Securing the network and information

Markus Peuhkuri

2004-03-11

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
- Vuotuinen kuluodotus
  $\Rightarrow$ investointi turvallisuuteen kannattaa jos

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

  Esimerkiksi, jos joku uhka aiheuttaa 100 ■:n kulun kerran päivässä, kannattaa sen torjumiseen käyttää hyvinkin tuhansia euroa vuosittain. Jos taas toinen uhka aiheuttaa 100 000 ■:n kulun kerrallaan mutta toteutuu vain 0,1 % todennäköisuudellä vuosittain, ei sen torjumiseen kannata panostaa paljoa.

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

Kuinka turvallisuus rakentuu

- Turvallisuus on prosessi, ei tuote
  - uusia turvallisuusongelmia tulee
  - ympäristö muuttuu: verkko, sovellukset, käyttäjät
- Turvallisuus riippuu heikoimmasta lenkistä

käytäjä	sovellukset	OS	laitteisto	verkko	palomuuri

Ei ole mitään merkitystä sillä, käytetänkö 40- vai 128-bittistä salausta tai 512- tai 2048-bittisiä RSA-avaimia jos salasanan saa arvattua, kysyttyä käyttäjältä tai salakuunneltua koneesta.

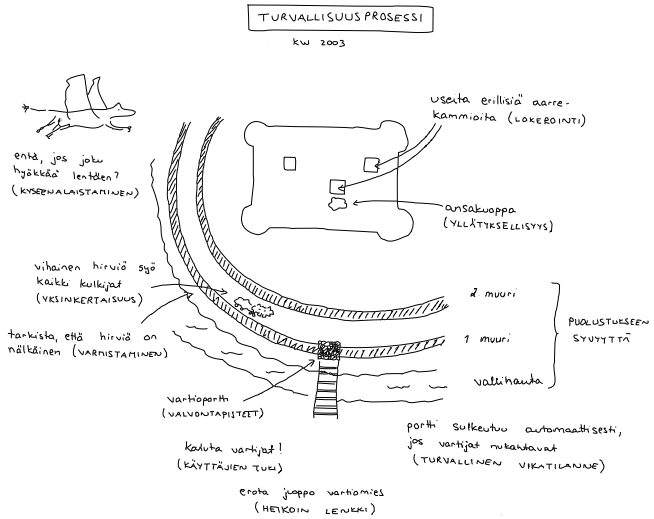
Turvallisuusprosessi

- Lokerointi: rajoita yhdestä ongelmsta johtuvat vahingot. Esimerkiksi pankkikorteilla ja -tileillä on tietty maksiminosto vuorokaudessa. Vastaavasti käyttäjillä tulee olla oikeudet vain niihin tietostoihin ja järjestelmiin, joita he tarvitsevat.
- Heikoimman lenkkin posto: on turha parantaa muita turvallisuuden osia, jos jonkun kohdan turvallisuus on selkeästi heikompi.
- Valvontapisteiden käyttö: turvallisuutta on helpompi valvoa, jos kaikki joutuvat kulkemaan tarkkailupisteen ohi. Tämä voi johtaa myös käytettävyysongelmiin.
- Puolustukseen syvyyttä: jos tunkeutuja joutuu murtamaan useita riippumattomia järjestelmiä, tehtävä on paljon vaikeampi. On kuitenkin varottava, että *JA*-ehto ei muutu *TAI*-ehdoksi. Esimerkisi maaliskuussa 2004 liikkunut Witty-mato `http://isc.incidents.org/diary.html?date=2004-03-22` hyödynsi palomuuriohjelman haavoittuvutta `http://www.securityfocus.com/bid/9913`. Muita palomuurien haavoittuvuuksia: `http://www.securityfocus.com/bid/9581` `http://www.securityf` `http://www.securityfocus.com/bid/9912` `http://www.securityfocus.com/bid/9915`

