Tämä on luentorunko. Hakasulut [..] viittaavat muualta löytyvään aineistoon ja merkintä [→..] osoittaa, että vain luennolla on esillä jotain lisämateriaalia. Ensimmäisen tunnin aiheena ollutta johdantoa ja kertausta tässä ei ole. Järjestelyt yms. löytyvät muilta verkkosivuilta.

TLT-3301 Verkon tietoturva

Luennot lukuvuonna 2008–2009

TLT-3301 Verkon tietoturva, 1. luento 1.12.2008

Osittain kertausta:
- Tietoturvan prosessi
- Hyökkääjät ja hyökkäykset

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus (+muut ohjeistot)
Tietoturvapolitiikka
- Olemus, laadinta, sisältö

Lyhenteitä: **TT**=tietoturva(llisuus), **TTP**=TT:n perusteet, **TTJ**=TT:n jatkokurssi.
Linkit näiden materiaaleihin ovat muotoa http://sec.cs.tut.fi/maso/materiaali.php?id=**<numero>**. ¸

Tietoturvan prosessi

Tietoturva on suhteellinen prosessi samaan tapaan kuin esim. terveys, kuten jo peruskurssilla todettiin [id=28]. Jatkokurssilla oli esillä baseline-prosessi [id=357, → kaavio].

Wadlow'n prosessi, 15 kohtaa:

1 Opettele verkkoasi uhkaavista tekijöistä kaikki mahdollinen
2 Suunnittele mahdollisimman hyvin ennen kuin toteutat mitään
3 Tarkastele suunnitelmaasi "patologisesti", pahantahtoisesti, ja korjaa turvallisemmaksi.
4 Toteuta suunnitelman mukaan.
5 Tarkista toteutuksesi aika ajoin, ettei mikään ole muuttunut.
6 Harjoittele, jotta varmasti ymmärrät millainen toteutuksesi on ja jotta osaat käyttää sitä.
7 Tarkastele toteutustasi "patologisesti", pahantahtoisesti, ja korjaa turvallisemmaksi. ¸
8 Huolehdi siitä, että käyttäjien on yksinkertaista toimia niin kuin olet tarkoittanut.
9 Tee hankalaksi toimiminen vastoin sitä mitä haluat.
10 Tee itsellesi helpoksi havaita ongelmat.
11 Tee hankalaksi kätkeä asioita, joiden et halua jäävän piiloon.
12 Testaa kaikki minkä voit.
13 Harjoittele kaikki mitä voit.
14 Paranna kaikkea mitä voit.
15 Toista tätä prosessia loputtomasti kaikilla abstraktiotasoilla.

Motivaatiota voi heikentää, että on erittäin vaikea tietää, että prosessi toimii. Mutta kun tämän hyväksyy, voi keskittyä antamaan näyttöä kaikesta siitä mitä on tehnyt... (ei kylläkään riitä) ¸

Hyökkääjät ja hyökkäykset

Howard oli luonnehtinut hyökkäyksiä taksonomiassaan. Wadlow esittää hieman toisenlaisen jaottelun. Kumpikin on esillä peruskurssissa [id=30] ja niistä on nähtävissä käsitekartta. Seuraavassa taulukossa on Wadlow'n mukainen erittely siitä, mitä hyökkääjien erilaisuus vaikuttaa vastatoimiin. Taulukko tuo esiin myös kolme yleistä hyökkääjien erilaisuutta kuvaavaa attribuuttia: **taito**, **motivaatio** ja **tilaisuus**. Viimeinen on tosin piilossa lukumäärässä ja todennäköisyydessä ja siihen vaikuttaa tietysti myös kohteen suojaus. ¸

Erityyppisiä hyökkääjiä H, ja heidän luokitteluaan asteikolla 1 .. 5 pienestä suureen.

	Browsers, campers, vandals	Spies, saboteurs	Tyytymättömät (entiset) työntekijät, (yhteistyö)kumppanit
H:n lukumäärä	5	1 (yleensä)	riippuu yrityksestä
Hyökkäyksen tod.näk.	5	riippuu yrityksestä	3-5
H:n motivaatio	1-3	3-5	5
H:n taito	1-5	3-5	3-5
Vastatoimet			
	Älä tarjoa autentikoimattomia julkisia palveluita, jotka H voi vallata.	Näyttäydy ulospäin kohteena, johon hyökkääminen on vaarallista – eli siitä joutuu vastuuseen.	
	Tutki julkiset palvelusi aika ajoin.	Eliminoi tunnetut DoS-keinot.	Pidä työntekijät ja sopimuskumppanit tyytyväisinä.
	Eliminoi verkkoläsnäolostasi piirteet, jotka voivat houkutella.	Rajoita julkista tietoa turvatoimistasi.	Suunnittele erottamismenettelyt; yleensä ja turvatehtävistä erityisesti
	Pysy ajan tasalla hyökkäysmenetelmien suhteen. Varmistu ettei järjestelmäsi ole haavoittuva.*	Vartioi ydinliiketoimintaasi erityisen hyvin.	

* yksi harjoitustyön kohteista¸

Valtionhallinnon lähiverkkojen tietoturvallisuussuositus

VAHTI-suositus 2/2001 on Valtionhallinnon lähiverkkojen tietoturvallisuussuositus ja se soveltuu yleisempäänkin käyttöön, kun viraston sijasta tarkastellaan yritystä. Tämä suositus on osa kurssivaatimuksia, vaikka sitä ei suoraan käsitelläkään tämän kerran jälkeen. Kun vastaavia asioita tulee luennoissa esille muista lähteistä, kuulijoiden/lukijoiden toivotaan vertaavan niitä suositukseen ja tekevän mahdollisia täydennyksiä suuntaan tai toiseen. Suosituksen keskeisten lukujen aiheet ovat:

2 Suojattavat kohteet
3 Uhat ja turvallisuustarpeet
4 Tietoturvallisuustoimenpiteet osa-alueittain (17 sivua)
5 Poikkeusoloihin varautuminen
6 Virastokohtaisten erityistoimenpiteiden suunnittelu ja toteutus
7 Suositusten toimeenpano ja valvonta¸

Keskeiset suositukset ovat tiivistelmän ja luvun 7 mukaan, edelleen tiivistettyinä seuraavat:

1. nimetyt lähiverkon **vastuuhenkilöt**, joiden **tausta** on asianmukaisesti selvitetty.
2. voimassa ja ajan tasalla oleva **tietoturvapolitiikka** sekä tietoturvallisuuteen liittyvät perusturvallisuus-, jatkuvuus- ja valmiussuunnitelmat.
3. lähiverkon kokoonpanon ja asetusten **kuvaus** sekä verkkoon kuuluvien suojattavien **kohteiden yksilöinti**
4. lähiverkkoa ja sen käyttöä koskeva **riskianalyysi**,
5. riskianalyysin perusteella **johtopäätökset** ja **kontrollien valinta** lähiverkon turvaamiseksi (riskianalyysissa otetaan huomioon nykyisin käytössä olevat kontrollit)

6. **toimenpideohjelma** kontrollien toteuttamiseksi: tarvittavat toimenpiteet, aikataulut, työmääräarviot, kustannusarviot, toteutuksesta vastaava henkilö ja toteutuksen edistymistä valvova henkilö.
7. suosituksessa esitettyjen toimenpiteiden **valvonta** (oma jatkuva sekä ei-oma ulkoinen ja sisäinen)
8. lähiverkon tietoturvallisuuden **kehittäminen ja ylläpitäminen** muuttuvien vaatimusten mukaisesti.

Termiä kontrolli eli valvontatoimenpide käytetään myös TT-toimenpiteen tai -mekanismin synonyyminä.

Suosituksen luku 4, Lähiverkon tietoturvallisuustoimenpiteet osa-alueittain

Suluissa on alakohtien lukumäärä.

Hallinnollinen tietoturvallisuus
- Yleiset periaatteet (17)
- Dokumentaatio (3)

Henkilöstöturvallisuus
- Lähiverkon vastuuhenkilöt (2)
- Lähiverkon käyttäjät (2)

Fyysinen turvallisuus
- Kulunvalvonta (3)
- Laite- ja kytkentätilat (5)
- Asiakaspalvelutilat (4)
- Sähkönsyöttö (1)

Tietoliikenneturvallisuus
- Verkon perusrakenne (11)
- Lähiverkkojen liittäminen toisiinsa (1)
- Lähiverkkojen liittäminen ulkoisiin verkkoihin ja etäyhteydet (5)
- Verkon komponentit (7)
- Tiedonsiirtomedia ja kaapelointikanavat (7)

Laitteistoturvallisuus
- Palvelimet (4)
- Levyjärjestelmät (2)
- Työasemat ja verkon muut komponentit (5)

Ohjelmistoturvallisuus
- Työasemat (2)
- Palvelimet ja verkon muut komponentit (1)

Tietoaineistoturvallisuus
- Tiedostojärjestelmien valinta (1)
- Tiedonsiirron salaus (3)
- Palvelimet, työasemat ja lähiverkon muut komponentit (3)

Käyttöturvallisuus
- Pääsykontrollit: käyttöoikeudet ja -valtuudet (15)
- Verkon hallinta ja valvonta (16)
- Varajärjestelyt ja toipuminen (11)
- Virustorjunta (1)
- Tulostaminen (3)

Muut ohjeistot + esim.

Tällä kurssilla käsitellään ja edellytetään luettavaksi oheistoja:

– Valtion tietohallinnon *Internet-tietoturvallisuusohje*, VAHTI 1/2003
– Valtionhallinnon *lähiverkkojen* tietoturvallisuussuositus, VAHTI 2/**2001**
– Turvallinen *etäkäyttö* turvattomista verkoista, VAHTI 2/2003
– Valtionhallinnon *etätyön* tietoturvallisuusohje, VAHTI 3/**2002**
– *Tietoturvapoikkeamatilanteiden* hallinta, VAHTI 3/2005
– Valtionhallinnon *sähköpostien* käsittelyohje, VAHTI 2/2005
– Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006
– Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006
– kevään 2004 *IDS-seminaarin* ja kevään 2005 *DoS-seminaarin* aineistoa. ¸

TTJ-kurssilla on jo luettu seuraavia, joita ei kannata unohtaa:
– Sähköisten *palveluiden ja asioinnin* tietoturvallisuuden yleisohje, VAHTI 4/2001
– Valtionhallinnon *tietoaineistojen* käsittelyn tietoturvallisuusohje, VAHTI 2/2000
(+ Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje, VM 19.1.2000)
– Arkaluonteiset kansainväliset tietoaineistot, VAHTI 4/2002
– Tietoteknisten *laitetilojen* turvallisuussuositus, VAHTI 1/2002
– Valtion *tietotekniikkahankintojen* tietoturvallisuuden tarkistuslista,VAHTI 6/2001
– Valtionhallinnon *salauskäytäntöjen* tietoturvaohje VAHTI 3/2008
– *Haittaohjelmilta* suojautumisen yleisohje, VAHTI 3/2004

Luettelo ja linkit ohjeisiin löytyvät TTJ-sivuilta [id=480]. ¸

Tarkastellaan muutamaa esimerkkiä (lähi)verkon rakenteista
Valtion tietohallinnon Internet-tietoturvallisuusohjeen (VAHTI 1/2003) mukaisesti
[kuvat sivuilla 38, 47, 58]. Kyseinen ohje on hyvää luettavaa tälle kurssille. Se asettuu abstraktisuudeltaan luentojen ja harjoitusten väliin (joka onkin aika suuri). Luku 2 (s. 11–41) kertaa internetin tekniikkaa, ja luku 3 (s. 43–82) käsittelee tarkemmin tietoturvaa. ¸

Tietoturvapolitiikka (TP)

[Wadlow Ch. 2 & Allen (Liite B)]

Olemus

TP on ollut monesti esillä aiemmilla kursseilla. **Lähiverkon TT-suosituksen** (vrt. edellä) mukaan:

> Virastossa pitää olla voimassa ja ajan tasalla oleva TP, joka on viraston johdon hyväksymä ja vahvistama. Riskien analysointiin pohjautuen ja TP:tä noudattaen pitää laatia *tietoturvallisuussuunnitelma*, joka kattaa lähiverkon tietoturvajärjestelyt. Lisäksi pitää olla tietoturvallisuuteen liittyvät *perusturvallisuus-, jatkuvuus- ja valmiussuunnitelmat*.

¸
TTJ-kurssissa määriteltiin:

> Jos tietojenkäsittelyjärjestelmä ajatellaan äärellistilaiseksi automaatiksi,
> **TP** kertoo, mitkä tilat ovat turvallisia ja mitkä eivät.
>
> **Järjestelmä** on turvallinen, jos mikään tilasiirtymä ei voi viedä sitä turvallisesta tilasta turvattomaan - eli ei voi tapahtua **turvaloukkausta**. Sama järjestelmä voi yhden TP:n mukaan olla turvallinen ja toisen mukaan turvaton.
>
> TP:n toteuttaminen tarkoittaa turvaloukkauksien välttämistä. Käytännössä siihen tarvitaan erityisiä välineitä, jotka voi olla rakennettu osaksi järjestelmää: **Tietoturvamekanismi** on olio tai järjestely, joka pakottaa jonkin osan TP:tä toteutumaan, eli estää tiettyjä loukkauksia.

¸

Wadlow antaa ymmärtää, että turvapolitiikka on tärkein yksittäinen asia verkon turvaamisessa. Sillä on seuraavanlaisia **tarkoituksia:** Se

- kertoo, mitä turvataan ja miksi.
- määrittelee, mistä aloitetaan ja millä kustannuksilla.
- on samalla organisaation osien välinen sopimus turvallisuuden merkityksestä.
- antaa turvahenkilöstölle syyn, perustelut ja oikeutuksen "ei"n sanomiselle tietyissä tilanteissa – ja auttaa heitä myös välttämään ylireagointeja.

TP:n laadinta ei ole yksinkertainen asia – syynä monet kiireisemmät työt, päätöksenteon mutkikkuus – jopa se mitkä tahot haluavat omia/välttää politiikan laadinnan. Lisäksi täydellinen TP on erittäin monimutkainen ja laaja.

Silti on tärkeämpää, että TP

- on olemassa kuin että parempi olisi vasta tekeillä.
- on tietoisuudessa eli jaeltu ja luettu, vaikka se ei olisikaan niin vahva kuin voisi.
- on ymmärrettävissä, vaikka se olisikin turhan yksinkertainen.
- sisältää yksityiskohtia vaikka osa niistä ei olisikaan vielä kohdallaan.
- ei jää ajastaan jälkeen vaikka se tarkoittaisikin taajaa muuntelua.

Allen esittää pitemmän luettelon vaatimuksia tehokkaalle TP:lle [s. 398]. Luettelon 13 kohtaa on tässä koottu ja jäsennetty. Ensinnäkin TP:ltä vaaditaan vastaavia ominaisuuksia kuin Wadlow'n listassa: TP:n pitää olla

- selkeä, johdonmukainen,
- hyvin määritelty, ymmärrettävä,
- realistinen, toteutettavissa ja omaksuttavissa oleva,
- ajantasainen ja hyväksytty.

Hyvin määritelty ei ole suoraan sama asia kuin selkeä ja ymmärrettävä, vaan se tarkoittaa käsitteellistä johdonmukaisuutta lakitekstin (tai matematiikan) tapaan. Listassa *johdonmukainen* viittaa enemmänkin TP:n käytännön johdonmukaisuuteen. Vastaavasti *ymmärrettävä* ja *realistinen* ovat eivät vielä takaa, että TP olisi *omaksuttavissa* ja *toteutettavissa.* Eikä näistä jälkimmäisistä ominaisuuksista seuraa suoraan edellisiä. Siihen, että TP on hyvin määritelty, liittyy vaatimus että TP olisi

- laajasti käytössä olevien standardien, ohjeiden ja menettelytapojen tukema.

Luettelossa on muutama TP:n sisältöön liittyvä vaatimus:

- TP:n pitää perustua rooleihin ja olla siis riippumaton virka-asemista
- TP:ssä pitää määritellä vastuunjako, ja lisäksi on syytä
  antaa ylläpitäjille erikoistilanteisiin laajennetut valtuudet, mutta normaalisti
  poistaa ylläpitäjiltä vastuun sellaisista riskeistä, jotka eivät heille kuulu.

Lopuksi, luettelon ensimmäinen vaatimus esittää, että TP:n tulisi

- olla pitkän tähtäimen tavoitteiden mukaisesti suunniteltu.

Politiikan laadinta

Wadlow esittää seuraavan **mallin**, jolla TT-vastaava voi saada aikaan kelpo politiikan ilman hankalaa ja hidasta virkatietä ja etukäteistä konsensuksen etsintää. Vaikka johdon tuki tässä mallissa muodostuu vasta "de facto" -politiikalle tai sen muunnokselle, tällä tavoin päästään ainakin liikkeelle jos TP alun perin puuttuu tai on aikansa elänyt.

1. **Laadi** sellainen TP, jonka saat aikaan parissa päivässä omin voimin,
esim. viikonloppuna jolloin ei ole häiriöitä.

Pituuden ei tulisi ylittää viittä sivua.

2. **Hanki** "turvakomitea" – organisaation eri tahoilta kolme henkilöä, joille TP on tärkeä.
Heidän tehtävänsä on tulkita ja täydentää/korjata TP:tä.
Heidän pitäisi voida kokoontua parin kuukauden välein. ¸

3. **Julkaise** TP yrityksen sisäisillä verkkosivuilla, ja päivitä sinne tulkinnat ja täydennykset.
Sivulla neuvotaan ottamaan yhteyttä turvakomiteaan, jos tarkennuksia tarvitaan (ks. kohta 4). Turvakomitea ei kuitenkaan ole lainkaan vastuussa politiikan toteuttamisesta.

4. **Toteuta** politiikkaa täydennyksineen kuin ne olisivat laki – siis kaikissa TT-vastaavan toimissasi. Johtokin huomaa tämän ennen pitkää.
Jos politiikka ei heidän mielestään ole hyvä, pidä huoli vain siitä,
että tilalle tulee jotain muuta sen sijaan, että TP pyyhittäisiin olemattomiin.
Tätä kautta on mahdollista saada johto sitoutumaan politiikkaan tai
ainakin pitämään se käytännössä voimassa. ¸

5. Vastaavasti jos kenellä tahansa on TP:n suhteen ongelmia,
pyydä häntä kirjoittamaan **ehdotus tulkintaohjeeksi tai täydennykseksi** – enintään sivun mittainen.
Se otetaan käyttöön, jos vähintään kaksi komitean jäsentä hyväksyy sen.

6. Kerran vuodessa muokkaat ja tiivistät TP:n muutoksineen **uudeksi TP:ksi**,
jonka alistat komitean hyväksyttäväksi. Palaa kohtaan 3. ¸

Politiikan sisältö

Wadlow'n mukaan tiivistettynä politiikassa on seuraavat viisi pääkohtaa.
(Oikeastaan nämä kohdat ovat sellaisia, joiden sisällyttämistä TP:hen Wadlow *suosittelee*.)

1. **Mitä turvataan:**
Verkon laitteet kannattaa luokitella turvatasoihin. Niiden avulla voidaan muissa kohdissa määritellä, keillä (ja millä) on pääsy laitteisiin ja miten usein laitteen turva-asetukset pitää tarkistaa.
Sanastona voi käyttää vaikkapa värikoodeja (pu-ke-vi-va-mu).
(Varsinaisiin monitasoisen turvan malleihin tässä ei silti tarvitse mennä).

2. Mikä on eri tahojen turvaintressien **prioriteetti**:
melko ilmeinen järjestys:
ihmisten henki ja terveys — lait ja säännökset — organisaation tietoturvatavoitteet — yrityskumppanien tavoitteet — vapaa tiedonvälitys. ¸

3. **Vastuut ja oikeudet**: jaottelu eri tahoille:
kaikki ‖ ylläpitäjät ‖ TT-vastaava ‖ sopimuskumppani ‖ vieraat

4. **Asianmukainen käyttö**:
Miten työntekijöiden pitää ja miten he eivät saa käyttää verkkoa. (Vastaavat roolit kuin 3:ssa)

5. **Seuraamukset**:
Miten määritellään turvaloukkauksen vakavuus (esim. asteikolle kriittinen, vakava, rajattu),
millaiset seuraamukset rikkojalle aiheutuu. Seuraamusten asettamista varten voidaan tarvita esim. Turvalautakunta, jossa on vähintään kolme johtajatason henkilöä. ¸

Allenin kirjan liite B kokoaa n. 20 sivulle kaikki kirjassa esitetyt politiikkamääritykset.

Niiden otsikot ovat kutakuinkin samat kuin kirjan alalukujen X.Y otsikot,
sillä useimmat alaluvut päättyvät suosituksiin siitä,
miten tekstissä käsitellyt asiat tulisi sisällyttää TP:hen.
(Tämän lisäksi jokaisen pääluvun X lopussa on taulukkomainen luettelo luvussa esitetyistä toimenpiteistä, jotka ovat suurinpiirtein samat kuin lukujen X.Y.Z otsikot, sillä ne ovat lähes kaikki muotoa *Tee jotain*).

Allen luonnehtii TP:n sisältöä myös yleisemmällä tasolla esittämällä
15-kohtaisessa luettelossa esimerkkejä aiheista,
joita kattava TP (”tietotekniikkaturvapolitiikka”) sisältää [Allen s. 399].
Luettelo ei vaikuta olevan minkäänlaisessa loogisessa järjestyksessä,
mikä sopinee korostamaan sen esimerkinomaisuutta. Siinä suhteessa sitä voi verrata
harjoitustyöohjeen vastaavaan aakkosjärjestyksessä olevaan luetteloon,
joka on liki kolme kertaa pitempi. ¸

Seuraavassa on Allenin luettelo alkuperäisin numeroin mutta yhdellä tavalla järjestetyssä muodossa, ja neljään ryhmään jäsennettynä. Osittelua lienee mahdoton tehdä täysin osuvasti, mutta todennäköisesti jollain logiikalla jäsennelty politiikka on selkeämpi kuin aakkosjärjestyksessä esitetty.

1. Tietokoneiden hankinta
14. Resurssit
3. Saantioikeudet – ainakin etuoikeudet
5. Valtuutukset

9. Saatavuus
13. Vikasietoisuus
10. Verkkoliikenne
12. Tietoliikenneyhteydet

7. Tunnistaminen
6. Autentikointi
2. Yksityisyys
4. Seurattavuus
8. Auditointi
11. Tietoturvaloukkauksista raportointi

15. Riskien vähentäminen

TLT-3301 Verkon tietoturva, 2. luento, 3.12.2008

Suunnitteluprosessista [Wadlow Ch. 4]
Turvasuunnittelun periaatteita; suojamekanismit
Henkilöstö [Wadlow Ch. 5 & 7]
turvallisuushenkilöstö; muu h.
Toimilaitteiden turvaaminen: [Wadlow Ch. 6, Allen Ch. 2]
työasemat, verkkopalvelimet (paitsi www), verkon toimilaitteet;
hankinta, asennus, päivitys.
Tietoturvan arvostaminen [Wadlow Ch. 11]

Kertaavia näkökulmia:
Turvallisuus "evoluutiona" – prosessina – taiteena eikä tieteenä – oikeina vastauksina¸

Turvasuunnittelusta

Tässä ei kuvata suunnitteluprosessia, vaikka lähteenä onkin Wadlow'n luku *Security Design Process.* Siitä aiheesta oli ensimmäisellä luennolla. Tässä esitetään ensin kokoelma periaatteita, joista on hyötyä prosessissa. Toiseksi luonnehditaan verkon turvajärjestelyjä vastaavanlaisella periaatetasolla.

Yleisiä periaatteita

Tässä on joitakin iskulauseita mielessä pidettäviksi turvasuunnittelun yhteydessä.

Jos et tiedä mitä olet puolustamassa ja miksi, et voi onnistua. Tämä on muistutus politiikan merkityksestä. Politiikkaa laadittaessa tavoiteltavia ominaisuuksia:
ymmärrettävyys
relevanssi
jostain on vaiettava
purevuus
ajankohtaisuus
oikea jakelu
kriisi on huonoin aika periaatepäätöksille, mutta siihen kannattaa varautua.
Tarvitaan siis myös ylemmän tason politiikka.¸

Turvallisuus ei ole koskaan absoluuttinen suure. Se suhteutuu erityisesti hyökkääjän taitoon, motivaation ja tilaisuuteen ....

Ihmiset tekevät virheitä. Suunnittelijan virheiden vaikutusta voi torjua monikerroksisella turvaamisella. Hyökkääjän virheiden varaan ei voi laskea mutta niitä kannattaa käyttää hyödyksi. Erityisesti niiden perusteella voi ehkä päätellä, onko hän ulko- vai sisäpuolinen. Valmistajan virheiden vaikutusta voi vähentää tekemällä itse testauksia.

On yli puoli voittoa tietää olevansa hyökkäyksen kohteena. *Passiiviset torjuntamekanismit* ovat sellaisia, joissa tietoa ei tule torjunnasta eikä sen epäonnistumisestakaan suoraan. Silti mahdollisimman suuri osa hyökkäyksistä kannattaa torjua tällaisilla keinoilla. Läpi päässeet pitää havaita ja raportoida ja sitten niin pian kuin suinkin katkaista *aktiivisilla menetelmillä* – erityisesti estämällä yhteydet kyseisestä osoitteesta.¸

Puolustaudu sekä hyökkäystä että hyökkääjää vastaan. Passiiviset menetelmät ovat edellistä ja aktiiviset jälkimmäistä varten.

Taistelu on harjoitusta ja kääntäen. Erityisesti siis harjoitella pitää silloinkin kun hyökkääjää ei ole mukana.

Hyvät komponentit eivät pelasta, mutta huonoista on varmasti haittaa. Keskeisten laitteiden ja ohjelmistojen päivitystarve kannattaa tarkistaa ja toteuttaa aika ajoin.

Ruoste ei lepää. Ilmeinen toteamus, joka ilmenee usealla tavalla: Vanha systeemi on monen tiedossa. Vähäinen huomio helpottaa kaikenlaisia asiattomia muutoksia. Harvoin tapahtuva käsittely vaikeuttaa operointia. ¸

Turvallisuus on jokaisen asia. Turvatietoisuudeksi muutakin kuin hankaloittavuus...

Jos turvallisuus on ristiriidassa liiketoiminnan kanssa, se todennäköisesti jää toiseksi.

Käytä luottamusta viisaasti. Työhönotto on ensimmäinen vaihe luottamuksen rakentamisessa. Suunnittele niin, että väärin kohdistettu luottamus ei aiheuta kovin suurta vahinkoa.

Turvallisuus on näkökulmakysymys. Tällä toteamuksella on kolmenlaista sisältöä: Hyökkääjälle on haitaksi, jos hän ei tiedä kaikkea verkosta. Sama pätee puolustajaan. Lisäksi puolustaja tai suunnittelija saattaa olla sokea omille virheilleen. Hänen kannattaa hakea muilta henkilöiltä uutta näkemystä verkkoon ja sen turvamekanismeihin. ¸

Puolustusmekanismien yleisjaottelu

Passiiviset, ulkoiset. Tunnettujen hyökkäysten torjunta. ”Ulkoisia”, mutta silti monitasoisia, esim. reitittimet estävät jonkin liikenteen, jota vastaavaa palvelua ei ole käynnistetty eikä edes asennettu.

Aktiiviset, sisäiset. Näillä voi muuttaa pelin ”sääntöjä” kesken ottelun.

Passiivinen seuranta, erityisesti lokitietojen kerääminen.

Aktiivinen seuranta, inhimillinen tarkkailu. Puuttuvaksi luultua palvelua ei kukaan ehkä satu edes yrittämään pitkiin aikoihin. Vain aktiivisuudella voi tarkistaa, voisiko yritys onnistua. ¸

Näiden kerrosten sisällä on **varsinainen verkko**, joka ei sellaisenaankaan saisi olla suojaton. Tämä tarkoittaa noin kolmea asiaa:

- käyttäjähallinta ja autentikointi ovat kunnossa,
- verkon rakenteessa on rajoitettu tarpeetonta näkyvyyttä ja luottamusta (esim. aliverkkojen avulla) ja
- fyysinen turvallisuus on kunnossa esim. kaapelointien ja laitetilojen osalta.

Mekanismien asettuminen sisäkkäin edustaa **kerrospuolustusta** (’defense in depth’), jota myös Northcutt ym. korostavat kirjassaan. ¸

Turvallisuushenkilöstö

Antti Sulosaaren diplomityössä ”Tietoturva-ammattilaisen osaamistarvekartoitus” (2005, http://www.iki.fi/antti.sulosaari/, ks. luku 3) haetaan kirjallisuudesta erilaisia profiileja ja todennetaan näitä haastattelujen kautta. Lähteinä on

- Juha E. Miettisen Yritysturvallisuuden käsikirja (2002)
- TaY:n silloisen tietoturvapäällikön Minna Mannisen esittämä jaottelu (2004)
- Whittmanin ja Mattordin kirja ”Principles of Information Security” (2005)
- Wadlow’n kirjan jaottelu (jota käsitellään jäljempänä)
- BS7799-standardi
- VAHTI-ohjeisto¸

Mikä on yhteistä? Se, ettei synny suurta yhtenäistä teoriaa. Tehtävät jakautuvat eri tasoille, eri tahoille, erilaista osaamista vaativiin, erilaisiin ryhmiin jne. Monet nimikkeet luonnollisesti toistuvat eri jaotteluissa. Esimerkiksi Miettisen esittelemät *yritysturvallisuuden* asiantuntijaprofiilit ovat johtaja, esimies tai päällikkö, tutkija, erikoisasiantuntija ja suoritetyöntekijä. Kaikkia heitä voi esiintyä myös verkon tietoturvaan liittyvissä tehtävissä.

Mielenkiintoinen havainto ehkä on se, että TT-työläisten taustassa TTY:n kaltainen ammattiaine on harvinainen. Enemmistön muodostavat erilaisissa IT-ammateissa työskennelleet. ¸

Tehtäväalueet

Organisaatiossa on yleisesti seuraavankaltaisia tehtäväalueita, vaikka ne voivatkin henkilöiden toimenkuvissa mennä päällekkäin:

Vartio 24/7, valvontajärjestelmän tarkkailu ja muut rutiinitehtävät.

