, virustarkistukset

  käyttäjät epäonnistuneet kirjautumiset, oudot yhteydenottopaikat, käyttäjämuutokset, epäonnistuneet yritykset suojattuun tietoon

  lokitiedostot eri sovelluksilta ja järjestelmistä: poikkeavuudet

- Lokitiedostot turvallisessa paikassa
  - kertakirjoitettavalle medialle
  - salatut tiedostot
  - suojautuminen täyttyviltä levyiltä
  - dokumentoi käsittely
- Tarkkaile verkkoa ja järjestelmiä jatkuvasti
- Huomioi fyysinen tunkeutuminen
  - tuntematonta laitteistoa verkossa, esim. modeemit
  - reititysmuutokset
- Tiedota tarkkailusta käyttäjille

Kuinka reagoida tunkeutumiseen

1. Määrittele toimintaohjeet ja politiikka
   - mitä tehdään missäkin vaiheessa
     - pyritään keräämään tietoa hyökkääjistä
       * otetaan yhteyttä hyökkääjän palveluntarjoajaan
       * estetään hyökkääjän pääsy
     - suljetaan järjestelmät niiden suojelemiseksi
     - tarkkaillaan hyökkääjää
     - palautetaan viottuneet järjestelmät
   - kuka tekee päätökset
   - ketkä vastaavat mistäkin osasta
   - onko toiminta laillista
2. Valmistaudu vastaamaan
   - mahdollisuudet palauttaa tiedostot
   - yhteystiedot ja hakemistot vastuuhenkilöistä
3. Luokittele hyökkäys
   - millä hyökkäyksellä tunkeuduttiin
   - mihin järjestelmiin ja dataan päästiin käsiksi
   - mitä tunkeutuja teki päästyään järjestelmään

    - talennenna murretut järjestelmät analysointia varten

4. Ota yhteyttä tarvittaviin tahoihin

5. Kerää tarvittava tieto esim. todistusaineistoksi

6. Varmistu, että tunkeutuja ei hyödy keräämästään tiedosta

    - muuta salasanat
    - uudelleenasenna järjestelmät
    - tee tarvittavat korjaukset ja päivitykset

7. Palaa normaaliin toimintaan

8. Huomioi tapahtunut esim. käyttöönottosuunnitelmissa

Toimipisteiden yhteydet

- Perinteisesti erillisillä yhteyksillä
    - vuokralinjat
    - kehysvälitys
- VPN-ratkaisu usein kustannustehokas
- Hyvä turvallisuus mahdollinen
  ⇒ avaintenhallinta kriittistä
- Oma vai operaattorin toteutus

Etätyöntekijöiden yhteydet

- Yritysten omat soittosarjat kalliita ylläpitää ja käyttää
- Mahdollinen turvariski
- VPN-pohjainen ratkaisu tässäkin mahdollinen
- Käyttäjä integroituu yrityksen verkkoon
  ⇒ normaalit palvelut käytettävissä

Yhteenveto

- Dokumentaatio
- Rutiinit
- Ajantasaisuus
- Uudistaminen

Viitteet

[1] T. Bates, E. Gerich, L. Joncheray, J-M. Jouanigot, D. Karrenberg, M. Terpstra, and J. Yu. Representation of IP Routing Policies in a Routing Registry (ripe-81++). Request for Comments RFC 1786, Internet Engineering Task Force, March 1995. (Informational). URL:`http://www.ietf.org/rfc/rfc1786.txt`.

[2] N. Brownlee and E. Guttman. Expectations for Computer Security Incident Response. Request for Comments RFC 2350, Internet Engineering Task Force, June 1998. (Best Current Practice) (Also BCP0021). URL:`http://www.ietf.org/rfc/rfc2350.txt`.

[3] D. Crocker. Mailbox Names for Common Services, Roles and Functions. Request for Comments RFC 2142, Internet Engineering Task Force, May 1997. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2142.txt`.

[4] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Request for Comments RFC 2267, Internet Engineering Task Force, January 1998. (Informational) (Obsoleted by RFC2827). URL:`http://www.ietf.org/rfc/rfc2267.txt`.

[5] B. Fraser. Site Security Handbook. Request for Comments RFC 2196, Internet Engineering Task Force, September 1997. (Informational) (Obsoletes RFC1244) (Also FYI0008). URL:`http://www.ietf.org/rfc/rfc2196.txt`.

[6] A. Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. Request for Comments RFC 2385, Internet Engineering Task Force, August 1998. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2385.txt`.

[7] T. Killalea. Recommended Internet Service Provider Security Services and Procedures. Request for Comments RFC 3013, Internet Engineering Task Force, November 2000. (Best Current Practice) (Also BCP0046). URL:`http://www.ietf.org/rfc/rfc3013.txt`.

[8] D. Senie. Changing the Default for Directed Broadcasts in Routers. Request for Comments RFC 2644, Internet Engineering Task Force, August 1999. (Best Current Practice) (Also BCP0034). URL:`http://www.ietf.org/rfc/rfc2644.txt`.