tunnistaminen		palomuuri			
käytäjä	sovellukset	OS	laitteisto	verkko	palomuuri

- Turvallinen vikatilanne: järjestelmät tulee konfiguroida siten, että vikatilanteessa valitaan turvallinen vaihtoehto, esimerkiksi estetään pääsy, jos autentikointipalvelimeen ei saada yhteyttä. Huomaa DoS-hyökkäyksen mahdollisuus!
- Yllätyksellisyys: turvajärjestelmissä on hyvä olla jotain muutakin kuin päälle näkyy. Sinänsä käyttöjärjestelmä- ja ohjelmaversioiden piilottamisella saatava hyöty on marginaalinen – haavoittuvuutta voidaan kokeilla mitään välittämättä. Hämärän turva ei saa kuitenkaan olla muuta kuin lisämauste: varsinaisen turvan tulee perustua koelteltuihin menetelmiin.
- Yksinkertaisuus: mitä laajempi järjestelmä, sitä enemmän siinä on potentiaalisia virheitä.
- Käyttäjien tuki: verkko ei voi olla turvallinen, jos käyttäjät eivät edistä sitä. Käyttäjä voidaan toki huijata paljastamaan salasanansa, muuten vaarantamaan verkon toiminta, tai toimia tahallisesti (sisäinen tietomurto) tuhoisasti, mutta yksittäisen käyttäjän aiheuttamaa tuhoa voidaan torjua esim. lokeroinnilla.
- Varmistaminen: ei riitä, että asennetaan purkki tai ohjelmisto X, on myös varmistuttava siitä, että se toimii kuten on tarkoitus.
- Kyseenalaistaminen: riskianalyysissä joudutaan tekemään joitakin oletuksia, jotta ongelma voidaan hallita. On tärkeää säännöllisesti arvioida uhkat ja olettamukset, koska ympäristön muuttuminen mahdollistaa uudet hyökkäykset. [10, s. 365]

Turvallisuus organisaatiossa



Turvallisuuden perusteet

- Estäminen: turvallisuuden kivijalka on ongelmien estäminen. Vaikka on täysin mahdotonta estää kaikkia mahdollisia uhkia toteutumasta, valtaosa ongelmista voidaan estää.
- Havainointi: kun järjestelmään murtaudutaan, on erittäin tärkeää, että tämä havaitaan mahdollisimman nopeasti. Näin pystytään rajoittamaan vahinkoja, mahdollisesti tunnistamaan hyökääjä ja korjaamaan aiheutuneet vahingot.
  - havaitseminen – turvaongelma vai sattumaa?
  - paikallistaminen – missä palaa?
  - tunnistaminen – kuka?
  - arviointi – miten vastataan?
- Vastaaminen: tuleeko esimerkiksi järjestelmät sulkea vai tuleeko enemmän tappioita kaupankäynnin katkeamisesta kuin hyökkäyksestä? Onko turvajärjestelyissä tai järjestelmien ylläpidossa syytä muuttaa tapoja?

Turvallisuus ↔ vaarattomuus

- Security ↔ safety
- Järjestelmän vaarattomuutta tutkittaessa, voidaan hyvin harvinaiset tapaukset jättää huomioimatta
- Turvallisuudessa pitää huomioida myös epätodennäköisiä yhteensattumia
  - hyökkääjä pyrkii saamaan järjestelmän nurin
  - menetelmä voi olla täysin arvaamaton
- Väärien positiivisten ja negatiivisten suhde oltava järkevä
- Absoluuttien turvallisuus tuhon alku (Titanic, Enigma)

Turvallisuuden viisi askelta

1. Mitä haluan suojata?
2. Mitkä ovat riskit?
3. Kuinka hyvin turvaratkaisu suojaa riskeiltä?
4. Mitä muita riskejä turvaratkaisu aiheuttaa?
5. Mitä kustannuksia ja kompromisseja ratkaisusta aiheutuu?

Iso paha Internet

- Televerkko
  - operoitu
  - yhteyksien kirjaus
  - muutamia, “luotettuja” osapuolia
  - hallinta- ja käyttäjäliikenne eriytetty[1]
  - äly verkkolaitteissa
- Internet
  - miljoonia liityntäpisteitä
  - ei (aina) yhteyksien kirjausta
    $\Rightarrow$ jäljittäminen vaikeaa
  - in-band hallinta
  - äly päätelaitteissa

Ongelmakohdat

- Operointi perustuu keskinäiseen luottamukseen

  DNS paikalliset valtuutukset
  $\Rightarrow$ mahdotonta varmistua oikeellisuudesta[2]

  reititys sisältää tiedon vaihtoa verkon rakenteesta ja vertaissuhteista
  $\Rightarrow$ liikennevirtojen muuttaminen mahdollista
- Hyödyt suuremmat kuin riskit
  $\Rightarrow$ tilanne voi muuttua Internetin merkityksen kasvaessa

Panostukset turvallisuuteen

- Toiminta keskittynyt *suoria tuloja* tuovaan toimintaan
- Turvallisuudesta ei välitöntä tuloa
  $\Rightarrow$ lasku laiminlyönnistä tullee “joskus” (vrt. vakuutukset)
- Oikea tasapaino ja prioriteetti turvapanostuksiin

Mitä kyselyt kertovat

Computer Security Institute & FBI: 528 yritystä, viranomaista, yhteisöä ja yliopistoa (USA)

- Yli puolet yli 1000 hengen yrityksiä, 28 % yli 10000
- 56 %:lla luvatonta käyttöä, 15 % ei tiedä
- 78 % internetistä, 18 % soittosarjasta, 30 % sisäisistä
- Useimmiten yksityinen häkkeri (82 %) tai työntekijä (78 %)
- Yhdysvaltalaiset kilpailijat (40 %)
- Myös vieraat valtiot (28 %) ja yritykset (25 %)
- Hyökkäystapahtumien määrä

lähde	1–5	6–10	11–30	31–60	>60	**??**
ulkopuolelta	46	10	13	0	0	31
sisäpuolelta	45	11	12	0	0	33

[1] Nykyisin yhteiskanavamerkinannon aikana. Aikaisemmin oli ohjaukseen käytetiin mm. tietyn taajuisia ääniä puhekanavassa, jolloin “phone phreak” onnistui.