Vasteryhmä, reagoi nopeasti ja päättäväisesti. Vastaa myös turvasuunnittelusta hyökkäysten ja muualla tapahtuneen kehityksen perusteella.

Jäljitysryhmä, reagoi perusteellisesti ja huolellisesti (forensics team)

Näiden lisäksi on työntekijöiden **koulutustehtävä**.¸

Täsmällisempi tehtäväluettelo

Tässä on yhdenlainen ryhmittely suurelle joukolle tehtävänimikkeitä ja tehtäviä, jotka Wadlow luettelee aakkosjärjestyksessä (!). Näiden lisäksi voisi vielä olla esim. jatkuvuussuunnitteluryhmä, joka tosin varmasti koostuisi muiden tehtävien suorittajista.

– **Turva-arkkitehti**, kaikkien turva-asioiden koordinaattori; kehittää uusia politiikkoja.

– **Sisäinen auditoija**: tarkkailee, että organisaation järjestelmät vastaavat suunnitelmia; on mukana suunnittelemassa järjestelmien spesifikaatioita; johtaa järjestelmäpäivityksiä ja -korjauksia tietoverkkoasiantuntijoiden kanssa.

– Turva**operaatioiden** päällikkö (yhteys tietohallintoon)
– Turvaoperaattori, päivittäistoiminnot, kuten oikeuksien päivitys¸

– **Kehitys**päällikkö (yhteys turva-arkkitehtiin)
– Kehitysinsinööri (integroi tuotteet ja kirjoittaa omaakin koodia)
– Autentikoinnin järjestelyt
– Lokitietojen keräämisen järjestelyt

– Isäntäkoneiden **turvaaja** (yhteys yleisen tason ylläpitäjiin)

– Verkon turvaaja: verkkoturvan suunnittelu ja toteutus
– Fyysinen turvaaja (mm. avaimet, kulkuluvat ja henkilökortit)

– **Vaste**päällikkö
– Vartija-tarkkailija (myös standardivaste)
– Dogfighter, varsinainen kärkitaistelija (+ensivaiheen vahinkojen kontrolli)
– Tason 1 vaste, — lajittelu vakavuuden mukaan ('triage on sec. incidents')
– Tason 2 vaste (pitempään kestävä loukkausten käsittely kuin tasolla 1)
– Vahinkojen arviointi ja korjaus (toinen vaihe) ¸

– **Jäljitys**päällikkö (Forensics team manager)
– Jäljitysanalyytikko (mm. selvittää tunkeutumisten menetelmiä)
– Lainvalvoja – yhteys viranomaisiin

– **Dokumentointi**päällikkö
– Dokumentoija
– Politiikan ja käytäntöjen hallinta (yhteys henkilöstöhallintoon)

– Sisäinen **tiedottaja** ('communications')
– Ulkoinen tiedottaja, yhdyshenkilö ('press liaison')

– **Tutkija**, myös kouluttaa.

– **Ylläpitäjä** turvatiimin omille järjestelmille (erillinen tehtävä yleiseen ylläpitäjään verrattuna, koska turvajärjestelmien omat turvavaatimukset ovat suuremmat kuin yleiset)¸

Mistä turvatiimin jäsenet saadaan ja miten heistä päästään eroon

Yleinen luotettavuus, vieläkin tiukemmin: taustan tarkistukset. Turva-alalla on hyödyksi kyky ajatella pahantahtoisesti tahtomatta silti pahaa. Fyysisen alan turva-ammattilaiset ovat mahdollisia mutta tarvitsevat runsaasti lisäkoulutusta.

Töihinotossa sopimukset salassapidosta, tekijänoikeuksista, hyväksyttävästä käytöksestä sekä ymmärrys tietoturvapolitiikan vaatimuksista ko. tehtävän kannalta.¸

Tietoturvatehtävistä eroamisessa on erityiset vaaransa. Wadlow ehdottaa, että eroaja allekirjoittaa lukeneensa ja ymmärtäneensä lausuman, jossa todetaan hänen olevan luonnollisestikin keskeinen epäilyjen kohde, jos lähiaikoina tapahtuu jokin erityinen tietomurto. Kyseessä ei ole sopimus, eikä allekirjoitus tarkoita hyväksyntää vaan ainoastaan sitä, että asia on tullut tiedostetuksi.

TT-vastaavan on syytä varautua kaikkien turvatiimin jäsenten (ei niinkään henkilöiden vaan tehtävien) osalta siihen, että ero on jonain päivänä mahdollinen. Tilanteen hoitamiseksi turvallisesti pitäisi yleensäkin olla politiikka. Tärkeimpien tehtävien tapauksessa olisi lisäksi oltava hyviä vastauksia kysymyksiin, kuinka nopeasti henkilön pääsy verkkoon pystytään estämään ja miten saadaan selville, mitä hän on tehnyt muutaman edeltävän päivän kuluessa.

Entä muu henkilöstö

Työhönotosta ja eroprosessista on yleisesti TTP:n materiaalissa. Yksi lisähuomio: mahdollisen uuden työntekijän haastattelun yhteydessä voi olla työympäristön esittelyä. Kaikkea ei kannata näyttää.¸

Verkon toimilaitteet ja niiden turvaaminen

Nyt laajennetaan TTJ:n esitystä verkon turvaamisesta ja turvallisen verkon rakenteista [id=403 ja id=351]. Tässä käsitellään siellä mainituista tietoverkon neljästä tasosta erityisesti kahta keskimmäistä, sovellusohjelmia ja käyttöjärjestelmiä. Näiden alapuolella oleva verkkoyhteyksien taso tulee esille myöhemmin. Näiden kolmen ympärillä oleva käyttöturvallisuuden taso tulee esiin kaiken aikaa, kun on kyse ihmisen toimista – nimittäin niistä, jotka tapahtuvat sen jälkeen kun on jo suunniteltu, dokumentoitu ja rakennettu.

Aluksi Wadlow'n mukaan melko yleisellä tasolla, jäljempänä Allenin mukainen toimenpideluettelo (eli pikakertaus + täydennys).

Wadlow: Verkon komponenttien "linnoittaminen"

Verkko koostuu komponenteista, joita voidaan luonnehtia sen mukaan, millä OSI-tasolla ne korkeimmillaan toimivat:

- Passiiviset komponentit: kaapelit
- Korkeintaan tason kaksi laitteet: keskittimet, sillat ym.;
  näihin ei kuulu turvallisuuteen liittyvää toiminnallisuutta.
- Varsinaiset toimilaitteet, tasosta kolme ylöspäin.

Fyysinen turvallisuus riittää yleensä kattamaan muut kuin kolmannen ryhmän. Sen laitteet voidaan luokitella edelleen OSI-tasoa mukaillen tehtävänsä mukaisesti yksinkertaisiin ja monimutkaisiin. Edellisiä ovat mm. reitittimet ja jälkimmäisiä palvelimet ja työasemat, mutta jälkimmäisiä voidaan käyttää edellisten tavoin. Koska yksinkertaisessa tehtävässäkin voi olla yleiskäyttöinen laite, on varottava, ettei hyökkääjä pääse käyttämään sitä "monimutkaisesti".
Varsinaisilla toimilaitteilla on noin neljän tyyppisiä rooleja tietoverkossa.

- Reuna: reitittimet ulospäin (ISP:lle) ja yrityskumppanien verkkoon,
  palvelimet etäyhteyksille, sähköpostille, www:lle, ftp:lle, DNS:lle.
- Sisäinen pohjarakenne ("infra"): palvelimia tiedostoille, tulostukseen, nimipalveluun, autentikointiin, uutisiin, ajan synkronointiin.
- Liiketoiminta: tietokannat, sisäiset verkkosivut, tutkimuslaitteet,
- Työasemat.

Niiden turvallisuustarpeet eroavat laitteiden yleiskäyttöisyyden, yhteyksien määrän ja luonteen, ylläpidon laadun ja ohjelmistojen yleisyyden puolesta. Roolien sekoittuminen aiheuttaa lisähaasteita; esim. työasemilla voi olla myös muita luettelon tehtäviä.

Viidenneksi varsinaisten toimilaitteiden tyypiksi voi olla syytä ottaa monenlaiset sensorit ja aktuaattorit, joita esiintyy esim. teollisuusautomaatiossa tai älykodeissa. Ne ovat "liiketoimintaa", mutta kytkeytyvät verkkoon omalla tavallaan, ja joskus liiankin näkyvästi. Katsausartikkeli tälle alueelle: Security for industrial communication systems [Dzung, Naedele, v.Hoff, Crevatin, Proc. IEEE, 93, 6, Jun 2005, 1152–1177]. Näiden verkottamiseen liittyviä asioita mm. ad hoc –verkkoja tarkastellaan B-osassa.

Toimilaitteen turvaaminen tarkoittaa:

- Sen kaikista ohjelmistoista käytössä on tuorein vakaa versio (jos se on myös turvallinen ...).
- Kaikki tiedossa olevat turvapaikkaukset on asennettu.
- On määritelty etukäteen (järkevällä tarkkuudella)
  - kaikki laitteen tuotettaviksi tarkoitetut palvelut ja
  - kaikki laitteeseen tarvittavat pääsyoikeudet ja
  - mitkä laitteeseen liittyvät tapahtumat kirjataan.
- Järjestelmän konfiguraatio (laitteessa ja muualla) toteuttaa nämä määritykset, siis:
  - kaikki muut palvelut, joihin laite kykenisi, on kytketty pois.

- käyttäjän ja ylläpitäjän pääsyoikeuksien rajaukset on toteutettu – lisäksi kaikki tunnetut menetelmät on otettu käyttöön, jotta muunlainen pääsy ei olisi mahdollista.
- tapahtumakirjapito on asennettu. ¸

Laitteen rooli verkossa vaikuttaa turvatarpeisiin. Seuraava taulukko erittelee joitakin tavallisia lähtökohtia em. yleisissä rooleissa olevien toimilaitteiden turvamäärityksille:

	työasema	*sisäverkkopalvelin*	*reunapalvelin*
login-pääsy	ei raj.	rajattu	minimi
ylläpitopääsy	ei raj.	suppea	suppea
palvelupääsy	ei kellekään	monille	max rajoitukset
autentikointi	keskivahva	vahva	erittäin vahva
palvelut	melko vapaasti monenlaisia	vain tietyt	erittäin rajatut
kyvykkyys	minimiraj.	keskink. raj.	max rajoitukset
kirjanpito	minimaalinen	voimakas	maksimaalinen

¸
Toimilaitteen turvaaminen alkaa käyttöjärjestelmän (KJ) konfiguroinnista. Se ei sinänsä ole turvatehtävä, mutta sillä (kuten KJ:llä muutenkin) on paljon vaikutusta turvaamisen onnistumiseen. Huomionarvoisia seikkoja:

- Järjestelmän myöhempi uudistaminen kannattaa tehdä helpoksi.
- Eri järjestelmät kannattaa tehdä mahdollisimman yhdenmukaisiksi.
- Ylimääräistä levytilaa kannattaa jättää asennusvaiheessa, jotta uudistuksia ei jatkossa tarvitse asentaa alusta pitäen.
- Kannattaa varata eri levyosiot
  - käyttäjien datalle ja KJ:lle
  - KJ:lle ja systeemin konfiguraatiolle (eli sen "persoonalle")
  - edellä mainituille ja ohimenevälle datalle (ohjelmien työtiedostoille ja lokeille yms.)
- Kaikki parametrivalinnat kannattaa merkitä, vaikka ne olisivatkin toimittajan tämänhetkisten oletusasetusta mukaiset [Allen]. ¸

Mitä KJ:n konfiguroinnin lisäksi sitten tehdäänkin, toimilaitteen asennuksen saattaminen turvalliseksi voi tapahtua kahdella eri tavalla:

- Valmis asennus muunnetaan käsin sellaiseksi kuin halutaan (unblanding).
- Asennusohjelmaa muutetaan tekemään haluttu asennus suoraan (templating). Vaikeampi kehittää kuin edellinen, mutta asennustulokset saadaan sitten vähällä vaivalla ja tiedetään samanlaisiksi.

Kumpaakin tapaa varten kirjoitetaan luonnollisesti **komentojonoja**. Lisäksi käytännössä tehdään jotain näiden väliltä. Tärkeä kysymys on, miten asennukseen voidaan tehdä uudistuksia ja päivityksiä, vai pitääkö uudistukset asentaa alusta asti – ja miten tuolloin toimivat em. skripit! Työmäärän optimointiin voi tähdätä olemalla **järjestelmällinen** ja **yhdenmukainen** sekä **varautumalla muutoksiin** ja **testaamalla** kärsivällisesti. Näin edistyy todennäköisesti myös turvallisuus. Sitä varten suositellaan myös **konservatiivisuutta**. Kun vanhoja laitteita yritetään turvata uusien vaatimusten mukaisesti, konservatiivisuus voi vaatia alusta asti rakentamisen – varsinkin jos edellinen turvaylläpitäjä ei ollut järjestelmällinen jne. [Konkreettinen ohje automatisoiduksi KJ:n asennusprosessiksi: Allen s. 33] ¸

Uuden toimilaitteen valintakriteerit perustuvat paljolti sen kykyyn torjua hyökkäyksiä. Tässä on eri puolia:

- Konfiguroinnin puolesta voi olla tai puuttua mahdollisuus seuraaviin toimiin:
  palvelujen määrän rajoittaminen ‖ tarpeettomien ohjelmistojen poistaminen ‖ palvelujen tarjonnan rajoittaminen osoitteiden mukaan ‖ palvelua tarjoavien ohjelmien oikeuksien rajoittaminen ‖ monipuolinen lokitietojen keräysmahdollisuus ja niihin liittyvät hälytykset ‖ lokitietojen turvallinen tallennus ‖ hyvien turvakäytäntöjen monipuolinen käyttömahdollisuus

(esim. oikeuksien rajoittamista ei tarvitse itse toteuttaa omilla lisäohjelmilla) ‖ turvallinen ylläpidettävyys ja uudistettavuus (mm. hallinnointioikeuksien rajaus)

- On uskottavasti todettu, että laite pystyy estämään tunnetut hyökkäykset
- On perusteita uskoa että uusistakin hyökkäyksistä selvitään:
  - laitteen aiemmat ongelmat ovat tiedossa
  - valmistajan tyyli on ratkaista ongelmia viipymättä ja mielellään niin että ratkaistuksi tulee yhden ongelman sijasta kokonainen luokka jota se edustaa.
  - tiedonkulku toimii

(Vrt. myös Valtion *tietotekniikkahankintojen* tietoturvallisuuden tarkistuslista,VAHTI 6/2001)¸

Allen: Verkkopalvelinten ja käyttäjien työasemien turvaaminen

Neljä monivaiheista kohtaa:

suunnittelu – konfigurointi – ylläpito – käyttäjien tietämyksen lisääminen

Suunnittelu

Turva-asiat mukaan tietokoneiden **käyttöönottosuunnitelmaan** (suunnittelu → yhdenmukaisuus → ennustettavuus → helpotusta ylläpidolle & turvaongelmien löytämiselle).

Määritä ja dokumentoi seuraavat 15 asiaa:

- kunkin tietokoneen käyttötarkoitus
  käsiteltävät/ talletettavat tiedot ja niiden turvavaatimukset.
- tarjottavat verkkopalvelut
  asiakas ja/vai palvelin ‖ palvelin mieluummin vain yhtä palvelua varten (jopa FTP ja HTTP erikseen); yksi syy: vastuiden erottelu.¸
- asennettava verkko-ohjelmisto
  KJ:n vai 3. osapuolen tarjoama
- käyttäjät
  pääkäyttäjä, muut roolit → ryhmiä
- käyttöoikeudet
  taulukko (pääsymatriisi ryhmittäin)
- autentikointimenettely
  KJ:n & palvelun ‖ mekanismit salasanasta biometriikkaan
- käyttöoikeuksien toteutustapa
  KJ:n tarjoaman lisäksi ehkä salaus
- strategia tunkeutumisen havaitsemiseksi
  mitä lokeja kerätään¸
- varmistus- ja palautusmenettelyt
  roolit ja vastuut ‖ välineiden valinta ja käsittely ‖ paikallinen vai verkkototeutus ‖ salaus? ‖ replikointi
- verkkopalveluiden jatkuminen virhetilanteessa / palauttaminen sellaisen jälkeen
  varajärjestelmät (kylmä – lämmin – kuuma)
- käyttöjärjestelmän asennusmenettely
  (vrt. Wadlow edellä)
- miten tietokone liitetään yrityksen verkkoon
  segmentit vain keskenään luotetuille koneille ‖ jos modeemi on välttämätön, autentikointi vähintään kertakäyttösalasanoilla; kytkentä vain kun tarvetta on.
- päivittäisen hallinnoinnin tietoturva-asiat
  työaseman ja paveluiden hallinnointi verkon yli, automaattisten työkalujen avulla (ks. jäljempänä)
- käytöstä poistettujen laitteiden sisältämä tieto
  menettelyt magneettisesta mekaanisiin
- tietokoneiden käyttöönottosuunnitelman ajantasaisuus
  uudet uhat, teknologiat, käyttäjäryhmät, organisaatioyksiköt; verkon rakennemuutokset¸

Palvelimen valinnassa huomioitavat tietoturva-asiat.

Periaatteessa samat huomiot kuin edellä Wadlow'n mukaan. Tässä vielä prosessina:

- toiminnallisuuden ja suorituskyvyn vaatimusten määrittely
  sitoutumisista riippumatta
- tarjolla olevan tuotteen turvaominaisuuksien ruotiminen
  myös muita lähteitä käyttäen
- kilpailevien tuotteiden käyttökustannusten vertailu
  sisällyttämällä hyökkäyksistä aiheutuvien kustannusten odotusarvo.¸

Konfigurointi, 8 tehtäväkokonaisuutta

Pidä käyttöjärjestelmät ja sovellusohjelmistot ajan tasalla

- arvioi ja asenna päivitykset.
  kaikki eivät sovellu ‖ täysi varmistus ensin ‖ mahdollisesti ensin testiympäristöön tai muutamaan koneeseen ‖ haavoittuvuudet ja muut haitat päivityksen kuluessa ‖ tapahtuneiden muutosten tarkkailu esim. Tripwiren avulla ‖ uudet aukot.
- uusiin koneisiin ajantasaiset ohjelmistot
- uudet eheyden tarkistustiedot
  kryptografiset tarkistussummat talteen ‖ myös muunlainen lähtötasoa kuvaava 'baseline'-tieto on mahdollinen ‖ työkaluna esim. Tripwire, josta lisää harjoituksissa.¸

Karsi palvelimelta turhat palvelut

- määrittele toiminnot
  palvelut ‖ tiedostojärjestelmä ‖ ylläpito: järjestelmä (konsoli vai etä) & palvelu (lataus muualta? Tarvitaanko ohjelmistotyökaluja?) ‖ verkkokonfiguraatio ‖ tuetut protokollat (muut kuin IP?)
- valitse turvallisempi vaihtoehto
  SSH — r-komento ‖ TCP wrapper — ilman
- asenna vain minimivalikoima palveluita ja sovelluksia
- uudet eheyden tarkistustiedot¸

Karsi työasemalta turhat palvelut

- määrittele toiminnot
  sovellukset ‖ tiedostojärjestelmä ‖ KJ:n oletuksena olevat palvelut (kuten www ja ftp) ‖ ylläpito ‖ verkkokonfiguraatio ‖ tuetut protokolla (muut kuin IP?)
- asenna vain tarpeelliset ohjelmistot
- uudet eheyden tarkistustiedot

¸

Konfiguroi verkkopalveluiden asiakkaat turvallisuutta edistävällä tavalla

- tunnista toiminnot, joista voi aiheutua tietoturvaongelmia
  luottamuksellisten tietojen lähetys julkisen verkon yli ‖ laajennettujen käyttöoikeuksien tarve ‖ ohjelmistojen lataaminen ja suoritus epäsuorasti tai käyttäjän toimesta ‖ tietojen särkeminen väärien asetusten takia ‖ asiakkaan koneen tai sen verkon tietojen paljastaminen ‖ asiakkaan kryptoavaimet ja valtuustiedot ‖ luottamussuhteet ‖ onko asiakas kiinni myös muissa verkoissa.
- seuraa toimittajien päivityksiä
- konfiguroi asiakas niin, että turvallisuus säilyy
  tarpeet vaihtelevat ‖ yleisohjeena mm. tämä: poista vähemmän välttämättömät toiminnot ja estä niiden käyttöönotto¸

Määrittele tietokoneisiin käyttäjien autentikointimenettely

- konfiguroi laitteistotason käyttöoikeudet
  BIOS- tai EEPROM-salasana
- käy läpi käyttäjätunnukset ja -ryhmät
  erityisesti: vierastunnusten poisto/rajoitus
- tarkista salasanapolitiikkasi ja varmista, että käyttäjät noudattavat sitä
  politiikan pääkohdat: salasanan pituus, muodostussääntö, vanheneminen, uudelleenkäyttö, muutosoikeus
- vaadi uudelleenautentikointi, kun tietokone on ollut käyttämättömänä
  joutonäyttö ‖ etäyhteyden logout ‖ toimikortti irti kun poissa
- estä sisäänkirjautuminen muutaman epäonnistuneen yrityksen jälkeen

DoS-vaara!

- asenna ja konfiguroi autentikoinnin lisämekanismit
  toimikortti ‖ todennuslaskin ‖ kertakäyttöinen salasana ‖ biometriikka¸

Konfiguroi käyttöjärjestelmään tiedostojen, laitteiden ja muiden kohteiden käyttöoikeudet

- määritä tarvittavat suojaukset
  pääsymatriisi käyttäjäryhmittäin
- konfiguroi käyttöoikeudet
  myös: periytyvyyden huomiointi, hyödyntäminen, vaatiminen
- asenna ja konfiguroi tiedostojen salaus luottamuksellisia tietoja varten¸

Määrittele tiedostojen varmistusmenettely

- laadi tiedostojen varmistus- ja palautussuunnitelma
  (vrt. edellä suunnitelman yhteydessä)
- asenna ja konfiguroi varmistustyökalut
  tod. näk. 3. osapuolen ohjelmisto on tarpeen ‖ palautustyökalut myös off-line -tallessa ‖ palautusten pääsyoikeusasetukset
- testaa palauttaminen varmistuksilta
  palautustarve harvinainen, mikä on lisäsyy testauksille¸

Käytä testattua mallikonfiguraatiota ja turvattua replikointimenettelyä

- luo ja testaa mallikonfiguraatio
- replikoi konfiguraatio muihin työasemiin
- tee tapauskohtaiset muutokset
- uudet eheyden tarkistustiedot¸

Ylläpito, 3 tehtäväkokonaisuutta

Suojaa tietokoneet viruksilta ja muilta haitallisilta ohjelmilta

- laadi suojautumissuunnitelma haitallisia ohjelmia vastaan
- asenna ja ota käyttöön virustorjuntatyökalut
- kouluta käyttäjät
- pidä virustorjuntatyökalut ajan tasalla¸

Konfiguroi tietokoneet turvallisen etäkäytön vaatimalla tavalla

- hallinnointikomennot vain autenttisilta ylläpitäjiltä ja koneilta
- käyttökomentojen toiminta alimmalla mahd. käyttöoikeustasolla
- ulkopuolisten mahdoton siepata, lukea tai muuntaa luottamuksellista tietoa
- tietojen siirtoon liikuteltava tallennusväline
- lokitietojen tutkiminen vain turvallisella menettelyllä
- uudet eheyden tarkistustiedot

Salli vain luvallinen pääsy tietokoneelle

- estä laitteisto-osien luvaton asennus
  modeemi ‖ irrallinen tallennusväline ‖ kirjoitin ‖ käynnistyslaite ‖ liittimien poisto
- sijoita tietokone turvalliseen tilaan¸

Käyttäjien tietämyksen lisääminen

Suunnittele ja ota käyttöön työasemien sallittua käyttötapaa koskeva politiikka

- käyttöpolitiikan sisältö (+ = myöntö; – = kielto):
  työasemat (+/–) ‖ laitteistomuutokset (+) ‖ ohjelmistojen asennus / poisto (+) ‖ minkälainen työskentely (esim. suhteessa turvaluokituksiin ja yksityisasioihin) ‖ verkkopalvelut (+/–) ‖ verkon yli lähetettävät tiedot (+/–) ‖ vastuut, esim. hallinnolliset tehtävät ‖ konfiguraatiomuutokset (+/–), jos on myönnetty tavallista suuremmat oikeudet ‖ ei jaettuja käyttäjätunnuksia ‖ salasanapolitiikan noudattamispakko ‖ suojaamattomien ohjelmien ja tiedostojen käsittely ‖ ei salasanojen murtamista ‖

ei palveluiden keskeyttämistä ‖ mitä seuraa jos rikkoo sääntöjä

- käyttäjien koulutus
  motivointi merkityksen kautta; myös vertaiset kouluttajina; sitoumuksen allekirjoitus
- politiikkamuistutus sisäänkirjautumisen yhteyteen¸

Turvallisuuden arvostaminen

On mahdollista, että tietoturvan tekijä osaa arvostaa työtään ja motivoitua siihen, vaikka se ei hyvin sujuessaan tuotakaan kovin näkyvää tulosta. Haasteellisempaa voi olla vakuuttaa toiset tästä ja kriittisen tärkeäksi arvostuksen hankkiminen voi muodostua tietoturvatyön rahoituksen hankkimisessa tai jatkamisessa. Tätä varten on yritetty luoda mittaamismenettelyjä, esim. VAHTI-ohjeessa 6/2006 ”Tietoturvatavoitteiden asettaminen ja **mittaaminen**”. Aiempi ohje mainitsee jo nimessään mihin tässä pyritään: ”Tietoturvallisuus ja **tulosohjaus**”(VAHTI 2/2004). Seuraavassa kuvataan arvostusongelmaa melko yleisellä tasolla Wadlow’n mukaisesti.

Laadullisesti ...

Miksi muilla saattaa olla hämärä käsitys turvatiimin toiminnasta?

Turvaprosessi saa toteuttajansa pitämään suunsa kiinni.
Jos teet työsi oikein, tulokset ovat pääasiassa kuitenkin negatiivisia.
Tulokset, jotka eivät ole negatiivisia, ovat yleensä vaikeita ymmärtää.
Tulokset jotka olisivat helppoja ymmärtää, ovat yleensä arkaluonteisia.¸

Yleisiä väyliä minkä tahansa työn esittämiselle, jotta toinen osaisi arvostaa sitä. Hän

1. näkee sen; tarvitaan näyttöä, jota saadaan keräämällä tietoa ja tekemällä laskelmia (numeroita, trendejä, vertailuja)
2. ymmärtää; tärkeätä konteksti mutta ilman liikoja yksityiskohtia.
3. on samaa mieltä sen arvosta; kannattaa kerätä palautetta ja muuttaa esitystään seuraavaksi kerraksi sen mukaan.
4. tietää, ettei osaisi itse tehdä sitä yhtä hyvin; silti ei kannata uskotella, että tehtävät ovat vaikeampia tai suurempitöisiä kuin ne oikeasti ovat.

5.–7. voi näyttää sen omalle pomolleen, saada hänet ymmärtämään ja olemaan samaa mieltä arvosta.¸

Miten yleisesti selitetään, mitä on itse tehnyt:

- Aseta odotukset sopivasti: ei riitä sanoa mitä on tehnyt vaan se pitää voida suhteuttaa siihen mitä olisit voinut tai sinun olisi pitänyt tehdä. Pelkkä vertailu politiikkaan ei riitä. Suhteutus aiempiin ajanjaksoihin tai muihin yrityksiin on hyödyksi. Jälkimmäiset ovat erittäin vaikeita hankkia (...)

- Esitä saavutuksesi näkyvästi suhteessa odotuksiin.
- Älä laadi kriteerejä vain näyttääksesi hyvältä niiden valossa. Hae palautetta myös kriteereistä.
- Esitä tieto kohtuullisen "teatraalisesti".¸

Mitä turva-asioita voi esittää määrällisesti

Monenlaisia tietoja on syytä kerätä rutiininomaisesti, mutta harvoja tietoja kannattaa kerätä, ellei niillä ole käyttöä. Tiedoista pitää myös laatia yhteenvetoja jonkin sopivan ajanjakson yli, esim. neljännesvuosittain.

Hyökkäysten näkökulmasta

- montako hyökkäystä tapahtui
- miten monta mitäkin tyyppiä; mitkä olivat yleisimmät tyypit
- miten määrät vertautuvat vastaaviin yrityksiin
- monessako hyökkäyksessä oli
  - mahdollista etsiä hyökkääjää
  - ja miten pitkälle päästiin
- hyökkääjien valikoima (”ampiaiset—paarmat—loiset”)
  - miten hyökkäykset jakautuivat
  - miten jakauma on muuttunut ajan kuluessa
  - miten se vertautuu muihin yrityksiin¸

Puolustuksen näkökulmasta

- montako hyökkäystyyppiä pystytään
  - havaitsemaan
  - torjumaan
- miten puolustus on muuttunut ajan kuluessa
- montako siirtymää tapahtui tilaan
  - ”mahdollinen hyökkäys”
  - ”varma hyökkäys”
  - ja moniko näistä sittemmin havaittiin oikeaksi
- montako hyökkäystä
  - hoitui passiivisilla mekanismeilla
  - tarvitsi ihmisen puuttumisen asiaan¸

Turvajärjestelmä

- kattavuus
  - työvuorojen osalta
  - pätevyyden osalta
- miten hyökkäykset jakautuivat työvuorojen suhteen
- keskimääräinen aika vastata
  - hyökkäykseen
  - muutospyyntöön
  - turvajärjestelmää koskevaan tiedusteluun¸

Kolmannen osapuolen auditointi

- paljonko aikaa viimeisestä täydellisestä
- mitkä olivat viime auditoinnissa esitetyt vakavat huomautukset
- mitä niistä (tai muista puutteista) on sen jälkeen korjattu
- mitä huomattavia puutteita auditoinnin jälkeen on havaittu

Tiedon hankinta ja koulutus

- mitä lähteitä seurataan uusien hyökkäysten varalta
- miten näiden lähteiden luettelon on muuttunut ajan kuluessa
- mitkä lähteet ovat hyödyllisimpiä
- mitä harjoitusta turvaryhmä on saanut¸

TLT-3301 Verkon tietoturva, 3. luento 8.12.2008

Lokitietoa [Wadlow Ch. 9+15, Allen Ch. 5-6]
Mitä loki tarkoittaa; Lokien keruu; Hallinnointi
Mitä laki sanoo lokitiedoista
Lokianalyysi
Tunkeutumisen havaitseminen [Wadlow Ch.9+15, Allen Ch. 5-6, seminaariraportti 2004]
DoS ja DDoS [seminaariraportti 2005]
,

Lokitietoa

Mitä loki tarkoittaa

Bishop määrittelee kirjassaan Computer Security (2003) hyvin yleisesti:

Lokitietojen keruu (’logging’) on tapahtumien tai tilastotietojen tallentamista, jonka tarkoituksena on tuottaa näkemys siitä, miten järjestelmää käytetään ja miten se suoriutuu.
Auditointi (’auditing’) on lokitietojen analyysia, jonka tarkoituksena on esittää järjestelmää koskeva tieto selkeässä ja ymmärrettävässä muodossa.