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

- Eri hyökkäystyyppejä
  - järjestelmiin tunkeuduttu 36% organisaatioissa
  - 42 % DoS-hyökkäyksen kohteena
  - 59 % kannettava
  - 45 % työntekijän luvatonta käyttöä
  - 80 %:lla työntekijöitä “väärää sisältöä” hankkimassa
  - 82 % tietokoneviruksia
  - 45 % luvatonta käyttöä
  - 1 % aktiivista salakuuntelua
  - 6 % puhelinliikenteen salakuuntelua
  - 15 % taloudellisia väärinkäytöksiä
  - 21 % tietovarkauksia
- Suurimmat menetykset
  1. tietovarkaudet
  2. palvelunesto
  3. virus
- WWW-sivuihin pääasiassa vandalismia ja DoS-hyökkäyksiä
- 50 % ei raportoinut tapahtumista viranomaisille, yleensä vain epaikattiin reijät
  $\Rightarrow$ Negatiivisen julkisuuden riski (70 %)

`http://www.gocsi.com`

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
  - 2 – 12 % verkkoliikenteestä haitallista
  - sähköpostista vieläkin suurempi osa
- esim. VPN- ja autentikointipalvelut, nimipalvelu, DDoS-hyökkäysten orjakone

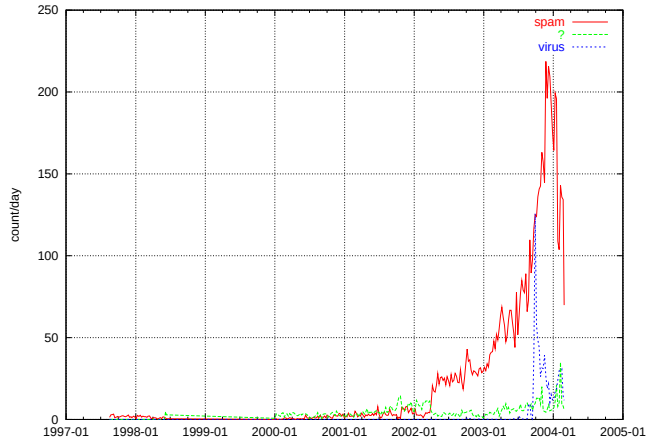
Tapahtumiin reagointi oltava suunniteltua

- hyökkäysten havainnointi
- hyökkääjien seuranta yhteistyössä

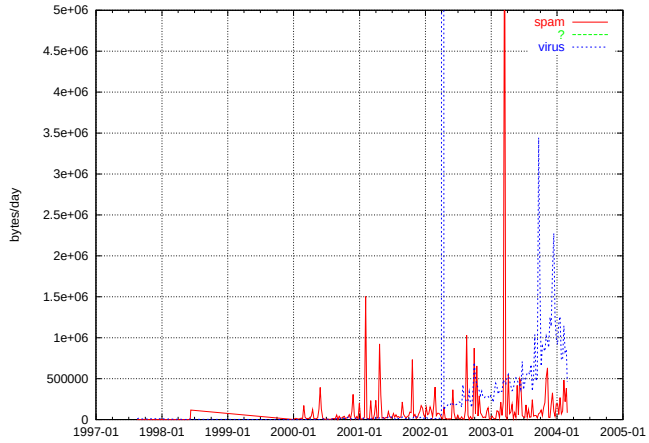
Viranomaisvaatimukset ovat minimi

- vaatimukset operoinnille
- avustus rikosten selvittämisessä

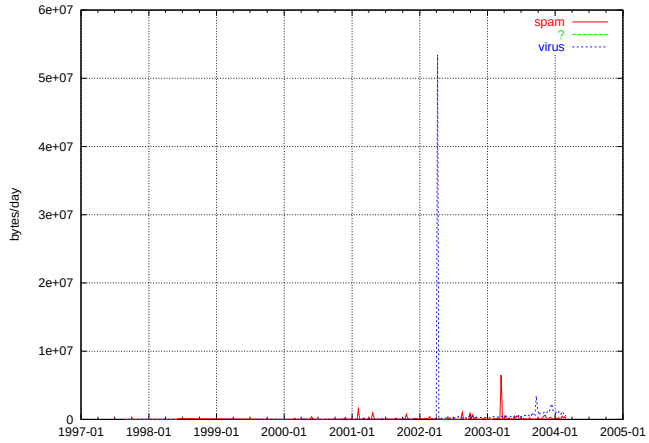
Roskaposti – kiusasta ongelmaksi



Roskaposti ja virukset – tavumäärä



Roskaposti ja virukset – tavumäärä



Mitä Suomen viranomaiset sanovat?

- Määräykset pohjautuvat vielä osittain “puhelinpalveluihin”
- Osittain IP-verkot huomioitu

Laki 565/1999 *yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta*

- tarvittaessa yhteistyössä
- turvataso “riittävä”
- kustannuksiltaan “kohtuullinen”
- tiedotettava tilaajille “erityisistä” riskeistä

6 § Teleyrityksen velvollisuudet

Teleyrityksen tulee huolehtia harjoittamansa teletoiminnan tietoturvasta. Teleyritysten tulee toteuttaa tarvittaessa yhteistyössä muiden teleyritysten kanssa turvataso, joka on tekniseen kehitykseen nähden riittävä ja kustannuksiltaan kohtuullinen.

Teleyrityksen on tiedotettava tilaajilleen telepalveluidensa turvallisuuteen liittyvistä erityisistä riskeistä sekä mahdollisuuksista niiden poistamiseen ja tähän liittyvien toimenpiteiden kustannuksista.

Ministeriö päättää tarvittaessa siitä, mitä on otettava huomioon kustannusten kohtuullisuutta ja turvatason riittävyyttä arvioitaessa.

THK 47/1999 M Teleyritysten tietoturvasta

- perustuu em. lakiin
- Viestintävirasto voi puuttua yrityksen toimintaan (uhkasakko tai toiminnan keskeytys)
- sakkoa laiminlyönneistä

Viestintävirasto 9 A/2003 M Tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa

- tietoturvaloukkaukset
  - tietomurrot teleyrityksen tietojärjestelmiin
  - hyökkäykset, joilla on vaikutusta televerkon palveluiden tai telepalveluiden käytettävyyteen
  - haittaohjelmien aktivoituminen teleyrityksen tietojärjestelmässä ja/tai televerkossa
  - yritykset saada teleyrityksen tai sen asiakkaiden tietoturvallisuutta vaarantavia tietoja teleyrityksen henkilöstöltä (nk. social engineering)
  - salakuuntelu- tai tarkkailu televerkossa tai järjestelmissä
- tietoturvaloukkausen uhat
  - merkittävät tietomurtoyritykset
  - tavallisuudesta poikkeava verkkoliikenne
  - järjestelmissä ja ohjelmistoissa havaitut huomattavat tietoturvan puutteet
  - laajat havainnot tunnetuista haittaohjelmista esimerkiksi sähköpostin liitetiedostoina
- vika- tai häiriötilanteet
  - yli tunnin kestäneet verkon toimintahäiriöt (puoli tuntia, jos vaikuttaa suureen määrän tilaajia)
  - tärkeän internetin peruspalvelun (posti-, nimipalvelin) yli puoli tuntia kestänyt häiriö

Viestintävirasto 48A/2003 M Viestintäverkon fyysisestä suojaamisesta

- murto-, palo- ja vesisuojaus

Viestintävirasto 30 D/2003 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*

Viestintävirasto 48A/2003 M: Viestintäverkon fyysisestä suojaamisesta

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

- verkkojen yhdysliikennepiste
- kansalliset juurinimipalvelimet
- teleliikennealuetason laitteet
- valtakunnallisen verkonhallinnan laitteita

Tärkeä tila vika häiritsee yli 5000 tilaajan liikennettä

- verkon tärkeä solmupiste
- palvelinhotelli
- postipalvelin, dhcp-palvelin
- 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

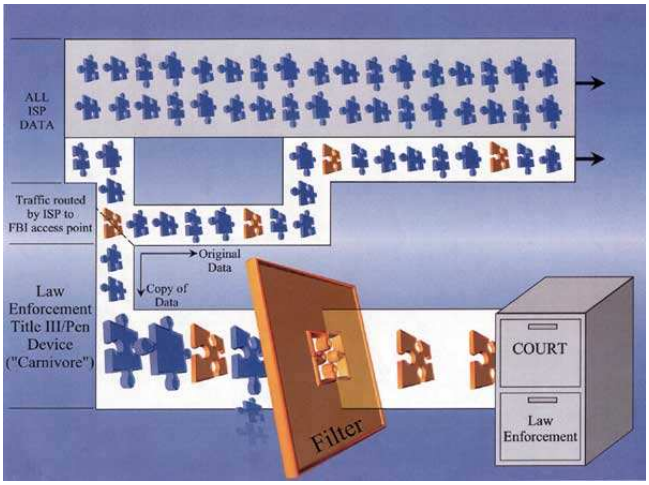
Erittäin tärkeiden tilojen lisävaatimukset