Näiden soveltaminen turvallisuuteen lähtee tietoturvapolitiikasta. Siinä on periaatteessa määritelty, mitkä järjestelmän tilat ovat turvallisia ja mitkä eivät. Analyysin tavoitteena on saada selville

- onko järjestelmä turvattomassa tilassa, ja jos on,
- miten siihen päädyttiin.

Jälkimmäisen tavoitteena puolestaan on

- vastaavien tapahtumaketjujen tekeminen jatkossa mahdottomiksi,
- syyllisten saattaminen vastuuseen. ,

Termeistä. Myöhemmällä luennolla (ja TT-johtamisen kurssilla) käsiteltävä *auditointi*, ’security audit’ on eri asia. Jos se pitäisi oikeasti suomentaa, voisi käyttää nimitystä *turvallisuuden tarkastus*. VAHTI-käsitteistön mukaan ’audit’ on *toimentarkastus*: ”Kohteen ja sen toiminnan tarkastus ennalta asetettujen arviointiperusteiden suhteen”. Vaikka luennoissa ja molemmissa kurssikirjoissa käytetään auditoinnin sijasta termiä *lokitietojen analyysi,* on syytä muistaa edellä sanottu, jotta muualla esiintyvät termit eivät johtaisi harhaan. ,

Varsin yleinen ilmaisu ’audit trail’ tarkoittaa nimenomaan lokitiedoista muodostuvaa *kirjausketjua*, eikä sitä miten tarkastus suoritettiin. Lokitietoja kutsutaan englanniksi myös nimellä ’audit log’. Asioilla on tietenkin yhteys: VAHTI-käsitteistön mukaan kirjausketju on ”Alkutositteiden, syöttötietojen ja tulosteiden aukoton ketju, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet.”

Sana loki, ’log’, esiintyy myös lokikirjassa, johon se on merenkulun käytäntöjen kautta päätynyt alkuperäisestä puupölkkyä tarkoittavasta merkityksestään. Lokikirjan kautta juontuu myös termi ’log-in’ eli sisäänkirjautuminen. ,

Lokien keruu

Perustavoitteet:

- vähentää todennäköisyyttä, että hyökkäys voi tapahtua ilman että siitä jää lokimerkintä.
- kasvattaa todennäköisyyttä, että hyökkäyksestä tehdyt lokimerkinnät huomataan sellaisiksi.

niin pitkälle kuin kustannusten ja hyötyjen vertailu antaa perusteita – turvajärjestelmän hinnanhan pitää olla verrannollinen sillä suojattavan järjestelmän arvoon. (Karkea arvio: ”naurutestin” ja ”vautestin” välimaastosta.)¸

On paljon todennäköisempää havaita hyökkäyksiä tai hyökkääjiä lokien tarkastelulla kuin itse teossa. Lokeja tarvitaan myös jälkimmäiseen tarkoitukseen. Yleisesti lokeilla on merkitystä kolmella eripituisella aikajänteellä:

- lyhyt: hyökkäykset juuri nyt; myös vikatilanteet,
- keskipitkä: tarvitaan kontekstia hyökkäyksen toteamiseen. Tyypillisesti DoS.
- pitkä: erityisen ”hienovaraiset” hyökkäykset.

Pitkällä aikavälillä merkitystä on myös kapasiteetin seurannalle ja suunnittelulle.¸

Lokisysteemin perusvaatimukset

Lokin ei pidä olla hyökkääjän ulottuvilla.
Lokisysteemin pitäisi pystyä havaitsemaan,
onko jokin laite odottamatta lakannut lähettämästä lokitietoja.¸

Mitä lokeja kerätään

Verkon pitää kirjata sellaiset tapahtumat, jotka tarvitaan, kun halutaan todeta

- tunnetut hyökkäykset
- epätavalliset pääsykeinot
- lokisysteemin toimintavarmuus¸

Kirjaaminen, jos mikään perustuu etukäteiselle suunnittelulle, ja se alkaa tietojen keruun hyödyllisyyden punninnalla. Tuloksena on (ehkä aiempia päivittävät) määritykset sille

- mitä tietoja kerätään ylipäätään, ja
  - mitä lokimekanismien kautta ja
  - mitä muilla tiedonkeruumekanismeilla kuten
    - manuaalinen kirjanpito (uutisia myöten), tietovirtojen seuranta
  - Pääluokat Allenin 3-sivuisesta taulukosta kerättävien tietojen tyypeistä:
    - Verkon suorituskyky — muut verkkotiedot
    - Järjestelmän toiminta — muut järjestelmätiedot
    - Prosessin toiminta — muut prosessitiedot
    - Tiedostot ja hakemistot — Käyttäjät — Sovellukset
    - Lokitiedostot — Turva-aukot [→ taulu 5.2, jaetaan paperilla]
- mistä tapahtumista tarvitaan hälytys¸

Lokimekanismeja

1. Syslog
2. SNMP
3. Erityiset mekanismit, toivottavia ominaisuuksia:
   - laajalti ja vapaasti käytettävissä
   - turvattavuus
     - viestien eheys
     - salakuuntelun esto
     - pääsynvalvonta
     - palvelun eston vaimentaminen
   - luotettavuus – siinä merkityksessä kuin UDP on epäluotettava
   - graceful degradation
   - hallittavuus¸

Ajan merkitys. Koneiden kellojen on oltava samassa ajassa: NTP-protokollan aikapalvelu GPS-tekniikalla. Lokipalvelimella voisi olla omakin oikea aika. Tällöin voisi tehdä vertailuja oikean ja

verkkoajan välillä ja havaita ongelmia, kuten hyökkäyksen NTP:tä vastaan. Vertailu voi toteutua muuallakin. Tällaisesta hälyttäminen on yksi esimerkki seuraavasta:

Tunnistimet / ilmaisimet (’sensors’) verkon eri kohdissa lähettämässä lokitietoa tai hälytyksiä. Esimerkiksi laitteiden toimivuuden ilmaisu, myös fyysisessä mielessä. Lokitietojen kertymisen ilmaisin tulee esille lokien hallinnoinnin yhteydessä jäljempänä.¸

Lokisysteemi ja lokien hallinnointi

Lokisysteemien ääripäänä on pienessä yrityksessä reititin ja sen takana oleva työasema.
Isossa yrityksessä voi olla

- fyysisesti eristetty lokiverkko, jossa
- reunalla suodatin joka hälyttää, jos joku yrittää liikennöidä ulospäin
- useita lokien keruukoneita
- riippumaton aikalähde
- lokien analysointiin tarkoitettuja työasemia
- erillinen *eheyden vahtikone*. Tehtävänä
    - kuunnella kaikkea liikennettä lokiverkossa ja
    - tarkastaa sen oikeutus ja
    - kaiken saapuvan lokitiedon oikeutus, sekä
    - saapuuko lokeja sieltä mistä ennenkin¸

Tarkemmin eheyden varmistamisesta:

- erittäin rajattu fyysinen pääsy laitteisiin.
- erillinen eheysmonitori, jossa konkreettisesti monille näkyvä näyttölaite.
- kerrostetut pääsyoikeudet, eli kirjoitusoikeus eo. monitoriin vain kahdella, varsinaisiin lokisysteemeihin vain muutamalla ja muilla asianosaisilla vain lukuoikeus. Lokien analyysijärjestelmään pääsy vain vasteryhmän päälliköllä, joka laskee sisään muut. Toinen tapa (parempi): ”kahden henkilön sääntö”.
- merkintöjen laskenta: lokiin menevät ja lokissa olevat lasketaan eri prosesseilla ja näytetään. Merkintöjen määrän pitää olla kasvava.¸
- ajoittainen tarkistus:
    tiedoston joka K:s rivi luetaan ja verrataan viime kerran luennan tulokseen. Sitä varten täytyy kahdentaa 1/K lokitiedostosta. Tarkistusten aikavälin pitää olla sen verran lyhyt, että vertailun ulkopuolelle jääviä uusia merkintöjä ei ehdi tulla kovin paljon: L uutta vertailumerkintää tarkoittaa noin K*L varsinaista uutta lokimerkintää. Jos K on 500, niin L voitaisiin pyrkiä pitämään enintään 10:ssä. Paljon arvoa K*L (tässä 5000) suurempi lokikertymä säädetään aiheuttamaan varoitus.
- koko lokin kahdentaminen, tai varmuuskopiointi¸

Muuta hallinnointia

Lokien keruun käyttöönotto

- miten käynnistys tapahtuu: kerran, ajoittain, vai aina kun järjestelmäkin
- onko riittävästi tilaa, samaan paikkaan voi tulla lokeja useasta lähteestä

Jotta tarpeelliset lokimerkinnät voitaisiin löytää ja riittävästi lokeja olisi tallessa:
tarvitaan lokitiedostojen hallintasuunnitelma:

- paloittelu
- tiedostojen kierrätys
- tiivistys, arkistointi

Arkojen lokitietojen suojaus voi edellyttää myös niiden salaamista (ja avainten suojaamista...) ja asianmukaista hävittämistä aikanaan (vrt. lokilaki jäljempänä)
Lokien lisäksi eheyssuojaa tarvitsevat lokimekanismit ja niiden tuottamat raportit.
Erityistoimia voidaan tarvita todisteiden säilyttämiseksi, jos tunkeutuminen on tapahtunut.¸

Vähän lokilakia

Lokien keruuseen ja käyttöön liittyy lainsäädäntöä, jota käsitellään tässä lyhyesti ja nimenomaan lokien kannalta. Keskeinen sisältö lähes kaikessa on henkilötietojen käsittely ja sitä kautta samat lait liittyvät verkossa tapahtuvan viestinnän, erityisesti sähköpostin käsittelyyn. Tästä näkökulmasta asiaan palataan tarkemmin (ensi kerralla), kun luetaan VAHTI-ohjetta 2/2005, joka on Valtionhallinnon sähköpostin käsittelyohje.¸

Julkisuuslaki, eli Laki viranomaisen toiminnan julkisuudesta (621/1999) antaa oikeuden pitää salassa tietoturvallisuusjärjestelyjä. Yksi tällainen tieto on se, millaisia lokeja järjestelmässä tarkkaan ottaen kerätään. Siis, lokitiedoista eikä edes niiden olemassaolosta ei tarvitse luovuttaa tietoja kenellekään, jolle tieto ei työtehtävien suorittamiseksi kuulu.

Käyttäjälle voidaan luovuttaa tietoa häntä koskevista lokimerkinnöistä, jos tieto sellaisen lokin olemassaolosta tai itse lokimerkinnästä ei vaaranna järjestelmän turvallisuutta.¸

Lokitiedoista voi muodostua **henkilötietolain** (523/1999) tarkoittama henkilörekisteri. Ei siis ole lupa luovuttaa sellaisia tunnistetietoja, joista selviää käyttäjän henkilöllisyys. Viranomaisilla voi olla oikeuksia saada tunnistamistietoja rikosten estämiseen tai esitutkintaan – edelliseen **poliisilain** (493/1995) ja jälkimmäiseen **pakkokeinolain** perusteella (450/1987). Näissä laeissa määritellään ja käytetään (luvuissa 3 ja 5) mm. käsitteitä *telekuuntelu, televalvonta* ja *tekninen tarkkailu,* joka voi olla *teknistä kuuntelua, katselua* tai *seurantaa*. Pakkokeinolaissa puhutaan myös *takavarikosta* (luku 4) ja sen yhteydessä mm. tietojärjestelmän haltijan velvollisuudesta luovuttaa salasanoja tms. ¸

Sähköisen viestinnän tietosuojalaki (516/2004) säätelee sitä, miten operaattorit saavat kerätä ja käsitellä viestintää koskevia lokitietoja, erityisesti *tunnistamis-* ja *paikkatietoa.* [→ §4 ja luku 3]

Laki yksityisyyden suojasta työelämässä (759/2004) koskee (mm.) työnantajan toteuttamaa henkilötietojen käsittelyä, teknistä valvontaa työpaikalla ja työntekijän sähköpostiviestin hakemista ja avaamista. Tässä laissa tulee esille siis lokitieto laajemmassa kuin tietoteknisessä merkityksessä. [→ §16–17 kameravalvonnasta; §21 mm. tietoverkon käytön valvonnasta]¸

Tietoturvaloukkauksia tai meneillään olevia hyökkäyksiä selvitettäessä voidaan luovuttaa reititystietoja esimerkiksi CERT-organisaatioille tai toisten järjestelmien ylläpitäjille.

Tietosuojasäännöksistä seuraa sellainenkin, että lokitietoja sisältäneiden tietovälineiden hävittämiseen pitää kiinnittää huomiota. Tietenkin asia on tärkeä myös yleisemmin lokitietojen arkaluonteisuuden takia.

Sikäli kuin lokien käsittelyn kautta pyritään torjumaan ja varsinkin löytämään hyökkääjiä, kuvaan astuu **Rikoslaki**. Tätä aihetta on käsitelty TTJ:ssä [id=161] ja siihen palataan hyökkäyksiin reagoimisen yhteydessä myöhemmällä luennolla.¸

Lokianalyysi

Perussääntö: Lokianalyysi ei saa koskaan häiritä lokien keruuta.

Wadlow: ”key priorities in a search through your logs”: Etsi
- liikennettä (ylipäätään), ja siinä
- poikkeamia (anomalioita)
- kytkentöjä (joita muodostuu koneiden välille)
- hahmoja (joita tapahtumat muodostavat)
- särkyneitä tai epätavallisia hahmoja

- luo hypoteeseja, ja
- datan avulla yritä
  - tukea niitä
  - kumota niitä

Lisää analyysia seuraavassa ja jäljityksen yhteydessä.¸

Tunkeutumisen havaitseminen

TTJ:ssä on yleiskatsaus IDS-aiheeseen [(→) id=350] ja tekniikoiden jaottelu [id=303].

Jo TTP:ssä esitetään [id=189], että on kahdenlaista IDS-menettelyä:

- tietämys- eli sääntöpohjainen IDS, eli hyökkäysmallin (”signatuurin”) havaitseminen
- käyttäytymispohjainen, eli tilastollinen IDS, eli anomalioiden havaitseminen.¸

Tilastollinen menetelmä tarvitsee seuraavanlaisia **esitietoja**, joita täytyy tietysti suojata ja pitää ajan tasalla: [Allen §5.3]

- tyypillinen verkkoliikenne ja sen suorituskyky
- järjestelmän odotettavissa oleva käyttäytyminen ja suorituskyky
- prosessien ja käyttäjien käyttäytymisen odotusarvot
- tiedostojen ja hakemistojen odotusarvot:
  - KJ:n tiedostot ja konfiguraatio
  - turvatyökalut ja niiden tiedot
  - sovellukset
  - julkiset tiedot, esim. www-sivut
  - yritystä koskevat tiedot, kuten talousraportit ja työntekijätiedot
  - käyttäjätiedot ja käyttöoikeudet
- järjestelmän laitteistoluettelo¸

Tietenkin tilastojen käyttämään ”normaaliin” kuuluvat myös politiikan asettamat säännöt, mutta sääntöpohjainen IDS viittaa siis sääntöinä esitettyihin tunnettujen *hyökkäysten* kuvauksiin, joita on valmiina erilaisissa tietokannoissa. [→ Esimerkkejä seuraavassa mainittavan dokumentin luvusta 4]

IDS-aiheesta pidettiin TTY:llä keväällä 2004 seminaari, jonka raportti on saatavilla sivulla http://www.cs.tut.fi/kurssit/8306000/TL-TT/2004/. Siitä löytyy vastauksia muutamaan seuraavista kysymyksistä, joiden tarkoituksena oli kattaa aihepiiri melko laajasti:¸

1. Mitä tunkeutuminen tarkoittaa, ketkä tunkeutuvat, miksi ja miten? [luku 2]
2. Miten tunkeutuminen ilmenee ja näkyy puolustajalle? Mikä vaikutus tässä on oman verkon rakenteella ja sitä koskevilla lähtötiedoilla?
3. Minne pitäisi katsoa, jotta tunkeutumisen voisi nähdä (siis mitä lokitietoja pitäisi kerätä ja miten)?
4. Miten tunkeutuminen löytyy lokitiedon massasta? [luvun 3 oli tarkoitus vastata tähän…]
5. Miten tunkeutumisten tunnusmerkkejä voidaan abstrahoida ja tallettaa tietokantoihin? [**luku 4**]
6. Mitä työkaluja on käytettävissä kohdan 4 kysymykseen? (Yleiskatsaus) [**luku 5**]
7. Mikä merkitys tilastollisella analyysilla on IDS:lle?
8. Miten verkon eri osia hyödyntävä tunkeutuja voidaan havaita? [luku 6]
9. Mitä voidaan tehdä automaattisesti hyökkäyksen pysäyttämiseksi?
10. Miten tunkeutujalle voidaan asettaa ansoja?¸

Lisäksi raportissa on Snort-työkalun esittelyä [luvut 7 ja 8], johon palataan harjoituksissa. Yhden luvun aiheena on WWW-palvelimen IDS ja se tulee esille ensi kerralla [**luku 9**]. Raportin viimeisessä luvussa erikoisaiheena on IDS sellaisissa langattomissa verkoissa, jotka muodostuvat tilapäisesti verkkolaitteina toimivien mobiililaitteiden välille [luku 10]. (Tällaisten ad hoc -verkkojen turvallisuutta on käsitelty saman seminaarikurssin kevään 2007 toteutuksessa.)

Tämän kurssin **tenttivaatimuksiin** asetetaan vain raportin luvut 4, 5 ja 9, mutta muitakin lukuja kannattanee silmäillä.

Allenin kirjan luvun 6 aiheena on **tunkeutumisen havaitseminen**. Luvussa 5 on jo esitetty, miten tunkeutumisiin pitää **varautua** politiikkamäärityksin, loki- ja esitietojen keruulla ja hallinnoinnilla sekä reagoinnissa tarvittavien työkalujen käyttöönotolla. Luku 7 puolestaan käsittelee **reagointia**.

Kun luvun 6 asioista karsii *fyysiset tarkistukset* ja *työkalujen eheyden varmistamisen*, jää jäljelle **Allenin / CERTin malli varsinaiselle tunkeutumisen havaitsemiselle**. Siinä on kolmen tyyppisiä tutkimuskohteita: ”dynaamisia, staattisia ja inhimillisiä”. (Erityisesti kaksi ensimmäistä luokkaa kertaavat ja perustelevat taulukossa 5.2 esitettyjä lokin keruukohteita.)

Valvo ja tutki (informoituasi ensin käyttäjiä)
- **verkkotoimintoja** (§6.3)
  - Tutki verkon hälytykset, virheraportit, toimintaa, liikennettä [→ §6.3.4–5]
- **järjestelmätoimintoja** (§6.4)
  - Tutki järjestelmähälytykset, -virheraportit, -toiminnan tilastot
  - Valvo
    - prosessien toimintoja ja käyttäytymistä [→ §6.4.5]
    - käyttäjien käyttäytymistä
    - verkkosniffereitä
  - Käytä verkon skannaustyökaluja
  - Tutki turva-aukkojen skannaustyökaluilla kaikki järjestelmät

Tutki tiedostoja ja hakemistoja ja etsi odottamattomia muutoksia (§6.5)
- Varmista eheys
- Tunnista odottamattomat muutokset ja niiden vaikutukset [→ §6.5.2]

Käy läpi käyttäjien raportit epäilyttävistä järjestelmä- ja verkkotapahtumista (§6.8)
- Analysoi raportti
- Arvioi, suhteuta ja priorisoi kaikki raportit
- Tutki kaikki raportit tai yhteenkuuluvien raporttien joukot

Allen luettelee ison joukon ohjelmistotyökaluja IDS-tarkoitukseen [→ taulukko 5.3].
Seminaariraportin luvussa 5 on kuvailevampi esitys lokityökaluista. [→ taulukko s.19 …]
Joissain yhteyksissä voi törmätä termeihin SEM tai SIM (Security Event/Information Manager), joilla tarkoitetaan lokityyppisen tiedon hallinnointiin tarkoitettua tietojärjestelmää.

Tuoreita näkökulmia löytyy esim. lehden *Information Security Technical Report* IDS-aiheisesta teemanumerosta *Volume 10, Issue 3, s. 133–184* (2005) [http://www.sciencedirect.com]

Palvelunestohyökkäyksen havaitseminen ja torjuminen

Palvelunestonkin tapauksessa tapahtuu yleensä ensin tunkeutumisia. Edellä käsitellyt IDS-menetelmät soveltuvat siten jossain määrin myös DoS-torjuntaan. Palveluneston varsinaisen uhrin kannalta tilanne voi näyttäytyä melko erilaisena.

DoS- ja DDoS-aiheesta pidettiin TTY:llä keväällä 2005 seminaari, jonka raportti on saatavilla sivulla http://www.cs.tut.fi/kurssit/8306000/TL-TT/. Raportista otetaan tämän kurssin **tenttivaatimuksiin luvut 2–5**. Niissä tarkastellaan ensin, miten DoS ja erityisesti DDoS tapahtuu tietoverkossa ja miten hyökkäykset ovat kehittyneet. Sen jälkeen käsitellään verkon suojaamista DoS-*vaikutukselta* ja DoS-hyökkäyksen *varsinaista torjuntaa* kohteessa.

Palvelunestohyökkäyksen käsittelyä internet-palvelun tarjoajan näkökulmasta on esitelty RFC:ssä 4778, joka on Current Operational **Security Practices** in Internet Service Provider Environments, (Informational, 2007). Sivuilta 29–31 (ja tarkemmin B-osassa):

> New techniques are continually evolving to automate the process of detecting DoS sources and mitigating any adverse effects as quickly as possible. At this time, ISPs are using a variety of mitigation techniques including:

sinkhole routing,
: asetetaan erityinen reitti tunnistetulle hyökkäysliikenteelle, jotta sitä päästään tutkimaan.

black hole triggered routing,
: asetetaan BGP-protokollalla reititys useisiin reitittimiin niin, että hyökkäysliikenne päästään pudottamaan.

uRPF,
: Unicast Reverse Path Forwarding, keino tulevan paketin lähdeosoitteen oikeellisuuden tarkastamiseksi reititystaulun perusteella.

rate limiting,
: liikenteen määrän rajoittaminen liikenneluokittain, esim. TCP-SYN-hyökkäyksen torjumiseksi.

specific control plane traffic enhancements.
: Tämä viittaa uudehkoihin hankkeisiin, joilla torjutaan reitityksen ja verkonhallinnan liikennettä häiritseviä DoS-hyökkäyksiä.

Sähköposti	
sähköpostin käsittely	[VAHTI 2/2005]
palvelin	[VAHTI 1/2003]
Seittipalvelu: yleistä — turvaaminen — IDS	[Allen Ch. 3, VAHTI 12/2006, seminaariraportti]
Palomuurit	[Allen Ch. 4]

Palvelinten turvaaminen oli esillä 3. luennolla. WWW-palvelulla on runsaasti erityisiä vaatimuksia, minkä vuoksi sitä käsitellään tässä erikseen. Sama koskee jossain määrin sähköpostia, joka otetaan esille kahden VAHTI-ohjeen pohjalta. Luennon loppuosassa käsitellään kahta varsin erillistä aihetta: Allenin kirjan ohjeita palomuurien soveltamiseksi ja Wadlow'n ohjeita auditoinnin järjestämiseksi. Palomuuriasioista on tarkemmin kurssi-Moodlen kautta saatavilla olevan Train2Cert-materiaalin moduuleissa 3 ja 4.¸

Sähköposti

Jo TTP:ssä esiteltiin [id=209] pitkä lista sähköpostiin liittyviä tietoturvakysymyksiä mutta ilman kummoisiakaan vastauksia. Roskapostin suodatuksen teoriaa oli esillä TTJ:ssä [id=92]. Nyt esitellään joitain vastauksia, jotka pitää kuitenkin itse lukea kahdesta VAHTI-ohjeesta.¸

Valtionhallinnon sähköpostien käsittelyohje, VAHTI 2/2005

Suurimmat sähköpostin käytön ongelmat liittyvät sen **monenlaisiin käyttötarkoituksiin** työntekijöiden yksityisestä viestinnästä alkaen sellaiseen asiakkailta tulevaan viestintään asti, johon liittyy **käsittelyvelvollisuuden** piirissä olevia asioita (valtionhallinnossa). Tässä välissä on yrityksen sisäinen ja yritysten välinen viestintä, ja kaikkeen viestintään mahdollisesti sisältyvät **luottamuksellisuus-vaatimukset**, joiden erikoistapauksena ovat henkilötietojen tarpeet.

Tämän mutkikkuuden hallitsemiseksi sähköpostin **käyttötarkoitus** organisaation toiminnan kannalta on syytä määritellä ja toteuttaa sähköpostin käyttöön liittyvät **suojaukset** sekä **käyttöpolitiikka** ja käyttäjien **ohjeistus** sen mukaisesti. VAHTI-ohje 2/2005 antaa yksityiskohtaisia neuvoja erityisesti kahteen jälkimmäiseen. Tietoverkon rakentajan ja turvaajan on syytä tuntea nämä ilmiöt hyvin, vaikka päätöksenteko ei olekaan yksin hänen vastuullaan.¸

VAHTI-ohjeen ytimen muodostaa luku 3, joka **luettelee** 103 suositusta 16 osa-alueella. Edeltävä luku 2 tarjoaa niiden taustaksi selityksiä ja viittaa moneen lakiin, jotka säätelevät sähköpostien ja niiden lokitietojen käsittelyä. Nämä lait esitellään luvussa 4.

Ohjeessa on useita liitteitä, jotka täydentävät suosituksia:

- L1, **suodatusohje** on kaikkein teknisin ja edustaa verkon turvaajan erikoisosaamista.
- L2, **käsittelysäännöt** tarjoaa esimerkin siitä, miten suositukset kannattaa tuoda sähköpostin käyttäjien tietoisuuteen.
- L4 antaa mallin siitä, miten tiedotusta voidaan jatkaa sähköpostin **lopputekstissä**.
- L3 ja L5 esittävät mallit **sopimusteksteiksi**. Ensimmäisellä on tavoitteena sitoutuminen salassapitoon ja toisella suostumus sähköpostien lukemiseen erikoistilanteissa.

Suositusten osa-alueet näkyvät heti sisällysluettelosta. Tässä ne ovat siitäkin vielä tiivistettyinä ja hieman ryhmiteltyinä¸

Sähköpostin
- ja lokitietojen käytön ohjeistaminen ja tiedottaminen
- käytön valvonta
- lokien kerääminen ja säilyttäminen

• Ylläpitohenkilökunta

• Osoitteet
• Osoitteiden julkaiseminen¸

Huomioitavaa, kun käsitellään sähköpostiviestiä, joka on tyyppiä
- Organisaation
- Virka
- Henkilökohtainen
- Muu

- Perille menemätön
- Väärään osoitteeseen saapunut

• Salaus ja todentaminen

• Työntekijän poissaolo
• Palvelussuhteen päättyminen

• Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen¸

Sähköpostipalvelin

Tässä esitellään, mitä Valtion tietohallinnon internet-tietoturvallisuusohje sanoo sähköpostista. Kyseessä on VAHTI 1/2003 ja siihen viitataan jäljempänä termillä **'Ohje'**.

Jos muuhun kuin yksityiseen viestintään tarvitaan **salausta** ja varsinkin **allekirjoituksia**, joudutaan varmistamaan yhteentoimivuus sekä yleisten salaus- ja PKI-standardien kanssa että käytettävien varmennepalveluiden kanssa. Ohje toteaa, että **S/MIME** on suositeltavin standardi sähköpostin salaukseen (Secure/Multipurpose Internet Mail Extensions), mutta ei varsinaisesti hyljeksi PGP:täkään.

Toisin kuin www-palvelun salaus ja autentikointi, sähköpostissa nämä tehtävät eivät kosketa varsinaisesti verkkoturvan rakentajaa, sillä operaatiot tapahtuvat **käyttöliittymän** tasolla. Tietenkin työasemien turvaamistehtävä tuo myös tällaiset asiat hänenkin toimenkuvaansa. Ohjeen liitteessä 2 onkin toistakymmentä toimenpidettä käyttöliittymän asennukseen.¸

Varsinaisesti **verkon turvaajalle** kuuluvat sähköpostijärjestelmän kaksi muuta osaa:
- paikallinen **jakeluohjelmisto**, joka toimittaa lukuprotokollien IMAP tai POP (tai HTTP:n) avulla viestit sähköpostilaatikon ja käyttöliittymän välillä.
- sähköpostin **välitysohjelmisto**, joka yleensä SMTP-protokollaa käyttäen liikuttaa viestejä sähköpostilaatikosta välityspalvelimien kautta kohteena olevaan postilaatikkoon.