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

Carnivore & Echelon

Carnivore FBI:n salakuuntelulaite

- Liitetään operaattorin verkkon
- Suodatus aktivoidaan oikeuden päätöksellä



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

Echelon US, UK, CA, AU, NZ tietoliikenteen tarkkailujärjestelmä

- radioliikenteen tarkkailu kuunteluasemilla
- verkkoliikenteen salakuuntelu
- valtioturvallisuus, teollisuusvakoilu

Erityisesti Post-9/11…

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
- yleensä valitetaan "miksi tämä ei toimi"
  $\Rightarrow$ 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 [11]

TCP SYN flood (myös NAPTHA)

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

DDoS (hajautettu DoS)

- murrettuja[3] tietokoneita käytetään orjina
- suuri määrä dataa lähetetään tiettyyn kohteeseen

ISP:n turvalista[9]

- 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.

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

  - 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 [8] tulee käyttää autentikointia
  - reititystietojen suodatus ja vaimennus
  - lähdeosoitteen suodatus (ingress)[4]
    * vain osoitteet, joihin on *reitti* toiseen suuntaan, sallitaan. Eräissä reitittimissä yksi komento.
    * ongelmia *Mobile-IP*:n kanssa
    * myös asiakkaan suuntaan (egress)
      $\Rightarrow$ estää tekeytymisen asiakkaan verkossa olevaksi koneeksi
  - suunnattujen levitysviestien esto [11]

- 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)

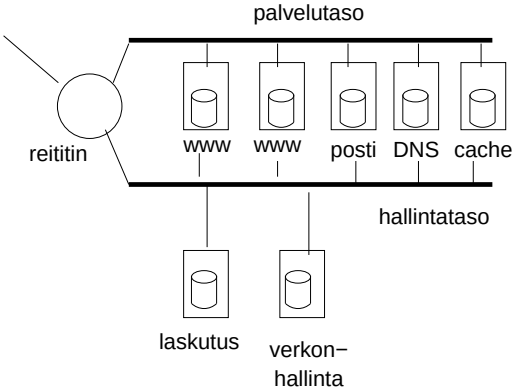
- Tärkeää tietoa sisältävät
  - laskutus
  - verkonhallinta

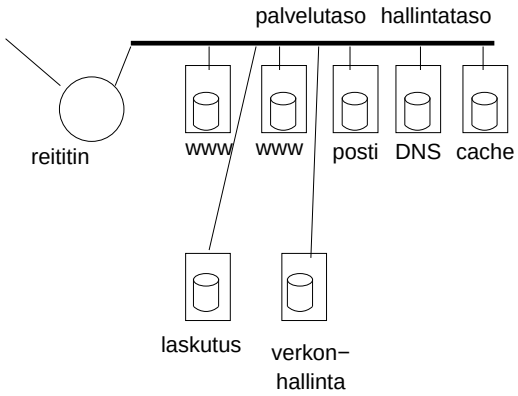
- Suuri liikennemäärä
  - sähköpostipalvelin (SMTP)
  - uutisryhmäpalvelin (NNTP)
  - WWW-käteispalvelin

- “Ohjelmoitavat” palvelimet
  - WWW-palvelimet
  - unix-palvelimet “shell”

Hallinnan ja palvelun eriyttäminen

- Liikenne ja hallinta eri verkoissa
  $\Rightarrow$ 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 (2001 lopussa yli 60.000 tunnettua, joista ainoastaan muutamia satoja on tavattu levinneinä “villinä”.)

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

Mato leviää itsenäisesti järjestelmästä toiseen verkon yli

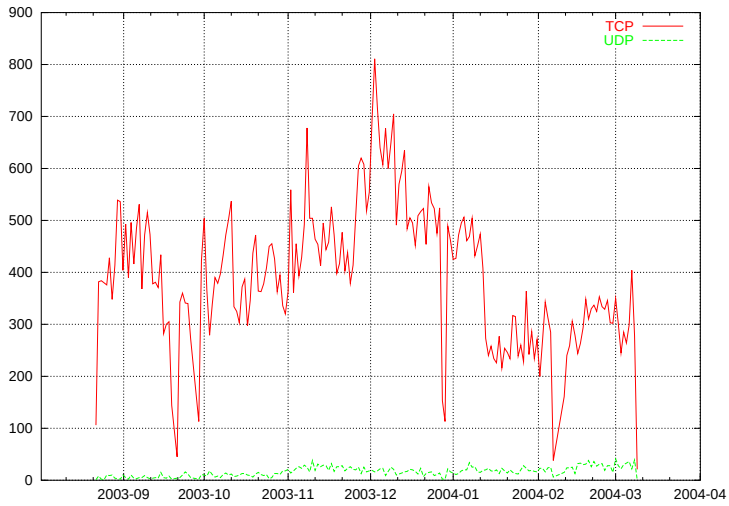
- voi heikentää myös verkon suorituskykyä
- CodeRed, Slammer

Troijan hevonen näennäisesti hyödyllinen ohjelma tai dokumentti jolla on salainen toimintatapa

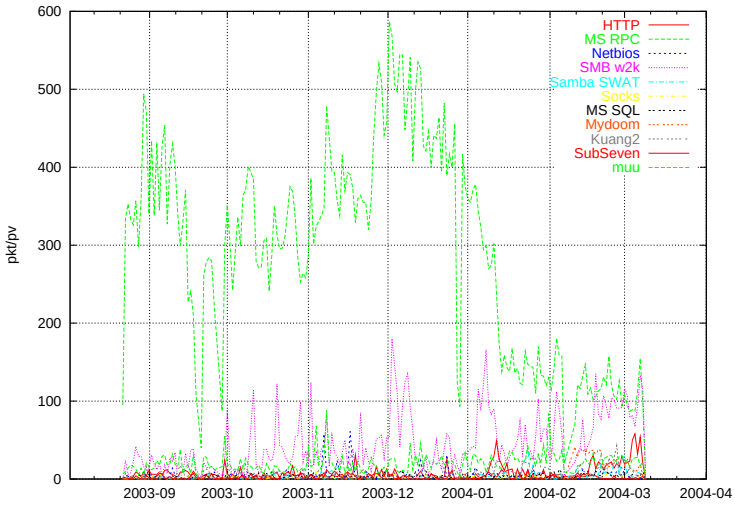
- voi esimerkiksi mahdollistaa murtautumisen koneeseen

- Kukin tyyppi voi
  - paljastaa tietoja, esim. lähtettämällä tiedostoja sähköpostise
  - tarkkailla käyttöä, esim. tallentaa salasanoja
  - mahdollistaa murtautuminen, esim. avaamalla takaportin
- Haittaohjelma voi olla myös *räätälöity* murtautumaan ainoastaan tiettyyn järjestelmään tai paljastamaan yksittäisen käyttäjän tietoja. Tälläistä haittaohjelmaa eivät normaalit virustorjuntaohjelmat välttämättä tunnista. Tämä on eräs tapa teollisuusvakoiluun.

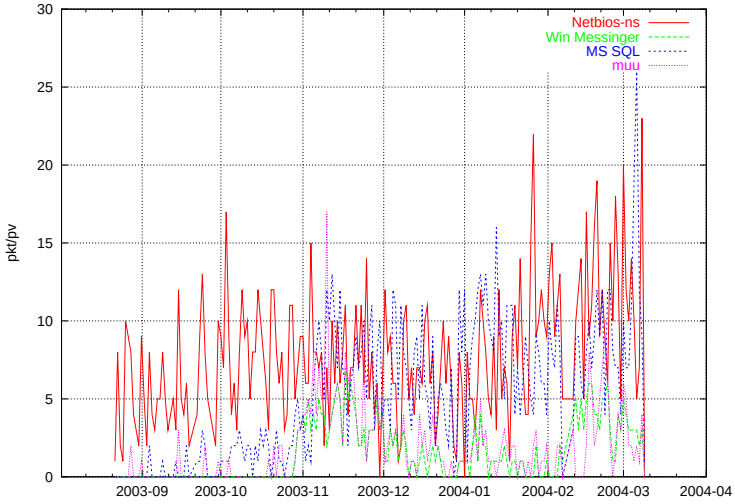
Haittaliikenteen määrä: ADSL-liittymä, ei konetta



Haittaliikennettä: TCP



Haittaliikennettä: UDP



Virusten/matojen “saavutuksia”

- Slammer (MS SQL-server 24.7.2002, 25.1.2003 mato liikkeelle)
  - Davie-Besse:n ydinvoimalan ohjausverkko toimintakyvyttömäksi, analoginen varmuusohjaus toimi (ja reaktori oli pois käytöstä huoltotöiden takia). Mato eteni VPN-yhteyden kautta erään alihankkijan verkosta voimalaoperaattorin verkkoon ja sieltä voimalan verkkoon — voimalan palomuuri oli konfiguroit pysäyttämään slammer, mutta siellä oli useita reittejä sen ohi.
  - Bank of America: 13.000 pankkiautomaattia toimintakyvyttömiksi
  - Washingon Mutual: 2.000 pankkiautomaattia, verkko- ja puhelinpankki
  - Canadian Imperial Bank of Commerce: Toronton pankkiautomaatit poissa käytöstä
  - Continental Airlines: lentojen viivästymisiä ja peruuntumisia: verkkolippuen ja sähköisen check-in toiminnan häidiöiden takia
  - Windows XP:n tuoteaktivointi ei toiminut verkkokuorman takia
  - Etelä-Korean suurimman ISP:n verkko pois käytöstä
  - Seattlen hätäkeskuksen (911) tietokoneet pois käytöstä
- Blaster (Windows RPC 16.7.2003, 11.8 mato liikkeelle)
  - Osatekijä Koillis-Yhdysvaltojen sähkökatkossa viiväestäen ja estäen diagnostiikkatietojen välittämistä keskukseen
  - 70-80 Nordea Pankin konttoria suljettu 14.8
  - 100 (1500:sta) partioauton tietokoneista saastui Jacksonville, FL
- Nachi (19.8.2003, paikkaa Blaster-haavoittuvuuden)
  - Air Canada: check-in:n hidastuminen
  - CSX Corporation: Itä-Yhdysvaltojen raideliikenteen ohjaus hidastui $\Rightarrow$junaliikenne pysähtyi