Vaikka viestien salaukseen ei otettaisi kantaa, käyttäjän **kirjautuminen jakeluohjelmistoon** pitää toteuttaa turvatusti, erityisesti niin, ettei salasana kulje verkossa selväkielisenä. Sisäverkossakin voi olla perusteltua salata yhteys sähköpostilaatikkoon. Sen voi toteuttaa SSL:llä tai SSH:lla. Haasteellisempi tehtävä on toteuttaa **salattujen viestien virustorjunta**. Ohjeen mukaan siitä tulee huolehtia salauksen purkavalla laitteella, *mielellään ei kuitenkaan omalla työasemalla*. Salaamattomien viestien tarkastus

haittaohjelmien varalta voidaan toteuttaa joko palomuurijärjestelmän tai sähköpostipalvelimen yhteyteen.¸

Tietoturvapolitiikassa voidaan määrätä haittaohjelmavaaran vuoksi rajoituksia sille, minkä tyyppisiä **liitetiedostoja** päästetään sisäiseen verkkoon. Esimerkkiohjeena on dokumenttien ottaminen vastaan vain PDF- tai RTF-muodossa, ja yli 4 megatavun liitetiedostojen jättäminen välittämättä. Pois jätetystä viestistä tai sen osasta pitää kuitenkin tiedottaa vastaanottajalle. Tarkastuksen ja rajoitusten on syytä koskea myös ulospäin lähtevää sähköpostia, jotta esim. CD:ltä saatua tartuntaa ei välitetä muualle.

Roskapostin suodattamisesta Ohje toteaa, että sähköpostipalvelimessa tapahtuva automaattinen viestien poistaminen voi olla liian riskialtista – eikä sitä pitäisi käyttää ainakaan kaikille avoimissa asiointipalveluissa. Toisaalta suositellaan välityspalvelimen konfigurointia siten, että se ei välitä eteenpäin ulkopuolelta lähetettyä roskapostia.¸

Asennusohjeita
Ohjeen liitteessä 2 on mm. **sähköpostipalvelimen asennusohje**. Seuraavassa on tiivistetty siinä olevat kohdat, hieman jäsentäen ja järjestystä vaihtaen.

Ensimmäisellä 8 kohdalla on otsikkona ”Sähköpostipalvelimen ylimääräisten palvelujen karsiminen”.
- asennus järjestelmälle varattuun laitteeseen
- vain tarvittavat palvelut
- pois tarpeettomat palvelut, kuten WWW-mail, FTP tai etähallinnointi
- pois turhat sähköpostikomennot, kuten VRFY ja EXPN (osoitteen ja listan jäsenyyden tarkistus)
- pois kaikki toimittajan dokumentaatio
- pois palveluilmoituksista järjestelmän sovellus-, käyttöjärjestelmä- tai versiotiedot
- kaikki soveltuvat päivitys- ja korjausajot
- soveltuvan turvallisuusasennuksen ajaminen (”hardening script”)

Viimeisen kohdan linnoitusskriptillä pitäisi voida toteuttaa listassa aiempana mainittuja asioita. ¸

Loput 24 kohtaa Ohje jakaa vain osittain osuvasti kahden otsikon alle: ”Käyttöjärjestelmän konfigurointi ja sähköpostipalvelimen pääsynvalvonta” ja ”Liitetiedostot ja sisällöntarkistus”. Seuraavassa tätä jakoa ei ole noudatettu. Lisäksi on merkitty *:llä kaksi kohtaa, joiden merkitys jää hieman epätarkaksi jo Ohjeen perusteella.¸

— sähköpostin **palvelinohjelman**
- pääsy tietokoneen resursseihin rajoitetuksi; oma rajattu tiedostoalue
- oma käyttäjätunnus, jolla minimioikeudet
* pääsyoikeuksien vahvemman tarkastelun mahdollistaminen, mikäli niitä tarvitaan
* tarkistus, ettei sitä ei ajeta pääkäyttäjän tunnuksin (root, admin)
- lokitiedoille vain kirjoitus
- lokitiedostolle riittävästi tilaa
- väliaikaistiedostoille riittävät, mutta rajoitetut oikeudet,
- sähköpostipalvelun omistukseen
- tiedostojen kirjoitus vain siihen varatulle alueelle
- chroot Linux- ja Unix-järjestelmissä
- sähköpostilaatikot eri levyille ja levypartitiolle kuin KJ ja sähköpostisovellus¸

— virustorjuntajärjestelmä
- keskitetty (sähköpostin välityspalvelimelle, palomuuriin tai sähköpostipalvelimelle)
- kaikille työasemille
- tietokantojen päivitys säännöllisesti ja riittävän usein
- käyttäjien koulutus: virusten vaarat, ja aiheutuneiden häiriöiden minimointi
- informoi käyttäjiä, jos virustorjunta on pettänyt¸

— sisällönsuodatus
    - politiikka
    - rajoitus liitetiedostojen koolle
    - epäilyttävät viestit pois
    - roskapostiviestit pois
    - ei hyväksytä sähköposteja palvelimilta, jotka ovat ns. mustallalistalla
    - tietyistä osoitteista tulevat sähköpostit pois (tarvittaessa)
— suojauksia
    - autentikoinnin vaatiminen jälleenlähettäville posteille
    - autentikointitietojen salaaminen
    - www-yhteyksien tukeminen vain, jos ne ovat aivan välttämättömiä ja silloin suojattuna SSL/TLS:llä.¸

WWW-palvelin

Yleistä

WWW-palvelimen kautta toteutetaan perinteisesti tiedonjakelua. Sittemmin käänteinen tiedonkulun suunta on tullut yhä tärkeämmäksi, kun seitin kautta on luotu liittymiä monenlaisiin ohjelmiin, mm. sähköpostiin ja tietokantoihin, kuten vaikkapa pankkitileihin. Niissä ja monissa kaupankäynnin sovelluksissa hoidetaan kokonaisia transaktioita yhden tai useamman seitti-istunnon kautta. Tässä ei käsitellä tällaisten kokonaisuuksien turvallisuutta. Näkökulma on seittipalvelun tarjoajan ja kohteena on torjua seuraavanlaisia uhkia:

- palvelu estyy tai jumiutuu. Ohjautuminen jonnekin muualle on mahdollista, mutta se ei ole palvelun hallinnassa.
- palvelu sisältö vääristyy, esim. häpäistyy tai toimii virheellisesti.
- luottamuksellisia tietoja paljastuu palvelusta (tai sen taustajärjestelmistä, vrt. seuraava)
- palvelun kautta murtaudutaan muualle kuin siihen itseensä: palvelin itse, yrityksen muu verkko, jokin muu verkko.¸
-

Uhkien toteutumisen seurauksena voi olla

- liiketoiminnalliset tappiot,
- korvausvastuu paljastuneista tiedoista tai
- siitä, että alustalta on murtauduttu muualle

Voisi olla kiinnostava keskustelunaihe katsoa,

- mitä kaikkea seittipohjaista toimintaa oikeastaan on olemassa,
- mitä siitä pitäisi palveluntarjoajankin kannalta suojata ja
- mitä muuta siihen tarvitaan kuin tässä tulee esille.

Yksi esimerkki on DRM, Digital Rights Management. Toinen, joka näyttäisi tosin vain selaajan intressiltä, on anonymiteetti. Jos se on palvelun ideana, täytyy palvelun tarjota sitä vakuuttavalla tavalla.¸

WWW-palvelinten turvaaminen (+VAHTI 12/2006)

WWW-palvelimen turvaamismenettely on yleisesti:

Tietoturvallisen palvelimen **asennus** – palvelinohjelmiston ja käyttöjärjestelmän turvallinen **konfiguraatio** – palvelimen eheyden **ylläpito**.

Palvelimen turvaamisen lähtökohtana on siis tietoturvallinen ”peruskonfigurointi” kuten palvelimille yleensäkin. Monet näistä aiemmin esillä olleista asioista kertautuvat jatkossa ”varsinaisen” konfiguraation yhteydessä.¸

WWW-palvelimen eristäminen (§3.2)

- eristetty aliverkko: ulkomaailman ja palvelun välinen liikenne ei kulje sisäverkossa.
- palomuuri; www-palvelimelta ei yleensä tarvita ulospäin TCP-yhteyksiä, UDP-yhteys DNS:ään voisi olla samassa (DMZ-)verkossa tai sisäverkossa olevaan palvelimeen, josta vasta on yhteys ulospäin.
- tukipalveluiden palvelimet toiseen eristettyyn aliverkkoon: tässäkin siis palvelinten välinen liikenne erillään sisäverkosta. [→ kuva 3.2]
- source routing ja IP-edelleenlähetys pois käytöstä, myös tukipalveluista.
- vaihtoehtoiset arkkitehtuurit: liikenne voidaan keskittimillä ja kytkimillä pystyä eristämään vaikka www-palvelin olisi sisäverkossakin, paitsi murtautumistapauksissa. Palvelin voi olla myös ulkoistettu. Tällöin yhteys mahdollisesti omassa verkossa olevaan tietokantaan tms. pitää suojata esim. VPN:llä, joka tapauksessa vahvalla autentikoinnilla ja salauksella.
-

Palvelimeen rajoitukset laitteiden, tiedostojen ja muiden kohteiden käytölle (§3.3)

- Kaikki palvelimellakaan oleva tieto ei ole julkista.
- Palvelinta varten oma käyttäjä- ja ryhmätunnus
- Suojaussäännöt käyttöjärjestelmän toteutettavaksi:
  - palveluprosessi voi vain lukea sivuston sisällön muodostavia tiedostoja ja
  - ei kirjoitusta samoihin hakemistoihin;
  - lokitiedostoille vain kirjoitusoikeus, luku vain ylläpitoprosesseille;
  - väliaikaiset tiedostot erityiseen hakemistoon ja
  - niihin pääsy vain prosesseilla, joka on ne luonut.

- DoS-hyökkäysten tehon vähentäminen, ”hengissäpysyttelyä”:
  - verkkoyhteyksien aikakatkaisu minimiajalla;
  - tasapaino yhtäaikaisten TCP-yhteyksien (avoin ja ½-avoin) sallitulla määrällä (pieni – suuri);
  - prioriteetteja palveluprosesseille;
  - ei kirjoitusoperaatioita (ja lokit eri paikkaan)

- sisäiseen käyttöön tarkoitettujen tietojen suojaus: ei tarjolle sivuja tarkoitetun hakemiston ulkopuolelta symbolisten linkkien eikä alias-nimien kautta, ohjelmalta pois mahdollisuus tällaisten seuraamiseen

- palvelinohjelmiston tarjoamien käyttökontrollien konfiguroinnin askeleet:
  - sivustolle (ja vain sille, ei esim. cgi-skripteille) hakemisto alihakemistoineen
  - erillinen hakemisto sisältöön liittyviä ulkoisia ohjelmia varten
  - em. hakemiston käyttöoikeuksien avulla voidaan myös estää sellaisten cgi-skriptien suoritus, joita eivät ole ylläpitäjän hallinnassa
  - tiedostolinkkien käytön estäminen (siis sama kuin ed. kohdassa)
  - sivuston sisällön täydellinen käyttöoikeustaulukko – oikeuden laji voi esim. Apachen `Limit`-direktiivissä olla mikä vain HTTP-metodi paitsi trace, esim. `<Limit POST PUT DELETE>Require valid-user</Limit>`. Tämä sallii muut metodit. `LimitExcept` toimii toisinpäin ja on siksi suositeltavampi. (http://httpd.apache.org/docs-2.0/mod/core.html)
- palvelimen hakemistolistaukset pois käytöstä
-

WWW-palvelimen lokitiedot ja -mekanismit (§3.4)

- mistä tiedoista kerätään lokia
  - tapahtumaloki, CLF (common log format): etäisäntä, etäkäyttäjä, tunnistettu käyttäjä (RFC1413), pvm, URL, pyynnön tila, siirretty tavumäärä. Muissa tapahtumalokin muodoissa (combined ja extended) mukana myös seuraava kaksi:
  - selaintyyppiloki: millainen selain
  - viittausloki: mistä selain linkittyi

    - virheloki, voi olla erillään tapahtumalokista
- täydentäviä lokitietoja voidaan tarvita ulkoisten ohjelmien toiminnasta
- lokin keruun käyttöönotto: suosituksena combined log format, jos se on käytettävissä; lisäksi käyttäjän tunnistetieto, ellei se hidasta liikaa
- lokin analysointityökalut, valinta ja konfigurointi.
-

Ohjelmien, skriptien ja plug-in-lisäkkeiden vaikutus turvallisuuteen (§3.5)

Yhteisnimellä (www-palvelimen) *ulkoiset ohjelmat*: cgi-ohjelmat ja -skriptit, plug-in -ohjelmat, servletit ja sellaisten kielet. Niillä voi tuottaa ainutlaatuisia testaamattomia yhdistelmiä ja konfiguraatioita. Siispä:

- kustannus-hyöty -vertailu; turvallisuuden lisäksi ylläpito kaikkineen
- toimittajien luotettavuus?
- ulkoisten ohjelmien kaikkien toimintojen tunteminen, ehkä lähdekoodin perusteella:
    - tiedostojen käsittely?
    - vuorovaikutus muiden ohjelmien kanssa (esim. sendmail)?
    - viittaukset ohjelmiin mieluimmin täydellisen eikä suhteellisen polun avulla
    - syötteidensä tarkistaminen?
    - suid-oikeudet?
- turva-aukoista voi olla tietoa julkisesti saatavilla – ei ole syytä jättää sitä vain hyökkääjälle.
-

Ulkoisten ohjelmien toiminnallisuuden minimointi (§3.6)

Ulkoisen ohjelman voi ottaa käyttöön muuttamatta palvelimen koodia.

- ulkoisesta ohjelmasta hankitun kopion aitous on varmistettava
- eristetty testikone
- turva-aukoille altistumisen rajoittaminen siivoamalla käyttäjän syöttämästä datasta mm. meta- ja escape-merkit
- palvelin voi levittää vahingollista koodia haitallisesti muodostetun kutsun takia. Estämiskeinoja: output-elementtien koodauksen purku, sisällön suodatus, evästeiden tarkistus.
- Server Side Include-komennot pois käytöstä tai rajoituksia – ainakin ulkoisten ohjelmien osalta (esimerkki SSI:stä : `Viimeksi muokattu <!--#flastmod file="index.html" -->`).
- palvelimen konfiguraatioon sisältyvät ulkoisten ohjelmien kutsut pois – esim. esimerkkiohjelmat
- ulkoisiin ohjelmiin pääsyn rajoittaminen: cgi-bin -hakemistossa ei tulkkeja eikä laajennettavia ohjelmia, eikä mitään arvattavan nimistä mitä ei tarvita
- pääsy ulkoisiin ohjelmiin vain valtuutetuilla käyttäjillä; erityisryhmä kotisivujensa ylläpitäjät
- ulkoisten ohjelmien suorittamiselle yksilölliset käyttäjä- ja ryhmätunnukset, erilaiset kuin tavalliseen palveluohjelman käyttöön
- ulkoisen ohjelman pääsy vain välttämättömiin tiedostoihin
- ulkoisten ohjelmien eheyden tarkistus, luotettavan lähtötilanteen taltioinnin perusteella
-

Todennus- ja salaustekniikat palvelimessa (§3.7)

- lähtökohtana tarve rajoittaa joidenkin tietojen käyttäjäkuntaa – yksilöittäin, ryhmittäin tai tilauksen perusteella.
- luottamussuhde käyttäjien ja palvelimen välille: *välttämättä* autenttisuus ja eheys, *todennäköisesti* luottamuksellisuus, *mahdollisesti* kiistämättömyys, *toivottavasti* saatavuus.
- osoitepohjainen todennus on rajoittunutta (mutta käytössä)
- todennus- ja salaustekniikoita:
    - perustodennus, ’Basic Auth.’, ei luottamuksellisuutta – edes salasanalle
    - SSL, suositus, jos luottamuksellisuutta tarvitaan;
      selain-palvelin -väli; ulottaminen käyttäjään ei suoraviivaista;
      tämä on myös keino suojata käyttäjiä valesivustoilta (etenkin ”kalastelusivuilta”).
    - Secure HTTP, SSL:n edeltäjä ja monipuolisempi mutta jäänyt taustalle.
    - SET, luottokorttimaksamisen protokolla, jäänyt taustalle. Suojaa palvelimen tietomurrolta, sillä korttitiedot eivät edes tule sen näkyville.
- SSL:n käyttöönotto

    - palvelimelle julkinen avain ja varmenne jakeluun tarvitsijoille tai (laajaan käyttöön) varmenteen hankkiminen luotetulta taholta, jonka mahdollisesti selaimet jo tuntevat.
    - käyttäjän perustodennus SSL:n suojissa tai
    - asiakasvarmenteen perusteella, mieluimmin niin, että se sijaitsee käyttäjäkohtaisella toimikortilla eikä selainkoneessa.
- muita ”salaustapoja”
    - Digest authentication: haaste-vaste -menetelmä MD5-algoritmilla parantaa perusautentikointia toistohyökkäystä vastaan, kunhan haasteet eivät toistu.
    - PGP-allekirjoitus HTML-kommentissa sivun aitouden toteamiseen.
    - vesileimaus: selaimella toimiva tarkistusohjelma voi saada käsityksen aitoudesta (lähinnä kuvat ja äänet, ei teksti). Soveltuu enempi tekijänoikeuksien vahtimiseen¸

Edellä annettujen teknisten ohjeiden täydennykseksi ja sitomiseksi sovellustasoon **LUE luvut 4 ja 5 VAHTI-ohjeesta Tunnistaminen julkishallinnon verkkopalveluissa (**12/2006**).** Tämä ohje ei juurikaan tekninen, mutta omalla alallaan se täydentää, täsmentää ja päivittää hyödyllisesti TTJ:ssä luettua Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohjetta VAHTI 4/2001 (id=477).

Aiemmissa kursseissa ei ole toistaiseksi ollut esillä phishing-hyökkäysten torjunnan mekanismeja. Niistä eivät myöskään kurssin lähdeaineistot puhu. Ne koskevatkin enemmän selaajaa eivätkä suoranaisesti verkon turvaajaa. Silti verkon politiikassakin voisi olla mukana ohjeita tai suosituksia jonkin hyväksi havaitun kalasteluntorjuntavälineen käytöstä esim. samassa yhteydessä, jossa käsitellään etätyöpisteen turvallisuutta. (Aihetta käsitellään syksyn 2008 seminaarissa TLT-3600.) ¸

Virallinen kopio sivustosta turvallisella isäntäkoneella (§3.8)
Eri asia kuin varmuuskopio, mutta ongelmatilanteissa ajaa saman asian. Vaatii ylläpitoa ja tyypillisemmin onkin lähde, josta julkinen versio päivitetään. Tallessa on hyvä olla myös aiempia versioita ja päivitysten historia. Virallisen version turvapiirteitä:

- käyttäjien pääsy rajoitettua; koulutustakin tarvitaan
- käyttöoikeuksien säätelyssä hakemistorakenne julkisen puolen tapaan (tai monipuolisemmin)
- vahva käyttäjän tunnistus; erityishuomio etäkäytettävien muokkausvälineiden tapauksessa
- todennetut ja salatut yhteydet www-palvelimeen:
    - yhteys käynnistetään turvalliselta koneelta päin
    - palomuuriin säännöt, jotka sallivat vain virallisen sivuston siirtämisen
    - siirrettävän sisällön salaus ja todennus
    - lisärajoituksia, mm. milloin siirto saa tapahtua
- manuaalinen varamenettely sivuston siirtoon, myös siten, että CD-ROM tai vastaava ladataan verkoitse joltain kolmannelta palvelimelta.¸

Tunkeutumisen havaitseminen WWW-palvelimessa

Otsikko on peräisin viime luennossa esitellystä IDS-seminaariraportista, luvusta 9 (= ”**LUE**”). Se perustuu kahteen artikkeliin (Almgren ym., 2000 ja Ryutov ym., 2003). Kumpikin esittää www-palvelimeen asennettavan havaitsemisjärjestelmän, joka voi toimia vaihtoehtona tai täydentäjänä NIDS-järjestelmälle. Menetelmä perustuu epäilyttävien sormenjälkien paikallistamiseen HTTP-pyynnöistä, tyypillisesti HTTP-pyynnön URL-osoitteista. Seuraavassa on lainaus luvun 9 yhteenvedosta (kirjoittajana Mikael Lindén):¸

Almgren on toteuttanut tunkeutumisen havaitsemisjärjestelmän, joka prosessoi Apache-palvelimen tuottamaa lokitietoa joko lennosta tai eräajona. Ryutov on niveltänyt tunkeutumisen havaitsemisen HTTP-palvelimen pääsynvalvontaan, ja korostaa, että tällöin epäilyttävät HTTP-pyynnöt voidaan muitta mutkitta evätä ennen kuin vahinkoa tapahtuu. Ryutov näkee WWW-

palvelimen osana organisaation tunkeutumisenestoinfrastruktuuria, jonka kanssa WWW-palvelin voi vaihtaa tietoa havaituista tunkeutumisyrityksistä ja tarpeellisista vastatoimista. Molemmat kirjoittajat näkevät WWW-palvelinpohjaisessa tunkeutumisen havaitsemisessa runsaasti etuja verrattuna verkkopohjaiseen tunkeutumisen havaitsemiseen.

Ryutovin järjestelmä on saatavana vapaan lähdekoodin ohjelmana. Sen ansiosta järjestelmän ylläpitäjät voivat halutessaan toteuttaa lisää tarpeelliseksi katsomiaan toimintoja sen lisäksi, että he voivat säätää EACL-sääntöjä (extended ACL).¸

Palomuurit

Yleistä

Eri lähteiden mukaan palomuuri on joko
prosessi,
laitteiden ja ohjelmistojen yhdistelmä, tai [Allen, Ch. 4]
tietokone, [Bishop, Ch. 26]
joka välittää pääsyn tietoverkkoon (hoitaa pääsynvalvonnan), estämällä tai sallimalla tietyn tyyppiset pääsy-yritykset perustuen turvapolitiikkaan, joka siihen on asetettu (eli konfiguroitu).¸

Suodattava palomuuri toteuttaa pääsynvalvonnan estämällä tai päästämällä lävitseen tietynlaiset paketit. Päätös tehdään pakettien otsikkotietojen perusteella pääsylistoissa ilmaistujen sääntöjen mukaan. Sovellustason välityspalvelimena (proxyna) toimiva palomuuri voi tehdä myös näin, mutta oman luonteensa mukaisesti se tavallaan *estää kaiken läpäisyn*. Sen sijaan se lähettää omissa nimissään eteenpäin sen liikenteen, joka pakettien sisällön perusteella on politiikan mukaista.¸

Palomuuri on jotain, joka sijoitetaan verkon erilaisten osien välille. Erilaisuus tässä yhteydessä on tietoturvapolitiikan erilaisuus. Tyypillinen eriävyys on julkisen ja yksityisen verkon välillä, mutta myös yrityksen verkon sisällä voi olla erilaisia osia, ja isossa yrityksessä varmasti on. Sellaisiin voi riittää verkkoja muutenkin eriyttävän reitittimen toiminnallisuus. Toisaalta nimenomaan turvallisuuden kannalta erilainen tarve muodostuu julkisen ja yksityisen verkon välimaastoon, jossa tarjotaan palvelua ulospäin käyttäen sisällä olevia tietojärjestelmiä. Tällainen vyöhyke on nimeltään DMZ, demilitarized zone, mutta se on yhtä vähän ”aseeton” kuin verkko muutenkaan, esimerkiksi autentikoinnin tai fyysisen pääsyn osalta. DMZ:ssa voi olla esim. sähköpostipalvelin ja www-palvelin, ja DMZ:n omiin tarpeisiin nimipalvelin. Omanlaisensa alue voi olla myös extranet, joka toimii esim. yrityksen yhteistyö-kumppaneiden välisenä sisäverkkona.¸

Palomuurijärjestelmän yleinen rakenne:
- Varsinaisen suodatuksen toteuttavia laitteita voi olla useita, joiden välillä on kuormanjakoa.
- Politiikan tallentamiseen voi olla oma komponenttinsa, joka siis hallinnoi suodatusosia. Se voi vastaanottaa ja taltioida niiden lähettämät lokitiedot.
- Ihmiskäyttöön on sovelluksia, yhtäältä politiikkojen ja toisaalta lokitietojen käsittelyyn.

Tällainen on jaottelu mm. Check Point’in FireWall-1:ssä. Sieltä on lähtöisin myös API-määrittely Content Vectoring Protocol (CVP). Se määrittelee asynkronisen liittymän, jolla erityyppiset palomuurit voivat välittää paketteja erilliselle palvelimelle, joka suorittaa sisällön tarkastuksen ja lähettää luvalliset paketit eteenpäin – siis sovellusvälityspalvelimen tapaan. Erityisesti kohteena on haitallinen koodi.¸

Toisen esimerkin palomuurijärjestelmän rakenteesta tarjoaa Ciscon Centri-palomuuri, jonka dokumentaatio esittelee seuraavat hierarkkiset osat:
- Turvallisuusjärjestelmä
  - Turvaydin

- Pakettien noukkija ja analysoija
- Turvatodennuksen moottori (security verification engine, SVEN), joka päättää pudotetaanko paketti, kuuluuko se avattuun yhteyteen vai perustetaanko sitä varten uusi.
- Ytimen proxyt, jotka luovat palomuurin sisälle protokollapinon (IP, ICMP, TCP, UDP, HTTP, SMTP, Telnet, FTP)

  - Kommunikointikanavia ydin- ja sovellustason välillä (Controlled Host Component and Communications Channels)
  - Lokinkeruuagentti
  - Autentikointiagentti, jonka kohteena voi olla muitakin kuin *palomuurin* käyttäjiä.
- Raportointijärjestelmä (generointia, ajastusta ja katselua)
- Monitorointijärjestelmä (poikkeamien ym. havainnointia varten)
- Hallinta-agentti
- **Turvatietokanta**, joka on yhteydessä em. neljään pääkomponenttiin¸

Vaikka tämä koskeekin tiettyä tuotetta, jossa korostetaan agenttitoiminnallisuutta, vastaavat toiminnat hienontavat yleensäkin edellämainittua palomuurin sisäisen rakenteen jaottelua. Tuonnempana käsiteltävä *topologia* puolestaan koskee ylemmän tason arkkitehtuuria.

Jos tavoitteena on, että sovellustason protokollat voisivat turvallisesti ja läpinäkevästi läpäistä, voidaan käyttää ns. kytkentäistä palomuuria (circuit firewall). Sellainen toteutuu SOCKS-protokollalla siten, että sovellusohjelmat käärivät datansa SOCKS-kirjaston tarjoamien rutiinien avulla ja yhteensopivat palomuurit pystyvät autentikoimaan liikenteen ja jatkossa laskemaan (releöimään) sen lävitseen. Palomuuri on siis SOCKS-palvelin, TCP-portissa 1080; myös UDP:tä voi käyttää.
(ftp://ftp.funet.fi/pub/standards/RFC/rfc1928.txt, versio 5, 1996)¸

Topologioista eli arkkitehtuurista

- Yksi laite kahden verkon välissä (”basic border”)
- Samassa laitteessa kolmas verkkoliityntä DMZ:aa varten
- Kaksitasoinen arkkitehtuuri: DMZ kahden palomuurin välissä.
- Useampitasoisuus on mahdollista, esim. lokiverkon näkökulmasta sisäverkko on jo ulompana.¸
-

Valintaperusteina on kustannusten ja hyötyjen vertailu seuraavilla osa-alueilla:

- Käytettävyys: komponenttien luotettavuus + varajärjestelmä (kuuma–lämmin–kylmä)
- Suorituskyky: mahdolliset kahdennukset (rinnakkaiset laitteet)
- Turvallisuus, vertailu erityisesti yksi- ja kaksitasoisen palomuurin välillä. Kahdesta palomuurista on ilmeisesti
  - lisäetuja turvallisuuden lisäksi: toisen irrottaminen verkosta voi olla mahdollista murtotapauksissa, liikenteen valvonta monipuolisempaa, mahdollisuus käyttää eri valmistajien tuotteita
  - lisäkustannuksia: laitteistot sinänsä, vikatiheys, verkkoporttien tarve
  - ”joko tai”, eli ei niin ilmeistä kummin päin: suorituskyky, hallinnan ja ylläpidon mutkikkuus.¸

Palomuurin käyttö(önotto)

Tässä esitellään Allenin kirjan luvun 4 ohjeisto.