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
- Konekohtainen ohjelmistopalomuuri
  - ohjelmisto tarkkailee koneen liikennettä
  - mahdollistaa ohjelmapohjaisen valtuutuksen: ainoastaan nimetyt ohjelmat saavat liikennöidä tietyllä tavalla verkkoon
    $\Rightarrow$ hienojakoinen turvallisuus
    $\Rightarrow$ estää haittaohjelmia
  - turvallisuus riippuu koneen turvallisuudesta: esim. troijalainen voi kytkeä palomuurin pois päältä ennenkuin liikennöi verkkoon. Helppoa koneissa, jossa ei ole erillistä pääkäyttäjää (koti-windowssit), mahdollista myös paremmissa järjestelmissä, mikäli on paikallinen turva-aukko.
- Läpinäkyvyysvaatimus

> The introduction of a firewall and any associated tunneling or access negotiation facilities *MUST NOT* cause unintended failures of *legitimate* and *standards-compliant* usage that would work were the firewall not present.[6]

- Tuottaa helposti “kova ulkoa, pehmeä sisätä”-suojauksen
  ⇒ *kun* hyökkääjä saa ohitetua palomuurin, ei enää vaikeuksia

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”

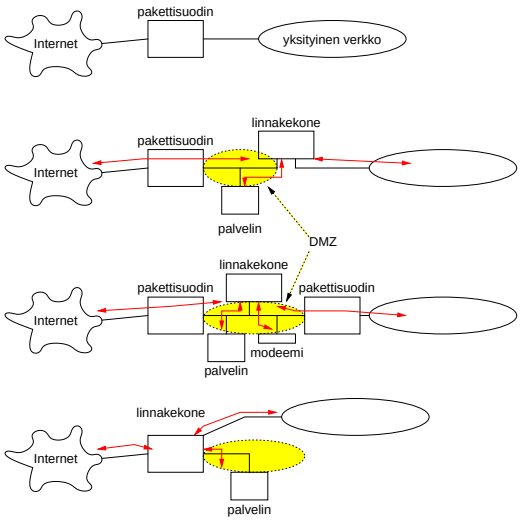
- läpinäkyvä (ei näy asiakaskoneelle) vs. konfiguroitava
- yhteyden “puolitus”
- vaatii suorituskykyä
- mahdollisuus analysoida dataa, esim. virustarkistus

Tilallinen tutkimus (dynaaminen pakettisuodatus)

- mahdollistaa tarkemman analysoinnin kuin pakettisuodatus
- suuret datamäärät mahdollista “laskea läpi”

- Monet tuotteet yhdistelmiä eri tekniikoista
- Useimmiten *hyvin konfiguroitu* pakettisuodin tarjoaa parhaimman suojan
  ⇒ palomuuri = reititin, jolla on asenne

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
          $\Rightarrow$ suuremmat hallintakulut, mutta pienempi riski ohjelmisto- ja laitteistovirheille
    - kuluista
2. Kasaa ja konfiguroi järjestelmä, järjestä tuki
    - onko järjestelmä turvallinen myös käynnistyessään
3. Testaa järjestelmä testiverkossa
4. Varmista, että turvallisuus ei riipu palomuurin toiminnasta
5. Ota käyttöön
    - ilmoita käyttäjille

Havainnointijärjestelmät

- IDS (Intrusion Detection Systems)-valvonta
    - tarkkailevat verkkoa passiivisesti
    - tarkoitus havaita hyökkäykset
    - tunnistavat hyökkäyksiä “sormenjälkien” perusteella
      $\Rightarrow$ vain tunnetut ongelmat havaitaan (vrt. virustorjuntaohjelmat)
    - usein turhan “meluisia” (liikaa vääriä positiivisia ja toisealta jää havaitsematta oikeita uhkia. Esimerkiksi suuren yrityksen IDS-järjestelmä voi antaa 3700 hälytystä vuorokaudessa, joista 48 vaatii lähempää tutkimista, joista 2 johtaa toimiin.)
- Hunaja-ansa: hyökkääjä ohjataan syöttiin, jolloin hyökkääjä paljastuu ja voidaan tarkkailla