Palomuurin käyttöönottomenettely (§4.1.2)

Jäljempänä lueteltavat vaiheet ovat tiivistettyinä nämä:

- valmistelu: suunnittelu – hankinta (myös tuen) – koulutus
- konfigurointi: asentaminen – IP-reititys – pakettien suodatus – lokit ja hälytykset
- testaus
- käyttöönotto¸

Suunnittelu (§4.2)

- ympäristön dokumentointi (”ellet pysty piirtämään sitä et pysty rakentamaan sitä”)
- palomuuritoimintojen valinta:
  - pakettisuodatus; reititin vai yleiskäyttöinen alusta?
  - sovellussuodatus
  - NAT
  - DoS-suoja
  - ACL:t ja autentikointi
  - VPN-tuki
  - lokien keruu
  - IDS
- topologian valinta kustannus-hyöty -vertailun perusteella
- suojaus luvattomalta käytöltä (normaalit: käyttöoikeudet, autentikointi + fyysinen suoja)¸
-

Palomuurilaitteiston ja -ohjelmiston hankkiminen (§4.3)

- laitteistokomponentteja: prosessorit, muisti, levytila, verkkokortit, laitteet asennukseen, testaukseen, varmistukseen, hallinnointiin, fyysinen tila, virtaa, kaapeleita, muu verkko, viestivälineet, varaosat
- ohjelmistokomponentteja: käyttöjärjestelmä, laiteajurit, palomuuriohjelmisto, tukiohjelmistot, generointi- ja analysointityökalut, korjaukset ja päivitykset kaikkiin
- heti kun kaikki tarpeellinen on luultavasti saatu, ”esiasennuksella” voi ehkä havaita puutteet ajoissa.¸
-

Palomuuria koskeva koulutus, (dokumentaatio) ja tuki (§4.4)

- Osaamisalueita: TCP/IP, palvelut, reititys, arkkitehtuuri, verkonhallinta, palomuurin laitteisto ja ohjelmisto, asennus, ylläpito, turvallisuus, varmistus, toipuminen, auditointi, lokijärjestelyt + valvonta.
- Tuen palvelutasosopimus: miten pitkään, miten, mihin aikaan, kuka saa, erityisongelmat, maksuperusteet, toimitusehdot (esim. tuorein versio ja paikkaukset).¸
-

Asenna palomuurilaitteisto ja -ohjelmisto (§4.5)

- asennus tuotantolaitteistoon, joka on testiverkossa
- pienin mahdollinen käyttöjärjestelmäkokoonpano: joko poistamalla ylimääräiset tai asentamalla vain tarvittavat. Jotkin palomuurien asennusohjelmat tekevät itse edellisen.
- kaikkien soveltuvien korjausten asentaminen. Päivitysten asentamisessa jo toimivaan järjestelmään on hyödyksi, jos on olemassa kuuma varajärjestelmä (kuten suositellaan).
- käyttäjien ja isäntäkoneiden pääsyn rajoittaminen ja vahvan autentikoinnin vaatiminen myös sisäpuolelta
- ohjelmiston käynnistyessä suodatuksen pitää tulla ensin käyttöön ja reitityksen vasta sitten
- varmuuskopio järjestelmästä asennuksen päätteeksi
- asennuksen toistaminen ja sen jälkeen dokumentointi ja (asennuksen kannalta) ulkopuolisen suorittama dokumentaation katselmointi
- jos jokin menee vikaan, asennusta voidaan joutua ensin tutkimaan monipuolisemmalla laitteistolla ¸
-

IP-reitityksen konfigurointi (§4.6)

- erillään operatiivisesta verkosta
- kaksitasoisessa ulompi palomuuri reitityksen osalta mutkikkaampi kuin sisempi, mutta sääntöjen osalta yksinkertaisempi¸
-

Pakettisuodatuksen toteutus (§4.7)

Sääntöjen päättäminen, dokumentointi ja asentaminen.

Päättäminen. Suunnitteluprosessi:

- viimeisenä sääntönä kaiken kieltäminen
- väärennettyjä osoitteita torjuvat (anti-spoofing-) säännöt listan alkuun. Voidaan ehkä saada automaattisesti reititystauluista.
- käyttäjien tarpeiden kartoitus tuottaa listan sallittavista lähde- ja kohdeosoitteista, protokollista ja porteista.
- pois listasta ne, joita politiikka ei salli. Tähän voivat kuulua myös sisältä avattujen TCP-yhteyksien paluupaketit, jos ei luoteta TCP-toteutusten eheyteen.
- lajittelu protokollan ja portin mukaan
- tiivistys peräkkäisten porttinumeroiden vaihteluvälin avulla¸

Dokumentointi. Jokainen sääntö pitää perustella ja suhteuttaa turvapolitiikkaan – ei pelkästään verkon rakenteeseen. Sääntöjen ryhmittelystä on apua. Toisaalta suorituskyvyn parantamisen takia tehdyt yhdistelyt vaikeuttavat ja vaativat siis entistä huolellisempaa dokumentointia. Versionhallinta auttaa, kun on tehty virheitä.

Asentaminen on iteratiivinen prosessi, jossa uusia sääntöjä lisätään ja tarkastellaan miten ne asentuvat ja testautuvat.¸

Palomuurin loki- ja hälytysmekanismit (§4.8)

Kohteena on kahdentyyppistä tietoa: pakettien kohtalo ja järjestelmän oma toimivuus. Lokien keruuseen suositellaan (tässäkin) erillistä verkkoa. Sinne neuvotaan siirtämään palomuuriin itseensä aluksi talletetuista lokeista tärkeät ja sellaiset, joita tullaan käyttämään. Silti levytilaa ei suositella säästelemään.

Pakettisuodatussääntöjä koskevien lokien täytyy olla tarkoituksenmukaisia: on tiedettävä, miksi niitä mistäkin säännöstä kerätään – jos kerätään. On mahdollista, että lokiasetukset ovat erilaiset eri vuorokaudenajoille tai sen mukaan, putoaako paketti ollessaan tulossa tai lähdössä (suhteessa palomuurijärjestelmään).

Lokitiedostojen täyttymisen kolme ratkaisua (§4.9.5): suosituksena yhteyksien katkaisu (ja tietenkin hälytys), vanhimpien päällekirjoitus, jatko ilman keruuta (!).¸

Hälytysmekanismin asetukset

- epäonnistuneet sisäänkirjautumiset palomuurin läpi
- onnistuneet kirjautumiset palomuuriin
- suotimien ja joidenkin tiedostojen muutokset
- käyttötapahtumat: lähellä oleva lokin täyttyminen, uudelleenkäynnistymiset
- suositus: hälytyksen lähetys keskitetyltä palvelimelta joka hoitaa myös lokipalvelimen hälytykset

Tarvitaanko lokien arkistointia; jos kyllä, se tarvitsee mekanismien lisäksi määräajat ja hävityssäännöt.¸

Testaus (§4.9)

Kohteita: politiikka ja sen toteutus; reititys, suodatus, loki ja hälytykset, häiriöistä toipuminen, suorituskyky. ”Sivullisen” suorittama turva-auditointi on tärkeää palomuurien testauksessa.

- testaussuunnitelma: säännöt muodostavat alueita moniulotteiseen ”pakettiavaruuteen”. Testiliikennettä pitäisi tuottaa joka ulottuvuudessa kolmenlaista: sallitun alueen ala- ja yläpuolella sekä alueen sisällä. Ei useinkaan mahdollista käytännössä.
- testaustyökalut: liikennegeneraattorit (SPAK, ipsend, ...), valvontatyökalut (tcpdump, ...), porttiskannerit (nmap, ...), turva-aukkojen etsintä (nessus, ...), IDS (snort, ...)
- testiympäristössä: palomuuri eristettyjen koneiden välissä, lokikone erikseen jos niin on tarkoitus; ensin reitityksen tarkistus ilman pakettisuodatusta, sitten suodatuksen tarkistus kaikesta mahdollisesta liikenteestä; avoimien ja suljettujen porttien skannaus; lokitietojen tutkiminen: onko merkintä tehty ja onko asianmukainen hälytys tehty.¸

- tuotantoympäristössä: muuten samaan tapaan kuin edellinen, mutta ei liikenteen generointia, vaan snifferin käyttö ja sitä kautta vastaava varmistus siitä, että suodatus toimii. Lisäksi kyllä hyökkäysten tunnistustyökaluja myös generoitua verkkoliikennettä vastaan pidemmän ajan kuluessa. Suosituksena on myös tuotantoympäristön yhteyksien vaiheittainen avaaminen (vrt. käyttöönotto) [→ s. 168–169]
- lokit: erikseen testataan täyttymisen hoituminen
- palomuurijärjestelmän testaus häiriö- ja virhetilanteiden varalta
- haavoittuvuuksien skannaus (toiminnan aikana)
- regressiotestiaineistoksi osajoukko varsinaisista testeistä, myös palvelukohtaista liikennettä. Näillä voidaan testata toiminnan kuluessa tehtyjä muutoksia.
- tuotantokäyttöön valmistaminen: lähtötasotiedot talteen ja konfiguraation varmuuskopio.
- jatkuvaan valvontaan valmistautuminen: politiikasta alkaen asialle varattuun työaikaan asti.
-

Palomuurijärjestelmän asennus ja käyttöönotto (§4.10–11)

Menettely riippuu siitä,

- korvataanko tai täydennetäänkö järjestelmällä vanhaa vai luodaanko sillä kokonaan uusi yhteys kahden verkon välille.
- käytetäänkö samoja vai eri IP-osoitteita kuin aiemmin,
- kerrotaanko muuttuneet osoitteet palvelimille
  - käsin;
  - reitityksenhallintaprotokollilla: RIP tai OSPF;
  - asiakastason hallintaprotokollalla: DHCP

Käyttäjille pitää myös kertoa uusista osoitteista.

Esimerkki. Alunperin on yksitasoinen palomuuri, joka kytkee sisäverkon, yrityksen ulkoverkon ja muun maailman. Tästä siirrytään kaksitasoiseen ottamalla tuo ulko-osa kahden palomuurin väliin (DMZ:aan). Siirtymä, jossa aiempi palomuuri jää ulommaksi, tehdään seuraavasti: [→ kuva 4.11 = T2C_4.4.2.3]

- sisäinen ja ulkoinen verkon osa kytketään uuteen palomuuriin,
- joka ilmoitetaan sisäverkon palvelimille oletusreitittimeksi ja
- jolle ulkoverkon palvelimet ohjataan reitittämään sisään menevä liikenne
- ja samoin ohjataan vanha (ulommaksi jäävä) palomuuri,
- siltä irrotetaan liityntä sisäverkkoon, kunhan on todettu että liikenne reitittyy ja suodattuu halutulla tavalla

Edellä mainitun Cisco-palomuurin dokumentaatiossa tiivistetään perusasennuksen ja -konfiguroinnin prosessi seitsemään tehtävään:

1. Määrittele hallinnolliset käyttäjätilit.
2. Pystytä verkko-oliot.
3. Määrittele verkon palvelut.
4. Määrittele käyttäjien autentikoinnin politiikat.
5. Määrittele turvallisuuspolitiikat.
6. Ota turvallisuuspolitiikat käyttöön.
7. Pystytä raportointi ja monitorointi.

Nämä vaiheet täytyy tietysti ymmärtää palomuurin tehtävän kannalta. Tämä luettelo ja kyseinen n. 10-sivuinen dokumentti eivät puutu lainkaan testaukseen, varmuuskopiointeihin ym. menettelyihin, joista edellä on ollut puhe.

TLT-3301 Verkon tietoturva, 5. luento 15.12.2008

Tietoturvapoikkeamatilanteiden hallinta [= VAHTI 3/2005]

Tunkeutumisiin reagoinnin prosessi [Allen, Ch. 5- ja 6-osia + Ch. 7]
Täydennyksiä [Wadlow, Ch. 12-13-14-16]
Viittauksia muihinkin lähteisiin:
D.Brezinski, T. Killalea:
The Guidelines for Evidence Collection and Archiving, RFC3227
T. Grance, K. Kent, B. Kim:
Computer Security Incident Handling Guide
NIST Special Publication 800-61
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
VAHTI-ohjeen ja muiden lähteiden tarkastelua kertauksen tapaan. (LUE) ¸

Tämän luentokerran aiheisiin liittyy kaksi vierailuesitelmää:
”Tietojärjestelmäsodankäynnistä”
Tästä tai muualta pitää oppia ainakin:
Millaisia eroja perinteisellä ja verkkosodankäynnillä voi olla?
Millaisia haavoittuvuuksia tietoyhteiskunnassa esiintyy?
Millaisia haavoittuvuuksia turvajärjestelmien omissa infrastruktuureissa voi olla?
”Tunkeutumisten jäljittämisestä ja oikeustoimien edellytyksistä”
Tästä tai muualta pitää oppia ainakin:
Mitä puolustaja saa itse tehdä ulkopuolisia hyökkääjiä tai omia työntekijöitä vastaan; mitä poliisi saa tehdä?
Rikosnimikkeet – ja niiden käytännön esiintyminen.
Esitelmään liittyvät erityisesti Vahti-ohjeen luvut 3.7 ja 3.8 :
Todisteaineiston turvaaminen
Sisäinen ja ulkoinen viestintä reagoinnin aikana¸

Tunkeutumisiin reagoinnin prosessi

Toimintamalli on yleisesti
(-1) Valmistautuminen: politiikat, työkalut
(0) Havaitseminen
(1) Analyysi, alustava
(2a) Rajaus (2b) Tiedon keräys ja (2c) tiedotus alkavat ja jatkuvat; samoin (2d) tarkempi analyysi eli jäljitys;
(3) Estäminen, reiän tukkiminen
(4) Paluu normaaliin, voidaan joutua aikaistamaan
(5) Oppiminen¸

Nämä vaiheet käydään seuraavaksi läpi Allenin mukaisesti kolmessa jaksossa
valmistautuminen – havaitseminen – varsinainen reagointi
Sen jälkeen täydennetään prosessia Wadlow’n hieman toisenlaisella näkökulmalla.

Aloitetaan kolmella perusohjeella kirjasta Practical Unix & Internet Security
(Garfinkel, Spafford & Schwartz 2003, Chapter 22)
”Don’t panic” (reagoinnin ensiohje)
”Dokumentoi mitä teet” (siis hyökkäystä käsitellessäsi)
”Suunnittele etukäteen!” ¸

Reagointiin valmistautuminen

Sisältää politiikat ja menettelytavat sekä työkalut, ja muut valmistelut (kuten lähtötiedot).

Politiikka ja menettelytavat (§5.2)
Päätetään ja dokumentoidaan

- tunkeutumisen havaitseminen ja reagointi osaksi turvapolitiikkaa
  - millaiset tapahtumat pitää tulkita mahdollisiksi tunkeutumisiksi; mainittava myös sellaiset, joita vastaan on vaikea suojautua (kuten DoS tai skannaukset).
  - toimenpiteiden järjestys (myös tärkeys-). Erityisesti missä vaiheessa ja missä järjestyksessä liiketoiminnat pitää palauttaa.
  - toimintavaltuudet: milloin saa irrottaa järjestelmän tai olla irrottamatta, ajaa alas tai olla ajamatta, valvoa liikennettä tai tiedostoja.
  - resurssit: tehtävien määrittelyt. Yksi mahdollisuus on perustaa vasteryhmä (CSIRT, computer security incident response team), ei välttämättä päätoiminen.¸
- menettelyt, joilla tunkeutumisen havaitsemispolitiikat toteutetaan: [kertauksena] ensinnäkin, mitä tietoja kerätään, miksi, milloin ja mihin. Mukana ovat myös lähtötiedot (esim. tarkistussummat) ja tietovirrat, joita ei talleteta (vaan vain mahdollisesti valvotaan). Toiseksi, miten mitäkin tietoja tutkitaan: missä järjestyksessä, miten usein, millä välineillä, millä seurauksilla ja valtuuksilla, ja miten pitkään (seuranta) ja laajalti (esim. korrelaatiot).
- menettelyt, joilla reagointipolitiikat toteutetaan (ks. vaiheet jäljempänä).
- roolit ja vastuut, siis muillekin kuin turvatiimin jäsenille.

Lisäksi

- katselmoidaan lainmukaisuus
- koulutetaan käyttäjät
- pidetään kaikki edellä sanottu ajan tasalla.¸

”Valitse, asenna ja perehdy reagoinnissa käytettyihin työkaluihin” (§5.5)

- käynnistyslevyistä ja jakelumedioista arkisto; sieltä tehty asennus voi toimia myös vertailukohtana.
- turvakorjauksista arkisto, jotta käyttöjärjestelmän uudelleenasennuksesta saadaan turvallinen.
- uudelleenasennusta tukevien työkalujen asentaminen: asennuspalvelimet, joilta saadaan käyttöjärjestelmät ja sovellukset; vastaavat välineet, joilla haetaan ja käsitellään ohjelmistokorjaukset.
- varmuuskopioinnin toimivuudesta huolehtiminen: ei siis pelkästään palautusten kannalta, vaan mielellään siirrettävillä laitteilla mahdollisuus varmistusten tekoon tunkeutumistilanteessa.
- arkisto testituloksista, joihin vertaamalla hyökkäyksestä toipumista voi tarkastella; mm. skannaustuloksena virallinen palveluiden lista.¸
- tiedotukseen liittyvien yhteystietojen keruu ja ylläpito
- turvalliset kommunikointimekanismit; mm. avaintenhallinta. Liikenneanalyysiakin pitää varoa, ennen kuin hyökkääjän annetaan tietää paljastumisestaan.
- työkalupakki: omalla mediallaan puhtaat ohjelmistot, jotka tarvitaan reagoinnissa. (Wadlow: myös porrastettu kätkentä kohteiden levylle; analogiana käsisammuttimet.)
- testijärjestelmien ja testiverkkojen oikea konfigurointi ja saatavillaolo: murretut järjestelmät voidaan siirtää niihin analyysia varten ja tuotantojärjestelmä ottaa paikattuna käyttöön. Myös sellainen laitteisto käy, jota muulloin käytetään johonkin toiseen tarkoitukseen (siivous jälkikäteen muistettava).¸

Tunkeutumisen havaitsemisvaihe

(Tiivistetty kertaus 3. luennolta ja muutama uusi asia)

Yleinen vaihejako
- tarkkaile ja havaitse poikkeavat tai epäilyttävät tapahtumat
- tutki ne
- jos selitys ei ole hyväksyttävissä rajoissa, käynnistä reagointi.

Aiemmin oli jo esillä seuraavat tarkkailun kohteet
- verkkotoiminnat (§6.3)
- järjestelmätoiminnat (§6.4)
- tiedostot ja hakemistot (§6.5)
- raportit käyttäjiltä ja muista lähteistä (§6.8)

Uutena nyt
- havainnointiohjelman eheys
- fyysiset havainnot
- poikkeamien vaatimat muut toimet kuin varsinainen reagointi¸

Havainnointiohjelman eheys (§6.2)
Hyökkääjillä on pyrkimys muuttaa paljastavia ohjelmia, perustyökaluista alkaen: käynnistyksen ohjelmat, editorit, ps, ls yms. Kaikkeen pitäisi siis suhtautua terveellä epäluulolla. Allen jatkaa tässä keinoista, joilla voi saada puhtaat ohjelmat käyttöön, mutta nämä asiat eivät ole enää havainnointia vaan jäljitystä, ks. jäljempänä.¸

Onko verkkoon liitetty luvattomia laitteita (§6.6)
Hyökkääjä ei välttämättä ole ulkopuolella, vaan voi esim. tulostaa suojaamattomalle kirjoittimelle aineistoa ja viedä sen mukanaan. Hyökkääjä voi hyödyntää joko itse asentamaansa tai käyttäjän asentamaa turvatonta laitetta. Torjuntaa:
- mitkä järjestelmät ja oheislaitteet on liitetty verkon infrastruktuuriin; niistä pitää olla luettelo, eikä tarkastuksista saa varoittaa etukäteen.
- luvattomia modeemeja voi etsiä myös puhelinverkon kautta.
- ohjelmallinen luvattomien laitteiden etsiminen kaikista sisäisistä verkkosegmenteistä.
- verkkolokeista voi löytyä odottamattomia reittejä yrityksen verkon ja ulkoisten verkkojen välillä. Tähän voidaan tarvita vertailua työasemien ja palomuurien lokien välillä.¸

Merkit luvattomasta fyysisten resurssien käytöstä (§6.7)
- fyysiset sisään- ja ulostulokohdat
- merkit peukaloinnista
- liikuteltavien medioiden fyysinen tarkistus
- raportointi¸

”Ryhdy tarvittaviin toimenpiteisiin” (§6.9)
Sen *lisäksi* tai *sijaan* että ryhdytään reagoimaan mahdolliseen tunkeutumiseen:
- dokumentoidaan kaikki havaittu poikkeuksellinen käytös tai toiminta; vasta myöhemmin saattaa ilmetä, että sellainen on osa hyökkäystä.
- tutkitaan kaikki dokumentoidut poikkeukset ja etsitään selitys. Jos kyseessä ei ollut hyökkäys tai sellaisen yritys, johtuiko ilmiö joistain luvallisista uusista ominaisuuksista tai muutoksista, luvallisen käyttäjän toimista virheet mukaanlukien, vai järjestelmän ”tavanomaisista” virheistä tai vikaantumisista?
- tutkimuksilla ja tiedonkeruulla on iteratiivinen luonne.¸
- hälytysmekanismien konfiguraatiota voi olla tarpeen päivittää tiukemmaksi tai löyhemmäksi

- lähtötasotietojen päivitystarve: poikkeuksesta tulee käytäntö — jokin uusi käytäntö muodostuu — aikaisempi normaali onkin nyt poikkeavaa — tai on jätettävä tarkastelujen ulkopuolelle.
- lokien ja muiden tietojen keruumekanismien konfiguraatioihin uusien hyökkäysten havainnointiin tarvittavat tiedot.
- jokainen raportoitu tapaus pitää ratkaista ja saattaa päätökseen jollain tavalla.¸

Varsinaiset reagointivaiheet

(Tiedotus, Analyysi, Tiedon keräys, Rajaus, Estäminen, Palautuminen, Oppiminen)

Tiedotus (§7.3)
Alkaa heti kun hyökkäys on havaittu, eli alustavan analyysin jälkeen, ja jatkuu kaiken aikaa. Saattaa hälyttää hyökkääjänkin ennenaikaisesti, ellei osata varoa. Pitää tehdä tiedottamispolitiikan mukaisesti:

- järjestys jossa eri tahoille tiedotetaan, lista aina saatavilla, ylläpidettynä. Kannattaa tuntea kontaktihenkilöt jo ennen kuin heihin joutuu olemaan yhteydessä tunkeutumisen takia. Eri tahoja:
  - keskeiset: vastuualueen esimies, vasteryhmä, julkisen tiedotuksen vastuuhenkilö,
  - muita: ylläpitäjät (voivat olla 1-luokassakin), turvahenkilöstö, help-desk, ISP,
  - muut asianosaiset ”alavirtaan” ja ”ylävirtaan” (eivät yleensä etukäteen listalla),
  - henkilöstöhallinto, lakimies, sisäiset tarkastajat,
  - oikeusviranomaiset, muut vasteryhmät, toimittajat
  - käyttäjät!
- keille kerrotaan mitäkin; arkaluonteisten asioiden rajaus.
- kirjataan, mitä kenellekin on kerrottu.
- käytetään turvallisia kommunikointikanavia¸

Analyysi (§7.2) eli jäljitys (Wadlow: forensic analysis)
Perustuu kaikkeen saatavilla olevaan tietoon. Alkuvaihe tästä ei ole vielä jäljitystä vaan alustavaa analyysia, jolla selvitetään erityisesti, onko hyökkäystä sittenkään tapahtunut (vrt. ”lämmin” tila jäljempänä). Murretuista järjestelmistä

- kerätään ja talletetaan aluksi järjestelmätiedot, joita myöhemmin ei enää saa talteen: verkkoyhteydet, prosessit, käyttäjät, avoimet tiedostot, muisti, välimuisti.
- seuraavaksi otetaan kahdet varmuuskopiot. Tässä vaiheessa tai viimeistään seuraavassa tunkeutuja huomaa, että hänet on havaittu.¸
- Murrettuja järjestelmiä tutkitaan erillään, joko alkuperäisenä muusta verkosta irrotettuna (ehkä laboratorioon siirrettynä) tai varmuuskopioiden perusteella. (Allen §6.2:) Varmuudella puhtaan ohjelmistokokonaisuuden käyttöön voi päästä seuraavasti (tarvittaisiin kyllä jo alussa):
  - levyn siirto puhtaaseen järjestelmään (ovatko edeltävän alasajon ohjelmat turvallisia?)
  - ulkoisen levyn käyttö uudelleenkäynnistykseen ja ohjelmistojen lähteenä
  - heikompi versio: ulkoinen lähde on CD-ROM, jolloin osaan alkuperäistä käyttöjärjestelmää pitää luottaa. (Lieneekö eroa edelliseen?)
  - levyn kopiointi ja kopion tutkiminen puhtaassa järjestelmässä
  - vertailu luotettaviin tarkistussummiin tai muihin lähtötietoihin (luotettavalla ohjelmalla!) paljastaa, mitä alkuperäisiä ohjelmia voi turvallisesti käyttää.¸
- Onko muissa järjestelmissä merkkejä tunkeutumisesta, erityisesti jollain tavalla samankaltaisissa?
- Lokien tutkiminen; palomuurien, reitittimien tai verkonvalvontajärjestelmien lokit voivat olla antoisia ja puhtaita, haasteena on tiedon lomittaminen eri lähteistä.
- Mitä hyökkäyksiä on käytetty sisäänpääsyssä?

- Mitä tunkeutuja on tehnyt**?** ¸

Tietojen keruu ja suojaus (käytäntöjä) (§7.4)

- Lähteinä kaikenlaiset lokitiedot, liikenne, tiedostot, ylläpitäjän konsoliloki, varmuuskopiot ajalta ennen ja jälkeen hyökkäyksen, IDS-työkalujen tulokset.
- Tiedot pitää taltioinnin lisäksi nimetä ja luetteloida. Apuna on hyvä käyttää pöytäkirjaa (vihkoa), jossa näkyy erityisesti päiväys, kellonaika, kuka teki merkinnän, mitä on kerrottu kenelle, keillä oli silloin vastuu ja pääsy järjestelmään. Tämä siis sen lisäksi, että mainitaan mitä tietoja kerätty.
- Todisteet talteen ja uskottavalla tavalla suojaan muutoksilta. Analyysi pitää tehdä eri kopioista.
- Talteen myös todisteiden hankkimisen ja käsittelyn kaikki vaiheet. Kun em. vihko päätyy todisteeksi, kaikkien sivujen on syytä olla tallella. Siispä eri vihko eri kerroilla.
- Kerätyt tiedot ovat myös varmuuskopioinnin arvoisia!¸

Rajaus (§7.5)

Lyhyen tähtäimen toimi, jolla torjunta saa liikkumatilaa, sillä tunkeutujan aktiiviset mahdollisuudet (todennäköisesti) loppuvat

- varsinaisiin toimiinsa
- havaituksi tulemisen jälkeisiin erityisiin vahinkoihin
- todisteiden hävittämiseen
- ulkopuolisiin järjestelmiin ulottuviin hyökkäyksiin.

Mahdollisesti ensin kuitenkin analyysia ja tiedonkeruuta. Jos näin halutaan tehdä tai jos liiketoimintaa pitkää jatkaa, vastuuta muualle etenevästä hyökkäyksestä voi ehkä rajoittaa viranomaisilta saatavien ohjeiden perusteella.¸

Rajaustoimia on eritasoisia ja niihin tarvittavista valtuuksista ja päätösten perusteista pitää olla tietoa turvapolitiikassa:

- Järjestelmän sulkeminen, lyhytaikaisenakin vakava tapaus! Sen lisäksi ongelmana voi olla joidenkin hyökkäystietojen menetys, esim. vain muistissa sijaitsevista prosesseista.
- Murretun osan irrottaminen verkosta. Normaalin (ja hyökkääjän automatisoiman) toiminnan jatkuminen irrotetussa verkon osassa saattaa sotkea. Jos taas irrotetaan hyvin suppea osa (esim. tietty laite), hyökkääjä voi edelleen olla sillä puolella, jota ei eristetty.
- Käytön pysäyttäminen: tiedostojärjestelmät, palvelut, käyttäjätunnukset. Edellyttää melko pitkällä olevaa analyysia.
- Verkon ja järjestelmän valvonta, erityiskohteena hyökkäykseen liittyneet mekanismit ja järjestelmät.
- Varajärjestelmien koskemattomuuden tarkistaminen, ja toisaalta korjaustoimenpiteiden toistaminen niissä. ¸

Murtautumisreittien tukkiminen (§7.6)

- Salasanojen vaihtaminen: suositellaan joka tapauksessa.
- Analyysin perusteella päätellyn tunkeutumiskeinon poistaminen. Samalla muutkin turva-aukot sopii paikata.
- Muuttuneiden tiedostojen palauttaminen: tarkistussummat ja/tai muutoslokit erinomainen apu tässä. Koskee myös järjestelmien konfiguraatiotiedostoja.
- Uudelleen asentaminen ja konfigurointi, jos valmistautuminen ei ole ollut riittävää, tai puuttuu luottamus muutostietojen tarkkuuteen. Konfiguraatioiden osalta tarvitaan myös katselmointia.
- Turvamekanismien parantaminen.¸

Normaaliin palaaminen (§7.7)

- Mieluummin vasta, kun uusi tunkeutuminen on tehty mahdottomaksi (eli käytännössä vaikeaksi) tai ainakin pystytään havaitsemaan nopeasti. Paluulla voi olla kiire. Tällöin analyysia pitää jatkaa ja rajausten merkitys kasvaa. Uuden tunkeutumisen riskiä voidaan pienentää nostamalla valvonnan tasoa. Muutenkin tunkeilijan paluu(yritykset) voivat tarjota lisätietoja. Tulijoita voi tiedon levittyä olla uusiakin.
- Palaaminen tapahtuu politiikan perusteella vaiheittain tyypillisesti liiketoiminnan tavoitteiden mukaisesti, minimoiden vaikutukset käyttäjiin.
- Hyökkääjä on voinut takaovien asentamisen lisäksi tehdä muutoksia datatiedostoihin. Käyttäjän tiedot palautetaan tuoreimman luotettavan varmistuksen perusteella. Se voi olla vanhempi kuin viimeinen ennen havaitsemisajankohtaa tehty, joka käy kyllä murtamatta jääneiden palautukseen. Silti käyttäjien on syytä suhtautua varauksella tiedostoihinsa (!) Käyttäjien ajettaville tiedostoille suositellaan samantasoista menettelyä kuin järjestelmän ohjelmillekin.
- Palautetun järjestelmän eheydestä saa käsityksen regressiotestillä.¸

Jälkihoito, oppiminen (§7.8)

- Tiedotuksen viimeistely
- Tunkeutumisen aiheuttamien kustannusten arviointi, myös pohjaksi mahdollisille investoinneille.
- Jälkikatselmointi alle viikon kuluessa, ettei asioita pääse unohtumaan: Miten kukin vaihe onnistui, mitä olisi kannattanut tehdä toisin, ja mitä parannuksia tarvitaan.
- Katselmoinnin tuloksista raportoidaan johdolle ja
- tehdään turvadokumenttien päivitys, ((mahdollinen uusi riskianalyysi))
- Tutkimukset ja oikeudenkäynnit voivat vielä jatkua.¸

Reagoinnista Wadlow'n mukaan

Esimerkki vastesuunnitelmasta, jossa neljä tilaa

Kylmä: normaali asiaintila, vahti tarkkailee järjestelmiä ja kerää lokeja.
Lämmin: Hyökkäys on käynnissä tai tunkeutumisen merkkejä on havaittu mutta ei varmistettu Vahti jatkaa työtään, vastepäällikkö tutkii tapausta.
Kuuma: Vakavasti otettava hyökkäys on käynnissä ja/tai tunkeutuminen on varmuudella todettu. Vahti (mahd. useampia) jatkaa entistä valppaampana. Vasteryhmä (yrittää) pitää tuotannon turvallisesti käynnissä ja torjuu lisähyökkäykset. Jäljitysryhmä määrittää tunkeutumisen laajuuden, menetelmän ja lähteen.
Jäähdytys: Tapauksen uskotaan olevan hallinnassa. Ryhmiä puretaan, eli lisäjäsenet vapautetaan, kun se on mahdollista. Vahti jatkaa työtään. Vaste- ja jäljitysryhmä viimeistelevät työnsä ja laativat raporttinsa.¸

Mahdolliset siirtymät

	Kylmä	Lämmin	Kuuma	Jäähdytys
Kylmästä		x	x	
Lämpimästä	x		x	
Kuumasta				x
Jäähdytyksestä	x		x¸	

Jokainen tilasiirtymä kirjataan ja jos suunta on viileämpään päin, päätökselle tarvitaan hyväksyntä muiden tilaan kuuluvien ryhmien päälliköiltä. Siirtymäpäätöksen tekee vastepäällikkö muissa paitsi kylmässä tilassa, jossa vain vahti on paikalla. Tilojen määritelmistä näkyy, miten väen määrä

muuttuu. Pääasiallisia tehtäväalueitakin on kolme, joten yhden tai kahden hengen turvatiimillä ei vastaavaan kyetä – vaan käydään varsin kuumana kaiken aikaa. Isossakin yrityksessä ryhmät voivat osittain toimia VPK-periaatteella.