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 taustapavelimiin (sovelluspalvelimet, tietokannat, hakemistot)
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
      $\Rightarrow$ johdon oltava takana
      $\Rightarrow$ työntekijöiden sitouduttava (oltava mukana määrittelyssä)
    - politiikkaa seurattava ja kehitettävä sekä noudattamista valvottava
      $\Rightarrow$ dokumentointi tärkeää
    - tarjoa säännöllisesti muistutus

Alihankkijat ja turvallisuus

- Usein tietojärjestelmiä hankitaan alihankkijoilta
- Näillä pääsy (asennuksessa) tietojärjestelmiin
  $\Rightarrow$ 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
    - monesti tioiminnan nopean jatkuvuuden ja todisteiden säilyttämisen ristiriita
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

Viranomaisyhteydet Suomessa

CERT-FI Viestintäviraston alaisuudessa toimiva ryhmä

Tietoturvaloukkausten havainnointiin, ratkaisuun ja ehkäisyyn tähtäävää yhteistoimintaa kansallisesti ja kansainvälisesti

`http://www.ficora.fi/suomi/tietoturva/certfi.htm`

Poliisi Rikosten tutkinta

Suojelupoliisi Vakoilu- ja tiedustelutoiminnan seuranta

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
  - etäkoneen eheys tärkeää
  - suojattava myös palomuurilla
- VPN-pohjainen ratkaisu tässäkin mahdollinen
- Käyttäjä integroituu yrityksen verkkoon
  ⇒ normaalit palvelut käytettävissä
  ⇒ etäkone mahdollisesti *väylä yrityksen verkkoon!* Palomuurisääntöjen lisäksi on huolehdittava myös VPN:n turvallisudesta.

Kuinka parantaa turvallisutta?

- Lisätään tekniikkaa
  - \- lisää monimutkaisuutta
  - \- järjestelmät jäykkiä ⇒ kierrettäviä
  - \+ lisää liikevaihtoa
- Vaaditaan parempi tunnistus
  - \- lisää monimutkaisuutta
  - \- virheellisten estojen määrä kasvaa
- Koulutetaan käyttäjiä
  - \+ motivoitunut käyttäjä erinomainen suoja
  - \- aina on onnistuttu hämäämään joitakin jonkinaikaa
  - – silti onnistuu, koska huijari vetooaa
    - vastavuoroinen auttaminen
    - auktoriteetti
    - sääli
    - “tiimipelaaja” — auta kaveria pulassa
    - ahneus
    - luottamusta pienin askelin

Yhteenveto

- Turvallisuuten auttaa
  - dokumentaatio
  - rutiinit
  - ajantasaisuus
  - uudistaminen
- Turvallisuus on monen asian summa
- Hyökkäykset muuttuvat ja muttavat pelin sääntöjä
- Turvallisuus on aina valinta ja kompromissi
- Tekniset järjestelmät kierrettävissä
  $\Rightarrow$ huolehdittava siitä, että järjestelmä ei romahda
  $\Rightarrow$ esim. roskapostiin löydettävä muu kuin tekninen ratkaisu

Hyviä lähteitä turvallisuusasioissa on mm.

- RFC2196 (FYI0008) Site Security Handbook [5]
- RFC2504 (FYI0034) Users' Security Handbook [7]
- RFC2828 (FYI0036) Internet Security Glossary [12]

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 2827, Internet Engineering Task Force, May 2000. (Best Current Practice) (Obsoletes RFC2267) (Also BCP0038). URL:`http://www.ietf.org/rfc/rfc2827.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] N. Freed. Behavior of and Requirements for Internet Firewalls. Request for Comments RFC 2979, Internet Engineering Task Force, October 2000. (Informational). URL:`http://www.ietf.org/rfc/rfc2979.txt`.

[7] E. Guttman, L. Leong, and G. Malkin. Users' Security Handbook. Request for Comments RFC 2504, Internet Engineering Task Force, February 1999. (Informational) (Also FYI0034). URL:`http://www.ietf.org/rfc/rfc2504.txt`.

[8] 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`.

[9] 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`.

[10] Bruce Schneier. *Secrets and Lies: digital security in a networked world*. Wiley Computer Publishing, 2000.

[11] D. Senie. Changing the Default for Directed Broadcasts in Routers. Request for Comments RFC 2644, Internet Engineering Task Force, August 1999. (Best Current Practice) (Updates RFC1812) (Also BCP0034). URL:`http://www.ietf.org/rfc/rfc2644.txt`.

[12] R. Shirey. Internet Security Glossary. Request for Comments RFC 2828, Internet Engineering Task Force, May 2000. (Informational) (Also FYI0036). URL:`http://www.ietf.org/rfc/rfc2828.txt`.