Wadlow'n tilamalli tarjoaa yksinkertaistetun kielen, jolla tekijät voivat nopeasti omaksua oikean toimintavan – opeteltujen joukosta. Tästä voi olla hyötyä, vaikka toiminta sinänsä sisältääkin paljon hienojakoisempia vaiheita. VAHTI-ohje huomauttaa, että siitäkin syntyy omanlaisensa poikkeustila, kun tietyt työntekijät siirtyvät omista toimistaan hoitamaan tietoturvapoikkeamaa. Ohjeessa ei käytetä mitään varsinaista tilasiirtymämallia. ¸

Tamperelaisen Contrasec Oy:n verkkokoulutuksessa esitellään nelitilainen malli: normaalitila – kohotettu valmius – häiriötila – poikkeustila. Edellä olevasta poiketen tässä ei siis ole jäähdytystilaa, mutta normaaliin voidaan tietysti palata kohotetun valmiuden kautta. Tässä mallissa vasta poikkeustilaa alkavat hoitaa muut kuin normaalit ylläpitäjät.

TeliaSoneran tietoturvatoiminnassa puolestaan on 3x4-taulukko, jossa
kriisit – IT-turvapoikkeamat – muut poikkeamat
on jaoteltu
pieniin – ei kovin vakaviin – vakaviin – erittäin vakaviin.
Tietenkin kriisit ovat vähintään vakavia. Tällaisen luokituksen perusteella kanavoidaan mm. tietotusta ja priorisoidaan korjauksia. (2006)¸

Harjoittelua

Wadlow ehdottaa "sotaleikkejä" harjoitteluun. Aluksi voidaan etsiä järjestelmään kätkettyä tiedostoa, joka seuraavalla kerralla pitää löytää ilman tiettyjä "saastuneita" apuvälineitä. Tällaisen lämmittelyn jälkeen kokemattomammatkin saattavat olla vastaanottavaisia ylläolevan kaltaisille suunnitelmille. Varsinaiset sotaleikit toimivat samaan tapaan kuin tavallisetkin sotaharjoitukset. Niitä voidaan käydä "kartalla" muistiinpanovälineiden ja systeemiä edustavan tuomarin avulla tai oikeassa "maastossa", yleistäen em. tiedostonkätkentää. Tässä ei tarvita systeemituomaria mutta pelituomari kylläkin.¸

Monenlaiset variaatiot ovat mahdollisia. Ne voivat liittyä siihen, miten tilanne pannaan liikkeelle, sovitetaan aikatauluihin, mitä vihjeitä tarjotaan ja onko konna etukäteen selvillä. Vastaavaan tapaan kuin turva-auditoinnin täydessä tunkeutumistutkimuksessa voidaan ehkä pelata vielä todellisemmin. Kaikissa tapauksissa on oleellista jälkipuinti ('post-mortem analysis'). Siihen liittyy:

- muistiinpanot, joita toimeenpanija ja tuomarit tekevät;
- osallistujien pitämä lokikirja (eli suurinpiirtein sama kuin kurssin harjoitusten päiväkirja);
- (lyhyt) harjoituksen purkutilaisuus, jonka tuloksen syntyy
- toimenpideluettelo tarvittavista parannuksista;
- tiivistelmä koko harjoituksesta.

Edellämainitun Contrasecin kaltaisten koulutusyritysten avulla on mahdollista harjoitella luontevasti, sillä niiden tiloihin voidaan usein rakentaa todellista vastaava verkko. Tämä tietysti edellyttää auditoijan tasoista luotettavuutta koulutusyritykseltä.¸

Hyökkäyksen käsittely

Seuraavassa on Wadlow'n esittämiä korostuksia

- Murphyn laki on voimassa.
- Automaattiset mekanismit havaitsevat ja torjuvat ikävystyttävät hyökkääjät.
- Kestää yleensä kauan ennen kuin huomaa olevansa vakavan hyökkäyksen kohteena. (ja:)
- Aikaa menee hukkaan ensimmäisten merkkien havaitsemisen ja hyökkäyksen toteamisen välillä.

- Todennäköisyys, että turvatiimi toimii nopeasti, tarkasti ja oikein, on verrannollinen
  suoraan siihen, paljonko harjoitusta he ovat saaneet ja
  kääntäen siihen, paljonko muita asiaan liittymättömiä tehtäviä heillä on.¸
- Pieni määrä vääriä hälytyksiä on hyväksi harjoitukselle.
- Suuri määrä on haitaksi.
- Hyökkäyksen kohteeksi joutuminen kylmiltään on huono juttu.
- Useimmat hyökkääjät ovat liian älykkäitä ollakseen helposti jäljitettäviä.
- Monet ISP:t tekevät jonkin verran yhteistyötä, kunnes ilmenee (implisiittisestikin), että ollaan harkitsemassa oikeustoimia. Sen jälkeen ne jäävät odottamaan virallista kutsua todistajaksi.
- Helpon pidätyksen todennäköisyys on käytännöllisesti katsoen nolla.
- Samoin helpon tuomion.
- Jokainen kiinnostava tapaus on myös kansainvälinen.¸
- Pitää
  - reagoida nopeasti ja päättäväisesti
  - kuluttaa hyökkääjän aikaa ja voimaa, turhauttaa ja ikävystyttää hänet.
  - herättää hyökkääjässä epäilys (kiinnijoutumisesta, ja siitä että vastassa on vahvempi tekijä kuin ehkä onkaan).
- Ei pidä
  - ryhtyä henkilökohtaiseksi: ei omaa nimeä — ei loukkaamista tai vihastuttamista.
  - motivoida hyökkääjää
  - hyökätä takaisin: väite itsepuolustuksesta ei toimi ‖ kohde voi olla väärä ‖ kohde voi saada perusteen oikeustoimiin ‖ omat oikeustoimet voivat vaikeutua ‖ julkisuus voi olla huonoa ‖ kyseessä on henkilökohtaisuus, joka voi motivoida ‖ kansainvälisyys voi mutkistaa asiaa ‖ ilman valtuuksia vastahyökkääjä voi joutua henkilökohtaiseen vastuuseen.¸

Edellämainitun Contrasec Oy:n toimitusjohtajan Timo Häkkisen esitelmästä (6.3.200***6***) poimittuja korostuksia ovat

suunnitelmallisuus ja oman verkon tuntemus,
johtajuus, muut roolit, paineensieto,
tiedonkulku ja tilannekuvan ylläpito

Esitelmän aiheena oli ”Toimet tietoturvaloukkaustilanteessa” eikä siinä mainittu VAHTI-ohjeita. ¸

Wadlow’n mukaan **vasteryhmän** tehtävät hyökkäyksen aikana sisältävät seuraavat vaiheet (1–7) ja tärkeysjärjestykset.

1) Hyökkäyshavainnon vahvistaminen
- vahdilta tilanteen selostus
- vahvistuksen hakeminen muista tietolähteistä
- päätöksen tekeminen
- *vasteryhmän* kutsuminen¸

2) Vasteeseen valmistautuminen
- määriteltävä, mistä hyökkäys on tulossa, jotta katkaisu olisi mahdollinen
- päätös siitä, tehdäänkö katkaisu (vai jatketaanko tiedon keruuta)
- kaikkien tietolähteiden eheyden tarkistaminen
- vahinkojen laajuuden alustava selvitys
- alustava arvio tunkeutumiskeinosta
- *jäljitysryhmän* kutsuminen

3) Rajaus (‘lockdown’)
- keskeisten infrajärjestelmien eheyden tarkastaminen
- tiedotus *jäljitysryhmälle*

- hyökkääjän pääsyn estäminen lähteenä olevasta verkosta
- ilmeisten pääsykeinojen sulkeminen¸

4) Vakauttaminen
- alustavat tiedot *jäljitysryhmältä*
- toissijaisten pääsykeinojen ja murtokohteiden tarkastelu
- lisärajaukset

5) Siivous
- liiketoimintajärjestelmien eheys
- *jäljitysryhmän* loppuraportti
- mahdollisia lisärajauksia
- murrettujen järjestelmien jälleenrakennus
- verkon ja järjestelmien toiminnan tarkastaminen
- tunkeutumiskeinon huolellisempi poistaminen¸

6) Uudelleenkäynnistys
- sellaisten rajausten poistaminen, jotka eivät liity hyökkääjään
- normaalin liiketoiminnan tarkastaminen
- jäljitysryhmän kotiuttaminen
- mahdolliset toimet hyökkääjää vastaan

7) Valvonta
- hyökkäyksen lähteen aktiviteetin seuranta, *vasteryhmän* toimesta ainakin vuorokausi, sitten
- *vahdin* normaaliksi toiminnaksi
- *vasteryhmän* kotiuttaminen¸

”Tietoturvapoikkeamatilanteiden hallinta” ja muut ohjeet

Yksi VAHTI-ohjeen lähteistä on Computer Security Incident Handling Guide, joka on NIST:n julkaisuna USA:ssa vastaavanlaisessa asemassa kuin VAHTI-ohjeet Suomessa (NIST=National Institute of Standards and Technology). NIST-sarjassa on useita muita seikkaperäisiä turvaohjeita, mm. niinkin erityisiin (joskin isoihin) asioihin kuin IDS:ään, turvapaikkausten käsittelyyn, langattomaan tietoliikenteeseen ja seittipalvelimen turvaamiseen (ks. myös http://csrc.nist.gov/publications/nistpubs/; Kurssin B-osassa joitakin ohjeita tarkastellaan lähemmin).¸

Muiden lähteidensä osalta VAHTI-ohje on varsin itseriittoinen: Puolustustaloudellisen suunnittelukunnan yhden julkaisun lisäksi viitataan vain muihin VAHTI-ohjeisiin. Lisätiedot pitää siis hankkia niiden tai NIST-ohjeen lähdeluettelosta. Tämä koskee esim. ohjelmistotyökaluja. Tietysti tällaiset ja muut verkosta saatavat tietolähteet on luontevampaa listata ajantasalla pysyvillä sivustoilla (esim. CERT-CC ja CERT-FI). Silti VAHTI- ja NIST-ohjeen teknisen luonteen eroa kuvannee hyvin se, ettei edellisessä mainita yhtään RFC-dokumenttia. Jälkimmäisessä viitteitä on useita, mm. tiivis RFC3227 ”The Guidelines for Evidence Collection and Archiving” (2002).

Tärkeää kaikissa VAHTI-ohjeissa on niiden pohjautuminen suomalaiseen lainsäädäntöön ja suomalaisiin käytäntöihin. Tämänkertaisen ohjeen tapauksessa mukana on mm. viittauksia vahingonkorvauksiin ja oikeustoimiin, joista edellä ei ole juurikaan ollut puhetta. Tutustu ohjeeseen kokonaisuudessaan ja **LUE** siitä luvut 3.7 ja 3.8 sekä liitteet 4–7.¸

TLT-3301 Verkon tietoturva, 6. luento 17.12.2008

Auditointi [Wadlow Ch. 10]

Kertauksena jatkokurssilta:

- IPSec, IKE, VPN
- Käyttäjähallinto ja kertakirjautuminen (→ Vahti…)
- Reititys

Verkonhallinta

Käyttäjähallinto, kertakirjautuminen, VAHTI 9/2006

Turvallinen etäkäyttö turvattomista verkoista (VAHTI 2/2003)

Verkon tietoturva?

- Trendeistä
- Opiskelusta ja työelämästä
- Tutkimusta?

,

Auditointi

Allen (s. 189): "Auditointi on tiedon järjestelmällistä vertaamista oletettua, dokumentoitua muotoa tai käyttäytymistä vastaan". Tämä lienee ainoa kohta jossa termiä käytetään. Allenin kirja ei siis käsittele auditointia yhtä laajasti kuin tässä tehdään Wadlow'n mukaan [Ch. 10]. Hän määrittelee mm. näin:¸

1. Vakavasti otettavan auditoinnin
   tarkoitus on paljastaa
2. kiinnostavaa ja
3. kattavaa tietoa
4. verkon tietoturvasta.

1. Muunlaisia auditointeja voivat olla sellaiset, jotka tehdään vain hyvän tavan (due-diligence) takia, esim. liikekumppanin vaatimuksesta.
2. Kiinnostavuus on sitä, ettei tietoa ollut ennestään. Ei kannata myöskään jättää mitään tiedossa olevaa korjaamatta ennen auditointia. Kiinnostavuus voi olla kipeää, mutta avaa silmiä sekä TT-toteuttajissa että johdossa. Ulkopuolisuus tarjoaa vääristymättömyyttä, metodologisuutta, uusia näkökulmia, jonka taustalla lukuisia vastaavia arviointeja.
3. Ei pelkästään ongelmia, vaan kiinnostavia seikkoja yleensä, mutta
4. ei suorituskyvystä tai käytettävyydestä.¸

Kattavuus ei myöskään tarkoita, että välttämättä kaikki verkon asiat ovat kohteena. Auditoinnin rajauksena voi olla:

- oman verkon ja internetin kytkentä
- oman verkon ja yrityskumppaneiden verkon välinen kytkentä
- etätyön toteutus
- verkon infrastruktuuri
- verkon liiketoimintakomponentit
- isäntäkoneiden arkkitehtuuri ja ympäristö
- fyysinen turvallisuus
- vahingoista toipuminen
- prosessit ja käytännöt
- vasteaika ongelmien selvittämisessä, vasteen toimivuus yleensä ja virka-ajan ulkopuolella¸
-

Kaksi päätyyppiä: tunkeutumistutkimus ja konfiguraatioanalyysi.

Tunkeutumistutkimus. Lähtötilanteita on kolmea lajia: auditoija käyttäytyy kuin hyökkääjä
- tietämättä kohteesta mitään
- osittaisen tiedon varassa, tyypillisesti kohteiden sijainnit, IP-osoitteita, modeemien puhelinnumeroita ym.
- täydellisen tiedon perusteella. Tällä simuloidaan sisäpuolelta tapahtuvaa hyökkäystä.

Oikeuksia voi periaatteessa olla kolmenlaisia:
- ei saa häiritä verkon toimintaa
- "täysi tunkeutuminen": sallitaan muutokset, jotka voivat aiheuttaa myös vahinkoa.
- rajoittamaton hyökkäys: kaikki oikeallekin hyökkääjälle sallitut keinot ovat käytössä.¸
-

Konfiguraatioanalyysi: tarkastelu sisäpuolelta
- täydellisen tiedon ja
- täysien pääsyoikeuksien pohjalta,
- silti valvotusti.¸
-

Vertailua

Tunkeutumisanalyysi (T)
Konfiguraatioanalyysi (K)

+ T ilmaisee todellisen ongelman (ja voi tuottaa lisärahoitusta verkkoturvalle)
+ mutta K on usein kattavampi
+ T on kohtuullisessa mitassa melko edullinen
– K on yleensä kalliimpi
+ T: rajoittamaton vastaa hyvin sitä, miten oikea hyökkäys tapahtuu
– T: mittaa enemmän auditoijan taitoa kuin puolustajan perusteellisuutta
+ K: toisinpäin¸

– T: vaikea laatia aikataulua (erityisesti tietää ennakolta milloin työ on valmis)
+ K: helpompi
– T: rajoitukset vääristävät
– T: muutokset (esim. salaluukut tai troijalaiset) heikentävät verkkoa myös muita hyökkääjiä varten
+ K voidaan tehdä valvotusti; tiedetään myös mitä auditoija sai tietää.
+ K:ssa pääsy rajoittuu lyhyeen ajanjaksoon
+ vähäinen vaikutus tuotantoon
– molemmissa auditoijaan pitää voida luottaa; molemmissa hän saa tietoa verkosta ja
– T:ssä lisäksi pääsyn verkkoon ja
– K:ssa tietoa viedään muualle analysoitavaksi¸

Auditoija voi olla

- itsenäinen konsultti
- tietoturvayrityksestä
- auditointiin erikoistuneesta yrityksestä

Odotusarvot saatavuudelle, luotettavuudelle, laadulle ja hinnalle ovat melko ilmeisiä.

Auditoijalta pitää voida edellyttää:

- ammattimaisuus
- varovaisuus
- avoimuus aiotuista erityismenetelmistä
- tarkka sopimus mikä on luvallista
- hyvin laadittu raportti ja esittely + kyselymahdollisuus
- hankitun tiedon oikea kohtelu

- auditoinnin tulosten luottamuksellisuus¸
-

Auditoija edellyttää asiakkaaltaan:

- vastuuvapaus niistä toimista joista on sovittu
- tietojen toimitus
- järkevä käytös: esim. ei vääristävää ennakkovaroittelua
- viime hetken muutosten välttäminen
- epäpoliittisuus; auditointia ei pidä käyttää valtataisteluun¸
-

Vaiheet

- neuvottelu & esiauditointi
- tiedon keruu (K: myös haastatteluja)
- analyysi toisaalla
- raportteja
  - T: vain onnistuneiden hyökkäysten kuvaus > yritettyjen ja rajoitusten takia yrittämättä jääneiden hyökkäysten kuvaus; haavoittuvuuksien luonnehdinta > ehdotetut korjaukset
  - K: vain havaitut ongelmat > miten niitä voisi korjata > verkon rakenteen analyysi ja tietolähteitä
- esityksiä
- reaktio: suunnittele miten korjaat — toteuta suunnitelma
- seuranta, jossa auditoija voi olla vielä mukana.¸

IPSec, IKE, VPN

TTP:ssä ja TTJ:ssä on esitelty IPSecin molemmat protokollat AH ja ESP ja niiden kuljetus- ja tunnelimoodit [id=296]. Lisäksi on käyty läpi avaintenvaihdon IKE-protokolla: alkuperäinen versio kaksine vaiheineen ja erilaisine autentikoinnin vaihtoehtoineen [id=297, id=298] ja IKEv2, jossa vaiheet on yhdistetty. Vaiheessa 2 muodostuva turva-assosiaatio SA tai IKEv2:ssa suoraan muodostuva Child_SA on tarkoitettu AH:n tai ESP:n käyttöön ja se talletetaan tietokantaan SADB. Sinne voidaan asentaa SA:ita myös käsin. Kukin SA on yksisuuntainen ja määräytyy kolmesta parametrista: SPI eli security parameter index, kohteen IP-osoite sekä ”AH vai ESP”. Indeksi SPI on ensimmäisenä kenttänä kaikissa IPSecin laatimissa otsikoissa.¸

Samaan tapaan kuin palomuurien säännöt vievät tietoturvapolitiikan käytännön liikenteen tasolle, IPSecin SPD-tietokannan säännöt ilmaisevat valitsimien (’selector’) avulla, millaiseen IP-liikenteeseen pitää soveltaa mitäkin suojausta vai voidaanko liikennöidä ilman IPSeciä. Tämä on lähtökohta SA:n muodostamiselle. Näistä on hieman lisätietoa TTJ:n materiaalissa [id=293], jossa on esitelty myös erilaisia malleja IPSec:n sijoittamiselle, nimittäin päästä-päähän, VPN, sisäkkäiset tunnelit, linkeittäinen tai tähtimäinen tunnelointi. VPN-toteutus voidaan tehdä muutenkin kuin IPSecillä [id=215], myös ylemmällä tai alemmalla protokollatasolla. Ylemmän tason protokollista suosituin on SSL. Sitä voidaan käyttää OpenVPN-hankkeen tavoin tunneloimaan koko TCP/IP-pino tai rajoitetummin vain yläpuolella oleva sovellustaso. Tällöin toiminta kuitenkin vastaa seittiproxya, johon voi ottaa yhteyttä useammasta paikasta. Toisen suositun sovellustasolla toimivan toteuttaa (Open)SSH.¸

Käyttäjähallinto, kertakirjautuminen, VAHTI 9/2006

Tietoverkkoa ei saada turvalliseksi pelkästään arkkitehtuurin, laitteisiin asennettujen mekanismien ja niiden konfiguraatioiden avulla. Paljon riippuu myös siitä, miten hyvin verkon käyttäjät noudattavat tietoturvapolitiikkaa. Tähän vaikuttavat monet psykologiset seikat, jotka jätetään tällä kurssilla

vähälle huomiolle, sillä ne liittyvät työyhteisön toimintakulttuuriin ja muuhun sellaiseen, joka ei ole tietoturvatiimin vastuulla. Tietoturvapolitiikan muotoiluilla voi kuitenkin edistää turvallisuutta myös psykologiselta kannalta. Tähän suuntaan vaikuttavat mm. yksinkertaisuus, ymmärrettävyys ja vastuiden selkeys (vrt. 1. luento). ”Käyttäjien hallitseminen” sen sijaan ei todennäköisesti ole hyvä menettely, jos se tarkoittaa esim. salasanan ajoittaista pakotettua vaihtoa todella entrooppiseen koneen valitsemaan salasanaan (vrt. myös ”turvasuunnittelu” 2. luennolla).¸

Verkon turvallisuudelle on silti keskeistä, että ”käyttäjiä hallinnoidaan”, mutta käyttäjähallinnossa on kyse itse asiassa **käyttäjäkunnan konfiguraatiosta**: sen määrittelemisestä, ketkä ovat käyttäjiä kulloinkin ja mitkä heidän oikeutensa ovat eri resursseihin. Isossa verkossa tehtävä on haastava, vaikka oikeuksien määrittelyä yksinkertaistettaisiinkin ryhmien ja roolien määrittelyllä. Radius-mekanismi on esimerkki siitä, että käyttäjähallintoa voidaan tehostaa keskittämällä, mikä ei silti tarkoita, että hallinto pitäisi jättää yhden palvelimen varaan – keskitetty palvelukin voidaan hajauttaa.¸

Kun verkossa on useita erityyppisiä palveluita, joita eri henkilöt käyttävät hieman erilaisin oikeuksin, voidaan harkita kertakirjautumisjärjestelyjen käyttöä. Esimerkki tästä on TTY:n seitissä vuonna 2003 käyttöön otettu ”tikettiautentikointi”, jossa hyödynnetään **PubCookie**-tekniikkaa. **Shibboleth** on uudempaa ja ylemmän tason tekniikkaa tähän tarkoitukseen. Sillä voidaan myös ulottaa luottamusta organisaatioiden välille ja tätä on tehty erityisesti yliopistomaailmassa. **Kerberos** puolestaan on perinteisempi järjestelmä kertakirjautumiseen. Tällaisilla mekanismeilla ei tietenkään ole sijaa ylläpitäjien ja turvatiimin autentikoinnissa silloin, kun kyse on järjestelmien ytimiin kajoamisesta. (Käyttäjähallintoa, Kerberosta, tikettejä ja toimialueita on esitelty TTJ:n materiaaleissa id = 472, 359, 387, 385, 393.) ¸

Käyttövaltuushallinnon periaatteet ja hyvät käytännöt, VAHTI 9/2006
esittää kokonaisvaltaisen ja melko epäteknisen *mallin* ”käyttäjäkunnan konfigurointia” varten.
LUE luvut 3 ja 4, jotta osaat sanoa hieman enemmän malliin kuuluvista vaiheista kuin seuraavassa tiivistelmässä [ks. myös kaavio 1, s. 14]:

Mallin pääosa käsittelee valmistelua, jolla luodaan **edellytykset** käyttövaltuushallinnolle.
Edellytysten luominen alkaa
- riskianalyysilla, jota tietysti uudistetaan aika ajoin. Muut toimet perustuvat tälle.

Valmistelu on hallintoa, ja sen ylimmällä tasolla tapahtuu
- johdon sitoutuminen
- tietojen ja järjestelmien omistajuuksien määrittely ja haltuunotto
- hallintaprosessien määrittely ja kuvaaminen¸

Tietojen tasolla tapahtuu
- luokittelu
- suojattavien kohteiden ja niihin liittyvien käyttöoikeuksien määrittely

Käyttäjiin liittyen määritellään
- roolit tai ainakin käyttäjäryhmät ja
- käyttövaltuudet, sekä
- suunnitellaan ja vastuutetaan säännöllinen valvonta, joka koskee käyttövaltuuksia ja niiden hallinnointia. ¸

Teknisemmällä tasolla
- suunnitellaan ja toteutetaan **valmiuksia**, jotta voidaan ottaa käyttöön hallintajärjestelmä.
- Lisäksi laaditaan rekisteriselosteet.

Käyttäjäidentiteettien ja käyttövaltuuksien **hallintajärjestelmään** kuuluu
- automaattinen luvitusprosessi
- tietovarasto käyttäjistä ja käyttövaltuuksista
- käyttövaltuustietojen siirto kohdejärjestelmiin
- jäljitettävyys- ja raportointitoiminnot

Käyttövaltuuksien hallintaympäristöön kuuluu myös tunnistaminen ja pääsynvalvonta.¸

VAHTI 2/2003: Turvallinen etäkäyttö turvattomista verkoista

Etäkäyttöön vaikuttavat palaset, ensinnä tekniikoista riippumattomat:
- etäkäyttöympäristö (koti, ...)
- käyttäjä ja rooli (työntekijäroolit, kumppani, ... ei kuitenkaan asiakas)
  - pohjana identiteetti
- käytön sisältö (aineistot, ...)

toiseksi tekniset järjestelyt, eli ”etäkäyttöratkaisu”:
- päätelaite,
- päätteen verkkoliitäntä,
- verkkoyhteys,
- palvelun verkkoliitäntä.¸

Joka palaseen Ohje esittelee suojausmekanismeja, jotka ovat tulleet esille kurss(e)illa. Viimeinen palanen on kaikkein monimutkaisin. Siinä jatketaan myös käyttäjien tunnistuksen, todennuksen ja pääsynvalvonnan käsittelyä (käyttäjän näkökulman oltua esillä erikseen). Palvelujen suojaus niiden verkkoliitännässä sisältää
- palvelujen ryhmittelyn (sisäverkon osittaminen),
- liikenteen suodattamisen,
- puskurivyöhykkeen (DMZ:n) luomisen,
- IDS:n.

Ensimmäinen ja kolmas kohta ovat tavallaan samaa asiaa, jota toteutetaan toisen kohdan eli palomuuri(e)n avulla.¸

Ohje esittää kolmiosaisen eteisverkon:

Internet-eteinen, eli ulko-DMZ, johon ulkoiset yhteydet päättyvät, ja jossa ovat
- tunnistus- ja todennuspalvelin,
- viraston ulkoinen DNS-palvelin ja
- ulkoinen sähköpostin välityspalvelin

Sisä-DMZ-1 sisältää web-postipalvelimen, jonka kanssa käyttäjät kommunikoivat SSL:n suojissa ulkoverkosta käsin. Palvelin puolestaan kommunikoi (vain) sisä-DMZ-2:ssa oleva sähköpostipalvelimen kanssa.

Sisä-DMZ-2:ssa sijaitsee (myös) VPN-palvelin, johon kaikki VPN-yhteydet päättyvät. Lisäksi sinne on asetettu sisäverkossa olevan WWW-palvelimen (tms.) proxy-palvelin. Kun etäkäytöstä on kerran kyse, tämä proxy edustaa *etäkäyttäjille* sisäpalvelinta. Voisi olla myös toisinpäin.¸

Ohje jakaa käyttötilanteet 4 ulottuvuudessa (x, y, z, w):

	1	2	3	
x:	säännöllinen	— satunnainen		
y:	kiinteä	— vaihteleva		yhteys/paikka
z:	viraston	— käyttäjän oma	— jonkun muun	päätelaite
w:	viraston oma	— kumppanin		työntekijä

ja toteaa näistä seuraavien esiintyvän käytännössä:

(x, y, z, w) = (1, 1, 1, 1) , (2, 2, 1, 1) , (1–2, 1–2 , 2–3 , 1) ja (1, 1, 1, 2).

Viimeisessä eli ’kumppanikäytössä’ viraston päätelaite tarkoittaa kumppanivirastoa, ja tilanne on melko harvinainen. Kolmanteen tapaukseen ohje esittää päätelaitteen hallinnan (puutteen) takia ymmärrettävästi varauksia. ¸

Ohjeen luku 5 esittää konkreettiset suositukset turvallisen etäkäytön arkkitehtuurille. Lähtökohdaksi todetaan:

- järjestelmäkomponenttien asianmukainen suojaus
- käyttäjien riittävä ohjeistus
- tarvittava tuki
- sovitut etäkäyttötoiminnan pelisäännöt
- sääntöjen valvonta

Seuraavassa esitellään askeleet (1 – 2 – 3 a-b-c-d-e – 4) vain **poimimalla** tai kokoamalla niistä joitain kohtia, jotka sopivat tässä vaiheessa täydentämään tai kertaamaan kurssin sisältöä:¸

1. Viraston etäkäyttöpolitiikka

...
Kirjava kokoelma hyviä käytäntöjä
aineiston salauksesta varuillaan olon kautta varmuuskopiointiin.

2. Etäkäytettävien sovellusten luokittelu

...
Lähtökohtina
tietoaineistojen turvaluokittelu
käyttäjäroolit ja niiden oikeudet.¸

3. Kunkin etäkäyttöluokan hyväksyttävät etäkäyttöratkaisut ja niiden minimisuojaustaso

3a. Päätelaitteiden suojaaminen

...
Pääsääntö: virasto hallinnoi laitteita, ohjelmistoja ja niiden asennuksia.
Fyysinen suojaus, myös mm. käynnistys- ja BIOS-salasanat sekä tiedostosuojaukset.
Tässä myös selainten turvallisuudesta, mm. luotetut tahot.¸

3b. Päätelaitteen verkkoliitännän suojaaminen (kaikki kohdat mainittu, tiivistäen)

Virustorjunta (siis tässä eikä edellisessä kohdassa)
Henkilökohtainen palomuuri ...
Valintayhteyden edelleenohjaus kiellettyä.
Uloskirjautuminen, ei pelkkä yhteyden katkaisu.

Tulevien kutsujen hylkääminen (ellei erikseen sovittu).

Yhteydet ulos Internetin kautta sallittu vain viraston määräämällä suojaustavalla.

Vain viraston hyväksymiä valinta- tai Internet-yhteyksiä.
Kaikki liikenne viraston hyväksymän palomuurin kautta.¸

WLAN-verkossa

päätelaitetta kohdellaan kuin Internetissä olevaa.

Salauksen käyttö: SSH:ta tai IPSec;

joka tapauksessa pelkän WEP:n lisäksi jotain muuta, *aikanaan [=nyt]* IEEE802.11i
Lisäksi ”verkon omia salaustoimintoja kannattaa myös käyttää.”

Konfigurointi- ja käyttöohjeita:
– vaihdetaan hallinnointisalasanat
– nimetään verkko (SSID) tavalla, joka ei ole heti arvattavissa
– estetään pääsy WLANista muuhun verkkoon ilman käyttäjän todentamista
– käytetään verkossa MAC-tunnistusta
– estetään SSID broadcasting
– estetään SNMP-käyttö langattomasti
– rajataan hallintayhteydet ja määritellään hallintamekanismit ja osoitteet
– pidetään lokia verkon käytöstä.

Bluetooth varauksella.¸

3c. Verkkoyhteyksien suojaaminen

...
”Yleispätevä ratkaisu verkkoyhteyden suojaamiseen on VPN [joskin VPN = IPSec]
Sen rinnalla voidaan käyttää selainkäytössä TLS:ää ja WTLS:ää,
sekä erityiskäytössä SSH:ta.”¸

3d. Käyttäjien tunnistaminen, todentaminen ja pääsynvalvonta

...
Kiinteä salasana vain julkisia aineistoja käsittelevien sovellusten käyttöön.

Suositeltuja todentamistapoja ovat **matkapuhelimen** käyttö (puhelinsoitto
sekä kiinteä tai kertakäyttöinen tunnusluku) sekä PKI-varmenteet
joko toimikortilla tai matkapuhelimessa vahvinta suojaa vaativia sovelluksia
käytettäessä.¸

3e. Palvelujen verkkoliitännän suojaaminen

...
Tästä oli jo edellä. Yksi korostus: ”VPN-yhteyttä tai muuta salattua yhteyttä ulkoverkosta
palomuurin läpi suojaamattomaan sisäiseen palvelujärjestelmään ei pidä sallia, koska sitä
voidaan käyttää porsaanreikänä sisäverkkoon.”¸

4. Määritellään ja suunnitellaan etäkäytön keskitetty valvonta ja hallinta

...
Sopiminen ulkopuolisten organisaatioiden kanssa periaatteista ja vastuista.
Vastesuunnitelma.¸

Viimeisenä on vielä ”Muista myös nämä”:

- Muista jäännösriski – älä tuudittaudu väärään turvallisuudentunteeseen.
- Älä luota yhteen suojausmenetelmään, suojaa monitasoisesti.
- Mitä et itse tiedä, sitä et tiedä.
  Käytä tarvittaessa apunasi asiantuntijoita, jotka tietävät.
- Pyri mahdollisimman yksinkertaisiin, hallittavissa oleviin ratkaisuihin.¸

Reititys

Reitittimien välinen tiedonvaihto voidaan normaaliin tapaan suojata autentikoinnin ja eheyden takaavilla mekanismeilla, mutta se ei ole kovin vanha asia. Esimerkiksi RIP-protokollassa ei ollut alunperin lainkaan autenttisuutta, toisessa versiossa oli ensin selkotekstinen salasana ja sittemmin MD5-tiiviste, mutta viestien eheydestä eivät RFC:t mainitse mitään. OSPF2-protokollassa voidaan tehdä vastaava kryptografinen autentikointi salasanatiivisteen avulla, mutta siinä myös paketin sisältö on MD5-laskussa mukana, joten eheys on turvattu.¸

Varsinainen turvaongelma tulee siitä, että hyökkääjän kontrolloima reititin voi valehdella ”autenttisesti”. Tietoturvallisuuden oppikirjat puhuvat erittäin vähän reitityksestä, vaikka aiheena olisi ”Network security”. Selityksen tarjoaa S.M.Bellovin esitelmässään Routing Security (2003, liittyy artikkeliluonnokseen, jossa esitellään katkaisuhyökkäys). Hän toteaa nimittäin, ettei se kuulu perinteisen tietoliikenteen turvallisuuden piiriin, ja itse asiassa tutkimustakin on tehty varsin vähän: ” Why so little work? – It's a really hard problem. – Actually, getting routing to work well is hard enough. ...”.

Reititykseen ja nimipalveluun liittyvistä turvakysymyksistä on kooste TTJ-materiaalissa [id=388].¸

Verkonhallinta

Reitityksen turvaamisen ohella verkonhallinta on toinen alue, jota tietoturvan oppikirjoista ei juuri löydy. W. Stallings on kirjoittanut verkonhallinnasta erikseenkin ja seikkaperäinen esitys löytyy hänen kirjastaan Network Security Essentials (2nd ed. Pearson 2003).

Verkon hallinnointi tarkoittaa yleisesti kaikkea, mitä verkon ylläpitäjien täytyy tietää verkon toimilaitteiden tilasta ja mitä muutoksia heidän pitää sen perusteella tai muuten tehdä näille laitteille. Osa-alueita on viisi: viat, konfiguraatio, laskutus (esim. pääsynvalvonta), suorituskyky ja turvallisuus. Näiden alkukirjaimet englanniksi muodostavat CIA:n ja AAA:n kaltaisen lyhenteen FCAPS. Kaikkia verkon toimilaitteita ei ole kätevää operoida paikan päällä, vaan tarvitaan menetelmä etähallinnointiin. Simple Network Management Protocol eli SNMP tarjoaa siihen työkaluja, mutta varhaisten versioiden turvaominaisuudet ovat olleet niin heikot, että niitä ole kannattanut ottaa muutosten teon välineiksi vaan pelkästään tietojen kyselyyn. Asiattomien ei olisi toki suotavaa päästä modifioimaan myöskään kyselyjä, mistä laskutustiedot ovat ilmeinen esimerkki. Versiossa 3 turvallisuus on mukana (→ B-osa).¸

Verkonhallinnan malli SNMP:n mukaisesti sisältää

- hallinta-asemat, joissa on (käyttöliittymä, muita työkaluja sekä) SNMP-manageri, jolla voi lähettää kyselyitä ja ohjeita
- hallinta-agenteille, joissa on SNMP-agentti ja
- hallintatietokanta (Management Information Base, MIB), jossa ovat hallittavien olioiden (muuttujien) arvot.
- Muitakin hallittavia laitteita voi olla kuin sellaisia, joissa on SNMP (tai edes TCP/IP). Tällöin jokin hallinta-agentti toimii proxyna.¸

Hallinta-asema voi kysellä hallinta-agentin tietokannan jonkin olion arvoa tai asettaa sen. Käytössä on UDP. Lisäksi hallinta-agentti voi lähettää oma-aloitteisesti arvon hallinta-asemalle: esim. uudelleenkäynnistyminen tai jonkin liikenteen määrän raja-arvon ylittyminen (“trap”, jollaista Allen mainitsee voitavan käyttää lokitietojen keruuseen; vrt. 3. luento).¸

Verkon tietoturva?

Tähän, viimeisen vakioluentokerran loppuun, mennessä kurssilla on käsitelty
kaksi kirjaa ja
muutama Vahti-ohje ym. lähde.
Edelleen muistetaan esitietokursseilta monia muita mekanismeja kryptologiasta alkaen.
Harjoituksissa sovelletaan joitakin menettelyjä ja käytetään oikeita ohjelmistoja ja laitteita.¸

Mitä *verkon tietoturva* siis on?

- mitä siitä voi tietää / osata ?
- mistä ja miten tietoa ja taitoa saa ?

- mitä siihen oikeastaan kuuluu ?
- minne se on menossa ?

- mitä se on tieteellisenä tutkimuskohteena ?

Seuraavassa on muutama huomio näistä asioista
Muita kysymyksiä / palautetta
→ päiväkirjoihin → vaikutus tulevaisuuden lisäksi omaan oppimiseen
→ tietoja mahdollista tutkimusta varten¸
Lisäksi kysymyksiä **ja** vastauksia rastitehtäviin!

Trendeistä

Katsauksia, esim.:

2005 nCircle Survey Results:Trends in Vulnerability and Risk Management
[→ http://www.securitymanagement.com/library/nCircle_survey1005.pdf]

Hyökkääjien trendejä opetusmateriaalissa (2005):

Concepts in Network Security
[→ http://download3.vmware.com/vmworld/2005/sln070.pdf]
sivuilla 2, 3 ja 4.

Myös: **harjoituslaboratorio VIAN**: Virtual Information Assurance Network
käyttää VMWare-virtualisointia
sivut 6 ja 10, viittaa seuraavaan aihepiiriin, joka saattaa niinikään olla trendi.

Tietosodankäynti:

mm. VIAN-aineistoa: http://www.itoc.usma.edu/
Viestiupseeriyhdistyksen linkkilista:
http://www.viestiupseeriyhdistys.fi/tekniikka/infosota.shtml¸

Opiskelusta ja työelämästä

Tarvitaan ainakin

teorioita, harjoittelua, kokemusta,
vuorovaikutusta, aktiivisuutta,
motivaatiota, muutoksen sietämistä¸

Guide to College Majors in Network Security (2005)
[http://www.worldwidelearn.com/online-education-guide/technology/network-security-major.htm (viitattu XII/2008)]

Trends in Network Security Careers

A number of large companies are turning to outside firms to provide security services and skills. This permits the primary company to concentrate on its specific business goals and to depend on its information technology provider to concentrate on those functions. This trend is creating a demand for skilled professionals who can take on these projects for the security firms.

One in five information technology positions involves networking professionals. Corporate budgets for security are growing about 25 percent each year, which is expected to continue for the next three to five years. Job openings for senior-level information security officers have increase by nearly 50 percent since 2003. The U.S. Labor Department estimates that an additional 10,000 trained security professionals will be needed by 2010. ¸

Samaisessa lähteessä mainitaan seuraavat verkkoturvan spesialistit:

- **Firewall specialist or administrator**
- **Disaster recovery specialist.** Tällainen toivuttamisen erikoisosaaminen (mahdollisesti ulkoistettu) saa lähteen mukaan motivaationsa USA:n lainsäädännöstä, joka vaatii tietynlaisia yrityksiä huolehtimaan tiedoistaan.
- **Forensics specialist.**
- **Wireless security expert.**
- **Information security officer.**
- **FBI investigator.** Tässäkin on USA-painotus ja taustalla on terrorismin torjunta.¸

Myös eo. lainausta vanhempi lehtijuttu korostaa verkkoturvan koulutuksen ja tutkimuksen tarvetta [L.D.Paulson: “Wanted: More Network-Security Graduates and Research.” IEEE Computer. February, 2002 http://www.cs.virginia.edu/misc/wulfnews.pdf]

Tutkimusta?

Oppikirjat ja VAHTI-ohjeet eivät ole tieteellisiä raportteja, mutta ainakin Allenin kirjan voi uskoa CERT-taustansa ansiosta heijastavan hyviksi tai ainakin toimiviksi osoittautuneita käytäntöjä. VAHTI-ohjeiden syntyprosessissa on mukana vertaispalaute, mikä vaikuttaa samaan tapaan.

Kurssin painopisteinä olevat hallinto ja käytäntö eivät ole kovin otollisia eksaktille tutkimukselle, ellei kyse ole kartoituksista ja hyvien käytäntöjen toimivuuden ”mittaamisesta”. ¸

Tutkimusraportteihin oli viittauksia esim. IDS- ja DoS-seminaarien teksteissä.
Tässä on vielä muutama viittaus, hyvin ”trendikkäästä” aiheesta:

A Multifaceted Approach to Understanding the Botnet Phenomenon
(M.A.Rajab, J.Zarfoss, F.Monrose, A.Terzis, 2006)
The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets

(E.Cooke, F.Jahanian, D.McPherson, 2005)
Revealing Botnet Membership Using DNSBL Counter-Intelligence
(A.Ramachandran, N.Feamster, D.Dagon, 2006)¸

Nämä artikkelit pohjautuvat erilaisilla tekniikoilla kerättyihin tietoihin bot-verkkoihin liittyvästä liikenteestä ja pyrkivät säätämään havainnointitekniikoita tarkemmiksi. Tutkimusta todetaan olevan toistaiseksi varsin vähän ja artikkeleissa jätetäänkin monia asioita selvitettäväksi myöhemmin. Työ jatkuu myös sen takia, että hyökkääjät tälläkin alalla kehittävät menetelmiään.

Havainnointitekniikoista kannattaa mainita:

- **hunajaverkot**, jotka on mainittu jo TTJ:ssä (id=303) ja ehdotettu että verkkoturvan tiimi voisi osallistua talkootyöhän esim. honeynet.org'in puitteissa (id=356).
- **darknetit**: käyttämättä jääneiden IP-osoitteiden kuuntelu, jolla saadaan selville internetin taustakohinan lisäksi mahdollisia hyökkääjiä, mm. bot-liikennettä. Tästä on TTY:llä diplomityö meneillään (2008).
- **DNSBL**, eli DNS blackhole list, josta viimeinen artikkeli kertoo. Bot-mestari saattaa ylläpitää bot-verkkonsa laatua seuraamalla, mitkä bot-koneet ovat tällaisella lähinnä spam-torjuntaan liittyvällä listalla. Näiden kyselyjen perusteella saatetaan päästä bot-verkon jäljille. Erikoinen havainto oli kuitenkin, että joitakin kyselyitä tekevät botit kuuluvat eri bot-verkkoon kuin kyselyn kohde-bot. Tässä on esimerkki siis hyvin edistyneestä kätkeytymisestä. ¸

TTY:llä

Helmikuussa 2008 päättyy Leonardo da Vinci -ohjelmaan kuuluva EU-projekti InCert, jossa laaditaan tämän kurssin tapainen sertifikaatti ja verkkokurssi laboraatioineen. Hankkeessa tarkasteltiin mahdollisuutta mutta ei päästy siihen, että osa laboraatioistakin toteutuisi virtuaalisesti. Tällaiseen suuntaan viittaa mm. artikkeli "Teaching Network Security in a Virtual Learning Environment". [Bergström ym., alunp. 2003, http://jite.org/documents/Vol3/v3p189-217-038.pdf] ¸

TLT-3301 Verkon tietoturva, B-osa, 1. luento 7.1.2009

Verkon hallinta
Käyttöturvallisuus ja **vaatimusluettelo, RFC 3871**
Turvahallinnon tutkimushankkeita

SNMP:n turvallisuus

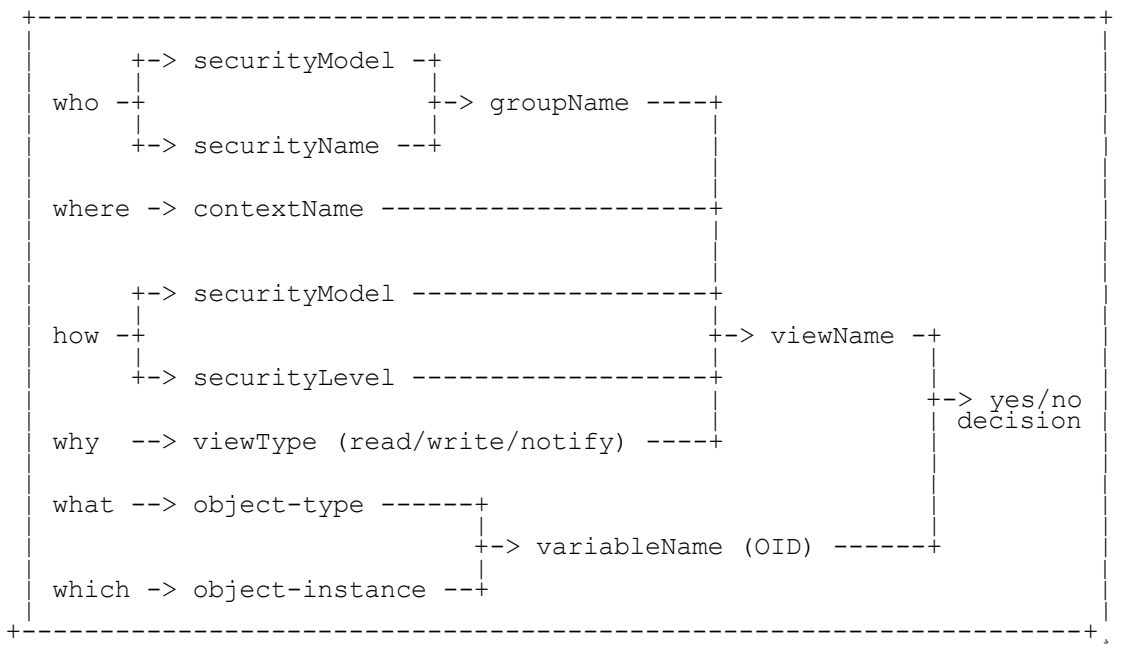
Alkuperäinen SNMP eli SNMPv1 määrittelee käsitteen *yhteisö* (‘community’), johon kuuluu hallinta-agentti ja sen tiettyjä muuttujia kysymään ja/tai kirjoittamaan oikeutetut hallinta-asemat. Yhteisön nimi toimii salasanana, jonka liittäminen viestiin (selväkielisenä) saa agentin tottelemaan.

SNMPv3 määrittelee edistyneempiä turvaominaisuuksia käytettäväksi SNMPv1:n tai v2:n kanssa (2004–). Ensinnäkin on tietoturvaprotokollan tapaisia suojamekanismeja (USM, seuraavassa) ja toiseksi monipuolinen pääsynvalvonnan malli (VACM, jäljempänä), joka eriyttää puoli tusinaa eri ominaisuutta, jotka SNMPv1 niputtaa saman yhteisönimen taakse.

User Security Model (USM) suojaa tiedon muuntelulta ja paljastumiselta, tietovuon muuntelulta (esim. toistohyökkäykseltä) ja impersonoinnilta, mutta ei DoS:lta eikä liikenneanalyysilta. Mekanismeina ovat ensinnäkin CBC-DES-salaus ja sen jälkeen tehtävä HMAC-autentikointi (joko MD5 tai SHA, jotka katkaistaan 96 bittiin). Kummallakin mekanismilla on oma avaimensa, joka konfiguroidaan (ainakin hallittaviin) laitteisiin, mutta se on käyttäjäkohtainen. Avain generoidaan ensinnä käyttäjän 2^{20}-tavuiseksi toistetusta salasanasta tiivistefunktiolla ja sitten laskemalla tiiviste siitä ja hallittavan kohteen tunnisteesta.

Viestin tuoreus tarkastetaan tietynlaisten aikaleimojen avulla. Ne eivät ole kellonaikoja vaan sekunnin välein kasvatettavan laskurin arvoja, jotka ovat yhteisiä kahdelle laitteelle siten, että toinen (yleensä hallinta-asema) ”synkronoi” oman tietonsa toisen lähettämien viestin mukaan. Kellon epätarkkuuden lisäksi synkronointia tarvitaan uudelleenkäynnistymisen yhteydessä, jolloin laskuri alkaa nollasta, mutta siihen liittyvä boot-laskurin arvo kasvaa yhdellä.

View-based Access Control Model (VACM) noudattaa seuraavan kaavion mukaista logiikkaa päättäessään, sallitaanko pääsy hallinnoitavaan kohteeseen (ks. RFC 3415, 2002).



- who: ’turvanimi’ on yhden ihmisen ja ’turvamalli’ erottelee esim. USM:n SNMPv1:stä. Tietyt turvanimet ja -mallit muodostavat ryhmän, jolla on samanlaiset oikeudet.
- where: missä laitteessa käsittelyn kohde sijaitsee (vrt. proxy-tilanne)
- how: ’turvataso’ määräytyy sen mukaan, miten hyvin pääsyä yrittävä viesti on suojattu, ja ottaa huomioon myös ’turvamallin’.
- why: mikä on pääsylaji. Tähän liittyy mallille nimen antava käsite ’MIB view’. Sellainen muodostuu MIB:n alipuiden kokoelmien mukaanottamisten ja poissulkemisten kautta.
- what ja which ilmennevät kaaviosta.

SNMPv1:n haavoittuvuuksia kuvataan CERTin tiedotteessa, joka lähti liikkeelle oululaisen tutkimusryhmän havainnoista: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (http://www.cert.org/advisories/CA-2002-03.html). Sen lopusta löytyvät myös linkit kaikkiin SNMP:n RFC-dokumentteihin.¸

Näkökulma käyttöturvallisuuteen

Vertailtaviksi aiempaan ja tulevaan (RFC 3871) tietoon poimintoja Ciscon sivulta Understanding Operational Security, jossa tarkastellaan MPLS-protokollalla toteutettavaa VPN:ää. ¸

Three Components of Security

Security depends on three components, each of which is independent of the others:

- **Architecture** (or algorithm) set in place: This is the formal specification. In cryptography it is the algorithm itself, in the case of MPLS VPNs, it is the formal specification (as defined in RFC4364).
- **Implementation** of the architecture or algorithm: Refers to how the architecture or algorithm is actually being implemented. Programming mistakes, such as buffer overflows, can affect this component.
- **Operation** thereof: This includes operator issues, such as choosing weak passwords on routers or workstations, or accidental disclosure of a shared key. For example, if configurations are sent to untrusted third parties.

Operational Threats

There are two types of operational security problems:

- **Accidental misconfigurations**: These are accidental in nature, and are by far the most frequent type of operational issues. Mistyping a value (such as the route target in MPLS VPNs) is one example, or forgetting statements in a firewall is another example.
- **Deliberate misconfigurations**: These are deliberate in nature but vary in their degree of maliciousness. For example, an operator that violates the security policy to allow their home system access through the

corporate firewall is not as likely to be as severe as a disgruntled employee who conducts acts of sabotage.

Operational Security Measures

The typical reaction when looking for a solution to a security problem is to look for features to configure. It is important to understand that operational problems cannot be fully solved by features, because the person making the misconfiguration may also remove the feature which is meant to protect against misconfigurations. Operational problems require operational solutions, and an operational competence of the organization.
Operational solutions include:

[Policy – Changes – Access Control – Authorization – Dual Control – Verification – Automation**]**

- **Operational security policy**: There should be clear guidelines on what operators are allowed to do and what they are not allowed to do. Escalation paths need to be defined that outline the steps to follow if an operator does not have the authorization required for a specific action. The operational security policy should clearly define the responsibilities and authorization, as well as disciplinary actions in case of breaches. The policy also acts as a deterrent against deliberate misconfigurations.
- **Change management process**: Every company running a network should create precise processes that define and control how changes to the network are executed. The state of the hardware, operating system and configurations should be monitored, and all changes should be logged and executed in a controlled way. The logs should be evaluated and checked for potential misconfigurations. The logs can also be used to demonstrate a deliberate breach of the operational security policy. (For this, the concept of *dual control* is important, see below.)
- **Access control**: It is a good practice to restrict access to network devices. Access restrictions are traditionally implemented in networks via AAA authentication. This security measure is typically executed; although, in many networks too many operators have access to network devices. Restricting this number to the minimum amount of operators necessary reduces the risk.
- **Authorization**: The access an operator has should be restricted to the minimum access needed for the operator to do their job. In most cases it is not a good idea for all operators to have full-enable access (level 15) to devices. This practice can be more difficult to implement; however, simple distinctions, for example, who can and cannot enter configuration mode, go a long way.
- **Dual control**: Security control and network control should not be the responsibility of the same group. Ideally, a security group controls who has access to what, and a network group executes the configuration actions. Typically the logs are controlled by the security group. This way it is much harder to deliberately misconfigure devices, since the security team could recognize a misconfiguration in the log files.
- **Secure and verify**: All of the above measures are active attempts to detect a change in the network, such as a configuration change. It is also possible to detect policy violations by analyzing the traffic on the network, or the state of dynamic information such as routing tables, ARP tables, etc. For example, intrusion detection systems can create alerts when flows are seen on the network that do not correspond to the policy. There are many other ways to

monitor for traffic anomalies. For example, Cisco IOS Netflow can be instrumental in detecting misrouted packets on the network and routing tables can be checked for missing or unknown routing prefixes.

- **Automation**: It is generally recommended to automate processes and procedures, specifically recurring verification processes, because humans tend to overlook details in log files and similar processes. Automated processes are also less likely to make mistakes; although if a mistake does happen it is often systematic and therefore easily detectable.

Turvavaatimuksia ISP:n verkolle

Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure, eli RFC 3871 (Informational, 2004) pyrkii määrittelemään turvavaatimukset laajan IP-verkon runkolaitteille.

Seuraavassa on luettelo RFC 3871:n vaatimusten (lyhennellyistä) otsikoista. Vaatimuksissa esiintyy RFC:lle tyypillisiä sanoja MUST, SHOULD, MAY ja näiden vastakohtia, eikä näistä otsikoista voi vielä päätellä muuta kuin, että tiettyihin asioihin kiinnitetään huomiota. Vaatimus voi olla myös moniosainen esim. siten, että laitteen TÄYTYY antaa mahdollisuus johonkin toimeen ja kyseistä toimea PITÄISI käyttää. Luetteloon on [-]:llä merkitty ne muutamat, joita suositus ei aseta kaikille hallinnoitaville verkon infralaitteille minimivaatimuksiksi. Ne ovat lisävaatimuksia 3-kerroksen reunalle.

Toiminnalliset vaatimukset (§2.1–2.13)

Laitteiden hallinta (§2.1)
- Kanavat turvalliselle hallinnalle

Hallinta datan kanssa samaa kanavaa käyttäen (’In-Band’) (§2.2)
- Avoimesti arvioitavissa olevan kryptoalgoritmien ja -protokollien käyttö
- Vahvan kryptografian käyttö
- Kryptoparametrien valikoitavuus
- Hallintatoimille korkeampi prioriteetti

Hallinta erillisen kanavan kautta (’Out-of-Band’) (§2.3)
- Konsoliliittymän olemassaolo
- Konsolilta pitää voida resetoida
- Konsoli edellyttää mahdollisimman vähän oheislaitteilta
- Konsolilta pitää voida autentikoitua tarpeen vaatiessa suoraan
- Datan ja hallinnan kanavien erottaminen
- Hallinta- ja datatasojen välillä ei saa olla edelleenlähetystä

Konfiguroinnin ja hallinnan käyttöliittymä (§2.4)
- Komentoriviltä (tai vast.) pääsee kaikkiin toimintoihin
- Hallintatoimenpiteiden ilmaisu komentojonoilla
- Hallinta myös ”hitaiden” linkkien yli
- Toimettoman istunnon aikakatkaisu
- Ohjelmistojen asennusmahdollisuus
- Konfiguraation etävarmuuskopiointi ja palautus
- Ihmisen luettavissa oleva konfiguraatiotiedosto (tekstimuotoisuus)

IP-pino (§2.5)

- Kaikkien kuulolla olevien palvelujen näyttäminen
- Minkä tahansa palvelun pois kytkeminen
- Kuulolla olevien palveluliittymien hallinta (esim. porttien)
- Palvelujen lähdeosoitteen hallinta
- [-] Automaattinen anti-spoofing verkoille, jotka ovat ’single-homed’
- [-] Automaattinen “bogonien” ja “marsilaisten” hylkääminen
  (= mahdottomat sekä väärin reitittyvät erityisesti ”spoofatut” osoitteet.
  RFC 4949, Internet Security Glossary ei tunne bogoneita ja ei suosittele marsilais-termin käyttöä.)
- [-] Pudotettujen väärennettyjen pakettien laskenta

Liikennöinnin nopeuden rajoittaminen (§2.6)
- [-] Tuki sille yleisesti (DoS-torjuntana),
- [-] suuntaan perustuen liittymäkohtaisesti
- [-] tilaan perustuen (niillä protokollilla joilla on tila),

Suodatuksen peruskyvyt (§2.7)
- IP-liikenne ylipäätään
- Liikenne jonka kohteena laite on ja
- [-] laitteen läpi menevä
- Toiminta ilman suorituskyvyn laskua
- Laitetta päivittävien protokollien suodatus (=reititystiedot)
- Suodatuksen tuloksena sallinta, torjunta (+ilmoitus) tai pudotus
- Kaikkien tulosten lokikirjaus

Pakettisuodatuksen kriteereitä (§2.8)
- Protokollan perusteella
- Osoitteen perusteella
- Protokollaotsikon minkä tahansa kentän perusteella
- Sekä sisään että ulos ,

Pakettisuodatuksen laskurit (§2.9)
- Täsmällinen suodatuksen osumien laskenta
- Laskurien näyttäminen yleisesti ja
- sääntökohtaisesti ja
- sovelluskertakohtaisesti (jos samalla yhteydessä voidaan soveltaa useita kertoja)
- Laskurien nollaus
- Laskurien on oltava tarkkoja

Muita pakettisuodatuksen vaatimuksia (§2.10)
- Lokin rakeisuuden määrittely sääntökohtaisesti

Tapahtumakirjanpito (§2.11)
- Lokien keruu avointen standardien perusteella
- Mahdollisuus kerätä loki etäpalvelimeen (useaankin)
- Lokitietojen luotettava siirto
- Mahdollisuus paikalliseen lokiin
- Tarkka aika!
- Aikavyöhykkeen ja UTC-eron näyttö
- Oletuksena UTC-aika
- Lokitiedot pitää aikaleimata
- Lokitiedoissa osoitteet todellisia
- Lokeihin sisältyvät turvatapahtumat
- Ei salasanoja!,

Autentikointi, valtuutus ja tilinpito (AAA) (§2.12)
- Käyttäjien kaiken pääsyn autentikointi
- yksilöittäin
- Samanaikaisten yhteyksien tuki eri käyttäjiltä
- Mahdollisuus poistaa kaikki paikalliset käyttäjätunnukset
- Tuki keskitetylle käyttäjän autentikoinnille ja
- mahdollisesti myös paikalliselle
- Eri autentikointimenetelmien sovellusjärjestyksen asettaminen
- Ei selkotekstisiä kiinteitä salasanoja
- Ei oletussalasanoja tai vastaavia kiinteitä tunnisteita edes alkukonfiguraatiossa
- Mahdollisuus eritellä tarkasti käyttöoikeudet ja
- asettaa ne käyttäjittäin ja
- oletuksena oltava 'ei-oikeuksia'
- Jos käyttöoikeus on muuttunut, tarvitaan uudelleenautentikointi
- Tarkkaan säädelty, mahd. fyysinen, takaovi ylläpitäjille¸

Linkkikerroksen laitteiden on toteutettava ylemmän kerroksen vaatimukset (§2.13)

Turvaominaisuudet eivät saa aiheuttaa käyttöongelmia (§2.14)

Turvaominaisuudet saavat vaikuttaa suorituskykyyn vain minimaalisesti (§2.15)¸

Dokumentaatio: Nämä ovat vaatimuksia valmistajalle
- Kaikki palvelut, joita laitteessa voi olla (§3.1)
- Palveluiden oletusarvot (§3.2)
- Palveluiden käynnistämisen prosessi (§3.3)
- Komentorivikäyttöliittymä (§3.4)
- Konsoliliittymä (§3.5)

Vakuuttavuus
- [-] IP-pinon alkuperä (§4.1)
- [-] Käyttöjärjestelmän alkuperä (§4.2)¸

Myös ITU on "standardoinut" turvaominaisuuksia. Ensinnäkin
E.408 (04 / 2005): **Telecommunication networks security requirements**

ja erityisesti puheena olevaa hallintaa:

M.3016.**0** (05/05) **Security for the management plane: Overview**
M.3016.**1** (04/05) **Security for the management plane: Security requirements**
M.3016.1 (2005) Corrigendum 1 (11/05) mm. "vain SNMP:n versiota 3 saa käyttää"
M.3016.**2** (04/05) **Security for the management plane: Security services**
M.3016.**3** (04/05) **Security for the management plane: Security mechanism**
M.3016.**4** (04/05) **Profile proforma**

Vasta "pre-versio" saatavissa (2009 alussa): M.3410 (08/08) **Guidelines and requirements for security management systems to support telecommunications management.** Summary: This recommendation describes a set of functions considered necessary for the management of security mechanisms deployed in current and next generation packet oriented networks. A logical collection of management functionality used to perform "Operations, Administration, Maintenance and Provisioning" (OAM&P) of security mechanisms, policies and services within a services and communications infrastructure.)¸

Verkon turvahallinnan apuvälineitä

Tässä esitellään lyhyesti kaksi tutkimushanketta. Tarkemmat tiedot pitää lukea lähteistä.

Luottamuksenhallinta

Ensimmäinen esimerkki on STRONGMAN = Scalable TRust Of Next Generation MANagement.
LUE: artikkeli sen arkkitehtuurista (Keromytis ym. 2003, ks. videoesitys 2001). Sen abstraktia mukaillen:

Suunnitteluperiaate, jonka ansiosta Internet on skaalautuva:
paikallista autonomiaa rajoitetaan vain kun se on välttämätöntä kokonaisuuden kestävyydelle.
Turvapolitiikkojen määrityksessä ja toteuttamisessa
ei ole saavutettu vastaavaa skaalautuvuutta ja hajautettua kontrollia.
Puute on korjattava, jos halutaan, että
päästä-päähän -mekanismit koskaan korvaavat lyhytnäköiset ratkaisut kuten palomuurit.

STRONGMAN tarjoaa kolme uutta väylää skaalautuvuuteen soveltamalla paikallisesti turvapolitiikkoja, jotka ovat kuitenkin globaaleja:

1. vastaavuustarkistin, joka tuottaa paikallisen autonomian.
2. mekanismi, jolla politiikkasäännöistä rakennetaan yhtenäinen, toteutettava sääntöjoukko
3. politiikan tulkinnan laiskuus, jolla vähennetään tilatietoa politiikan toteutuspisteissä.

Artikkeli soveltaa näitä **hajautettuun palomuuriin**
= globaalin politiikan soveltaja jokaisessa päätepisteessä.

Pohjalla on KeyNote-järjestelmä (vrt. TTJ:n B-osa)
→ käyttäjät identifioidaan julkisten avainten perusteella.

Konfiguroitsija ja turvatarkistin

Toinen esimerkki on POSITIF = Policy-based Security Tools and Framework.
Se oli EU-projekti 2004–2007 (Torino, Wroclaw, Vodafone ym.) ja lupasi tuottaa myös open source -koodia. Vaikea niitä on löytää sivustolta http://www.positif.org/ . Seuraavassa on siitä lainauksia ja välissä artikkelista A. Lioy: Security analysis and configuration of large networks (Proceedings of *ISSE-2006*, pp. 259-265). **LUE** näitä lähteitä sen verran lisää, että allaoleva konkretisoituu.

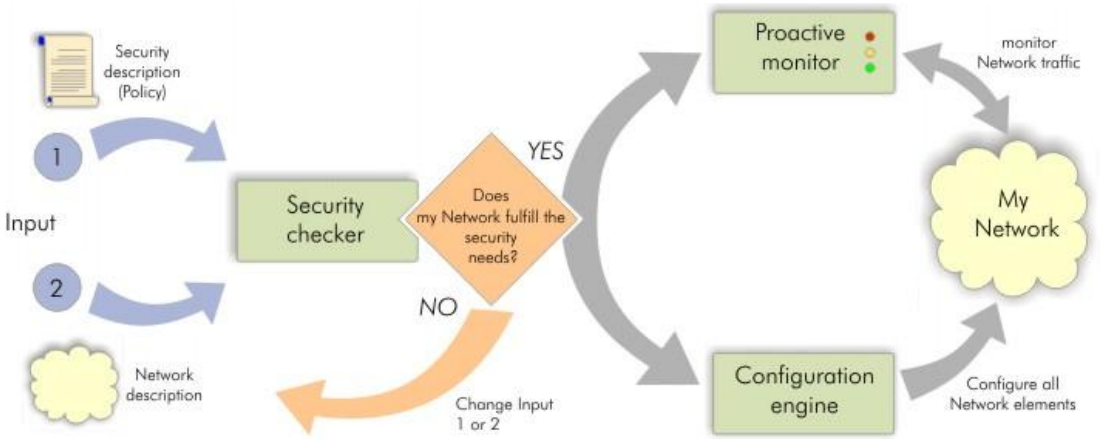
> Today state-of-the-art network systems are becoming increasingly complex in terms of:
>
> - Multiple access ways: wired/wireless; PC / PDA / Cell. Phone
> - New applications with new challenges: P2P, large scale multimedia applications
> - Multiple vendors and HW/SW-platforms due to the growing of nodes and needs within the network
> - Increasing amount of intrusions / spam

> So network administrators need support in order to handle these issues more easily. Besides better training, they need:

- Better security tools and moreover a **better coordination** among these tools
- A reliable / guaranteed answer to the question: "will my network fulfill the desired security needs?"
- An automated support for handling alerts within the network. Or even better: a proactive system that continuously checks the network and provides a self learning mechanism through the handled alerts, attacks and other critical events.

We believe, that the traditional firewall of today will disappear in near future! Security issues will be handled by all elements of the network according to their abilities. ¸

This is how the POSITIF-framework looks like in an overview:



The framework needs two descriptions as an input:

1. The Security Description: The idea is to describe on different levels the security needs of your network.
2. The other input is the description of all elements of your network. Including the security capabilities of each node.

The format for both of these descriptions will be a subset of CIM. [Common Information Model] ¸

Security Checker

The interesting question for every System administrator is: Will my network fulfill my security needs? The POSITIF framework has developed a module to answer this question accurately. In addition to that answer, the security checker gives you also a sort of measurement of the actual level of security achieved by the policy given the network architecture.

two outputs:
- which attacks can be countered by the system and
  ≈ a measure of the security of the system
- how it should be configured to achieve the desired protection level.

It does NOT dynamically scan a real system and look for known vulnerabilities.
INSTEAD: a static analysis of an ICT system,

¸

Configuration engine

Once you can be sure, the your network fulfills the required security needs, you need to configure all your network elements.

When you think of a Multi vendor and/or multi HW/SW-platforms this is not an easy task.

The POSITIF framework has developed an automatic configuration engine to load the desired configuration into the various elements, like firewalls and switches / routers / hubs.

> The generic nature of these [configuration] data is useful for two reasons.
> - First, for defence-in-depth we can easily require that all elements with a certain capability do enforce the same protection rule. For example, we could filter unwanted traffic not only at the network border but in every element with a filtering capability, be it a router, a switch or a server.
> - Additionally, the use of a generic configuration allows an optimal splitting between the blockindependent and the block-specific parts.

Proactive Monitor

The proactive Security Monitor checks permanently the network for any behaviour that violates the deployed security policy. It does not only collect the events through sensors it also compares monitored data against the policy. This method allows the detection of even unknown attack signatures.

The monitor works in two ways: It uses standard threats and vulnerabilities and secondly the enforced policy.

If an event is monitored the output will be an alarm with certain severity. Also semiautomatic or automatic reactions can be enforced. If a security violation is detected an updated security policy will be deployed either to the full system or part of the targeted system.

The Monitor also tests the proper behaviour of the enforced policy by sending dummy attacks to a part or the network and verifying the result of the attack.

The main difference to solutions on the market is the active and passive component of the PSM. Together with the POSITIF Framework the security of a complex network can be raised easily.

TLT-3301 Verkon tietoturva, B-osa, 2. luento 14.1.2009

ISP:n turvakäytäntöjä

Vallitsevien käytäntöjen kartoituksella on Opsec-työryhmässä saatu aikaan RFC 4778, **Current Operational Security Practices in Internet Service Provider Environments** (Informational, 2007).

Uhkamallina RFC mainitsee seuraavat ja niiden yhdistelmät

```
Reconnaissance
Man-In-The-Middle
Protocol Vulnerability Exploitation
Message Insertion
Message Diversion/Deletion
Message Modification¸
```

Palvelunesto mainitaan erikseen koska se on usein seurausta muista em. uhkista.

Hyökkäysten lähteiden jaottelu:

```
Active vs Passive Attacks
On-path vs Off-path Attacks
Insider vs Outsider Attacks
Deliberate Attacks vs Unintentional Events
```

Uhkien seuraukset toiminnalle:

```
(Unauthorized) Disclosure
Deception
Disruption
Usurpation¸
```

ISP:n toimintojen suojaukset esitellään näihin turvapalveluihin jaoteltuina:

```
1 User Authentication
2 User Authorization
3 Data Origin Authentication
4 Access Control
5 Data Integrity
6 Data Confidentiality
7 Auditing/Logging
8 DoS Mitigation
```

Suojauksen kohteena olevat ISP:n toiminnot puolestaan jaotellaan seuraavasti. Kussakin kohdassa luonnostellaan ensin uhkat, sitten selvitetään tavanomaiset käytännöt (=RFC:n pääanti). Tähän on merkitty numeroilla, mitkä edellisistä turvapalveluista tulevat kyseeseen (ja - tarkoittaa ”not implemented”). **LUE** ainakin kunkin kohdan ”`Security Practices` ” eli alaluvut 2.x.2 missä x=1..6.

```
Device Physical Access                          1 2         7
Device Management In-Band and Out-of-Band       1 2 3 4 5 6 7 8
Data Path  (hyötykuorman suojaaminen)             3 4     7 8
Routing Control Plane                             3 4 5 - 7 8
Software Upgrades and
      Configuration Integrity/Validation        1 2 3 4 5 6 7 8
Logging Considerations                            - 4 - - 7 8
```

¸

Samassa luvussa 2 on vielä lisätietoja kahdesta tärkeästä aiheesta. **LUE** nämä alaluvut 2.7. ja 2.8.

Filtering Considerations
Denial-of-Service Tracking/Tracing

Suodatus tapahtuu kolmella tasolla, jotka ovat data, hallinta ja reitityskontrolli. DoS-jäljityksessä esitellään (3. luennolla mainitut)
Sinkhole Routing
Black Hole Triggered Routing
Unicast Reverse Path Forwarding
Rate Limiting ¸

Reitityksestä

NIST-ohjeisto SP800-54 Border Gateway Protocol Security(2007) esittelee BGP-protokollan, selittää sen merkityksen Internetille ja tarjoaa joukon parhaita käytäntöjä, joilla BGP:n toimintaa voi turvata. Kyseisten käytäntöjen pitäisi olla sovellettavissa lähes kaikissa nykyisin (2007) saatavilla olevissa BGP-reitittimissä. On myös olemassa lukuisia laajennusesityksiä BGP:hen, mutta ne vaativat muutoksia protokollaan eivätkä mahdollisesti ole yhteensopivia nykyisten toteutusten kanssa. Vaikka dokumentissa esitetyt suositukset voivat huomattavasi parantaa BGP:n turvallisuutta, ne eivät muodosta täydellistä puolustusta kaikkia uhkia vastaan. Yksilöllisten tarpeiden mukaan näistäkin pitää valita sopivimmat. ¸

Ohjeisto esittelee seuraavat hyökkäykset BGP-protokollaa vastaan:

- Peer Spoofing and TCP Resets
- TCP Resets Using ICMP
- Session Hijacking
- Route Flapping
- Route Deaggregation
- Malicious Route Injection
- Unallocated Route Injection
- Denial of Service via Resource Exhaustion
- Link Cutting Attack ¸

Jokaisen torjumiseen mainitaan ja arvioidaan joitakin mekanismeja, jotka ovat osittain yhteisiä (kuten IPsec). Osa mekanismeista esitellään erikseen ja ne ovat:

- Prefix Filtering
  - Special Use Addresses
  - “Bogon” Addresses
  - IPv4 Filtering Guidelines
  - Access Control Lists
  - Peripheral Traffic Filtering
  - Reverse Path Source Address Validation
- Sequence Number Randomization
- Generalized TTL Security Mechanism (TTL Hack)
- MD5 Signature Option
- IPsec
- BGP Protocol Variations and Configuration
- Router Protection and Physical Security

ja lisäksi kaatumisesta toipumiseen:

- Graceful Restart Mechanism for BGP
- Virtual Router Redundancy Protocol¸

”Johdon tiivistelmän” mukaan suositukset ovat seuraavat:

Käytä pääsylistoja; saatavina lähes kaikissa reitittimissä (§4.2)

Käytä BGP:n uudelleen käynnistyksessä “graceful”-ominaisuutta, jos se on mahdollista, ja sovella tuoreimpia valmistajan suosittelemia oletusasetuksia (§5.1).

Käytä BGP:n vastinolion autentikointia: joko IPseciä tai BGP MD5 -mekanismia. (§4.5 ja 4.6).

Käytä prefiksin rajoittimia estämään reititystaulujen täyttyminen. Mikäli naapuri lähettää rajan ylittävän määrän prefiksejä, reitittimen pitäisi estää tai lopettaa BGP-istunto sen kanssa ja lähettää varoitus ylläpitäjälle (§4.2)

Salli vastinolioiden yhteydenotot vain porttiin 179, joka on BGP-istunnon avauksen normaali portti.¸

Konfiguroi BGP sallimaan vain määrättyjen verkkolohkojen mainostaminen. Tämän avulla reititin ei pääse vahingossa tarjoamaan läpikulkua verkkoihin, joita AS:ssä ei ole listattuna (AS=autonomous system; §2.3).

Suodata pois kaikki bogon-prefiksit, eli sellaiset virheelliset prefiksit, joita reiteissä ei pitäisi lainkaan esiintyä (§4.2.2). Tämä vähentää kuormaa ja vähentää hyökkääjien mahdollisuuksia käyttää keksittyjä osoitteita DoS-tarkoitukseen tai muuhun.

Reitittimien pitäisi suodattaa vertaisolioilta tulevat viestit, mikäli mahdollista. Kyseessä on siis ingress-suodatus (§4.2 ja 4.2.5).

Älä salli tarpeettoman tarkkoja prefiksejä, koska suuren määrän ylläpitäminen voi kuormittaa järjestelmää liikaa. Suositukset vaihtelevat siitä, mikä on liian tarkkaa, mutta järkevä kriteeri voisi olla välillä /24 – /30.¸

Kytke pois ”fast external failover”, jotta voit välttää merkittävät reittimuutokset, jotka olisivat vain seurauksia vastinolioiden ohimenevistä ongelmista keepalive-viestin lähetyksessä. Kyseinen failover-ominaisuus oli suunniteltu tarjoamaan nopea siirtymä vaihtoehtoiseen järjestelmään linkin kaatuessa. Ilman tätä ominaisuutta siirtymä ei tapahdu ennen kuin BGP:n keepalive-ajastimet tunnistavat linjan katkenneen. Ei ole epätavallista, että linjat pudottavat BGP-istuntoja ja sitten palautuvat. Tästä käytetään termiä reitin lepatus (route flapping; §3.2.4). Tiheä lepatus saattaa laukaista lepatuksen vaimennuksen ylävirran vastinolioissa. Nopean ulkoisen failover-ominaisuuden tuottama lepatuksen vaimennus ylävirran reitittimissä saattaa pitkittää vastinolioprefiksin saavutettavuutta ja sitä kautta tehdä järjestelmästä epästabiilin. Näin ollen poiskytkentä on normaalisti myönteinen kompromissi nykypäivän Internetissä.¸

Lepatuksen vaimennuksella on sekä myönteisiä että kielteisiä vaikutuksia ja nykytutkimuksen valossa se on parempi kytkeä poisi ellei organisaatiolla ole vahvoja syitä sen käytölle. (§ 3.2.4 käsittelee lepatuksen vaimennusta eli route flap damping -ominaisuutta, RFD)

Jos RFD:tä käytetään, pitempiä prefiksejä pitää vaimentaa vaimentaa voimakkaammin. Niillä on taipumus olla vähemmän stabiileja, joten pitemmät RFD-ajat ovat suositeltavia. Esimerkinomaisia RFD-vaimennuksen puoliintumisaikoja ovat
– .. /21 – enintään 30 min. Valmistajien suosituksena tavanomainen on 15 min.
– /22 .. /23 – enintään 45 min
– /24 .. – enintään 60 min.

Älä käytä RFD:tä verkkolohkoille, joissa on DNS:n juuripalvelimia.
These networks are normally the most stable, and can be expected to remain operating in all but the most exceptional circumstances. Damping these netblocks would therefore be likely to have more negative results than benefits. DNS root servers are also critical for Internet operations, so degraded access to them could cause widespread disruption of network operations.

Käytä pehmeää uudelleenkonfigurointia silloin kun se on käytännöllistä.
Normally a change in policy requires BGP sessions to be cleared before the new policy can be initiated, resulting in a need to rebuild sessions with consequent impact on routing performance. Thus, spoofed policy changes could be used for a denial of service attack, even if the policy changes themselves do not violate AS rules. Soft reconfiguration allows new policies to be initiated without resetting sessions. It is done on a per-peer basis, and can be set up for either inbound or outbound or both (for updates from and to neighbors, respectively). A recent improvement to soft reconfiguration is Route

Refresh (RFC 2918 [36]). The route refresh capability allows dynamic exchange of route refresh requests between BGP peers, to obtain a readvertisement of Adj-RIB-Out. This capability avoids the need to store unmodified copies of the routes learned from peers at all times.

Talleta vastinolioiden muutokset eli tee lokimerkintä aina kun vastinolio tulee tulee tilaan Established tai poistuu siitä. Tästä muodostuu hyödyllistä tietoja, jonka avulla voi selvittää virheitä tai tutkia turvaongelmia. ¸

Nimipalvelusta

NIST-ohjeisto SP800-81 on Secure Domain Name System (DNS) Deployment Guide (2006) toteaa DNS:n erityispiirteeksi turvallisuuden kannalta sen, että tieto on julkista eikä sen käyttäjiä rajoiteta maantieteellisen sijainnin tai muun topologian mukaan.

Ohjeiston mukaan erityisongelmia on:

- Hyökkääjä joka väärentää DNS-solmun, voi estää kaikkien pääsyn resursseihin joista kyseinen solmu vastaa.
- Väärennetty tieto voi myrkyttää kyseistä DNS-tiedon osajoukkoa tarjoavan DNS-solmun välimuistin.
- DNS:n ketjumaista tiedonhakua on mahdollista häiritä särkemällä autoritatiivisen tai välillisen DNS-tiedon eheys.
- Jos DNS:ssä talletettu nimidata ei noudata DNS-standardia, tuloksena voi olla ylimääräistä kuormaa tai vanhentunutta tietoa joka voi johtaa DoS:iin.¸

DNS:n turvaaminen yleisellä tasolla:

- DNS:n ajoympäristön turvallisuus: KJ, sovellukset, prosessien eristäminen, verkon vikasietoisuus.
- DNS-transaktioiden turvaaminen yhteisiin salaisuuksiin perustuvien MAC-koodien avulla (IETF:n TSIG-määritys).
- Nimikyselyjen ja -vastausten turvaaminen DNSSEC:n määrittelemillä digitaalisilla allekirjoituksilla.
- Eheystarkistusten soveltaminen DNS-dataan.¸

Johdon tiivistelmään asti on nostettu keskeiset vaiheet DNSSEC:n käyttöön:

- nimipalvelimen asennus
- eheystarkistus
- avainparin luonti
- vyöhykkeen (eli nimidatan) allekirjoittaminen
- allekirjoitetun vyöhykkeen lataaminen palvelimeen
- DNSSEC:n kytkeminen käyttöön
- Mahdollisesti: julkisen avaimen lähetys hierarkiassa ylemmälle tasolle delegointia varten

Näistä ja muista turvaamisen vaiheista muodostuu 33-osainen tarkistuslista, joka on koottu lukujen 7–11 loppuun alalukuihin nimeltä Recommendations Summary.¸

Langattomat verkot

Langattoman lähiverkon standardi IEEE 802.11i sisältää käsitteen Robust Security Network (RSN), joka tarkoittaa että langattomien yhteyksien (RSN-assosiaatioiden) turvallisuus on kryptografisten mekanismien ansiosta “keskimääräisellä tai korkealla tasolla”. NIST-ohjeisto SP800-97 vuodelta 2007 käsittelee RSN:n toiminnan ja askelet, joilla sellainen voidaan muodostaa. ¸

Ohjeiston keskeinen osa tämän kurssin kannalta on 17-sivuinen tarkistuslista, jossa käydään läpi vaiheet esisuunnittelusta alkaen ja päättyen käytöstä poistoon. Jokaiseen toimeen on merkitty, mitä komponenttia se koskee: päätelaitetta (STA), pääsypistettä (AP), autentikointipalvelinta (AS) vai useampia näistä. Autentikointipalvelin on RSN:n mukana tullut uusi komponentti. Lisäksi jotkin toimet koskevat AP:n ”takana” olevaa jakelusysteemiä (DS), joka on tyypillisesti langallinen lähiverkko, jossa AS sijaitsee. Silti RSN koskee vain linkkitason turvallisuutta eli väliä STA–AP tai STA–STA. Jälkimmäinen eli päätelaitteiden välinen tapaus edustaa ad hoc -tyyppistä verkkoa. ¸

Keskeinen kryptoprotokolla on 4-tiekättely, jolla linkin osapuolet varmistavat, että kummallakin on osapuolien välinen yhteinen avain PMK (pairwise master key). Samalla synkronoidaan vaihtuvat avaimet ja valitaan kryptoalgoritmit. Avainten hallinnointiin liittyy melko mutkikas hierarkia, jossa on mukana myös ryhmäavaimia. Ohjeistossa on selostettu kryptologisia seikkoja melko paljon. Lisää mutkikkuutta koituu siitä, että 802.11i-standardi soveltaa aiempia menetelmiä, joilla WLAN-turvallisuutta ja erityisesti heikoksi osoittautunutta WEP-mekanismia on paranneltu. Erikseen on vielä laadittu ohje *Guide to Securing Legacy IEEE 802.11 Wireless Networks* (SP800-48r1). Kryptoprotokollia käsitellään tarkemmin omalla kurssillaan (mm. EAP, Extensible Authentication Protocol variaatioineen). ¸

Tarkistuslista sisältää yhteensä 58 suositusta selityksineen. Monet niistä ovat tuttuja verkon turvaamisen yleisistä periaatteista. **LUE** suositukset niin, että tiedät mitä WLAN-spesifistä niissä on eri vaiheissa. Vaiheet ja niihin liittyvien suositusten määrät ovat:

Alustus: 11; suunnittelu: 9; hankinnat: 16; asennus: 10; käyttö ja ylläpito: 11; käytöstä poisto: 2.

TLT-3301 Verkon tietoturva, B-osa, 3. luento 21.1.2009

Päällysverkoista: p2p- ja yhteistyöverkot kuten Grid.
Ad hoc -verkoista (oheistekstin pohjalta)¸

Ensin viittaus tutkimukseen, joka liittyy kahden viikon takaiseen Strongman-hallintatyökaluun: *Design and Implementation of Virtual Private Services* (S. Ioannidis ym. 2003). Lainaus tiivistelmästä:

> Laajat hajautetut sovellukset sähköisessä kaupankäynnissä ja online-kaupassa yhdistävät verkkoliikenteen ja lukuisia tallennuksen ja laskennan komponentteja. Resurssien hallinnan hajautuminen ja toimintaympäristön mutkikkuus luo suuria haasteita tietoturvallisuudelle. Politiikkojen käsittely useissa paikoissa vaatii käyttämään tavanomaisia työkaluja kuten palomuureja ja tiedostojen hakemistorakenteita kömpelöillä ja virhealttiilla tavoilla.
>
> Tässä hankkeessa esitetään virtuaalisten yksityispalvelujen lähestymistapa kyseiseen ongelmaan. Ensinnäkin politiikan määritys ja politiikan toteutus eriytetään siten, että saadaan paikallinen autonomia – kokonaisvaltaisen politiikan puitteissa. Jokaisella toimialueella on sitä koskeva joukko oikeuksia, jotka rajoittavat sen resurssit ja määräävät mitä palveluja sen pitää toteuttaa. Virtuaaliset yksityispalvelut takaavat turvapolitiikkojen noudattamisen koordinoitujen toteutuspisteiden kautta.

Ideana siis Strongmanin tapainen paikallinen politiikan toteutus. Tässä on kyseessä vielä ”tavanomainen” verkko, ei P2P tai ad hoc. ¸

Yhteistyöverkot

Artikkeli *Operational Security Requirements for Large Collaborative Compute Infrastructures* (H. Khurana ym. 2007) käsittelee erityispiirteitä sellaisessa verkossa, joka muodostuu useiden organisaatioiden välille ja joka sisältää erityisiä yhteisesti käytettäviä tietojenkäsittelyresursseja. Tyyppiesimerkkejä tällaisista ovat GRID-verkot. Turvaamisen haasteita ovat organisaatioiden ja usein myös maiden rajojen ylitys ja heterogeeniset resurssit. Monet artikkelin esittämistä ongelmista ja ratkaisuista ovat kuitenkin tuttuja normaalista verkon turvaamisesta. Tässä on artikkelin nimen mukainen luettelo siitä, mitä pitää muodostaa tai ottaa huomioon: ¸

Turva-arkkitehtuuri, jossa on ainakin
- organisaatioiden rajat ja turvapiirit
- vaatimukset kunkin resurssiluokan turvaamiseksi
- työkalut, tekniikat ja mekanismit joilla vaatimukset voidaan toteuttaa
- arkkitehtuuria koskevat riskianalyysi erityisesti jäännösriskin löytämiseksi¸

Sopimukset eri organisaatioiden välille
- Perusturvallisuussopimus, jossa on ainakin
  - vähin hyväksyttävä ehkäisypolitiikkojen ja -proseduurien taso
  - lisävaatimukset niille toimipaikoille, jotka tarjoavat kriittisiä resursseja, esim.
    - käyttäjätilien hallintaa.
- Loukkausten käsittelyn sopimus, jossa on ainakin
  - yhteystietoja
  - turvallisen viestinnän vaatimukset ja ratkaisut
  - vastesuunnitelma (normaaliin tapaan, mutta mukana yhteistyön vaatimus)
  - ulkoisen viestinnän säännöt¸

Toteutuksen integrointisuunnitelma, ainakin
- arviot henkilöstön ja koulutuksen tarpeesta

kustannusarvio: henkilöstö, työkalut, mekanismit
suunnitelma toimenpiteiden ajoituksesta ja käytännön toteutuksesta
auditoinnit ja harjoitukset, erityisesti yhteensopivuuden takaamiseksi
ylläpitosuunnitelma¸

Osapuolia edustava turvahallinnon auktoriteetti, työryhmä, joka
laatii em. dokumentit
saa niille suostumuksen kaikilta organisaatioilta
hoitaa dokumenttien päivitykset
määrittelee lisätoimia, esim. kriittisiin paikkoihin asennettavien ohjelmistojen turva-arvioinnille¸

Toinen artikkeli on *Re-thinking Grid Security Architecture* (Y. Demchenko ym. 2008). Se on edellistä teknisempi ja viittaa lukuisiin Grid-rakenteiden turvaamishankkeisiin (turhan vaikeaselkoinen kurssivaatimuksiin otettavaksi).

Kaksi viikkoa sitten oli Strongmanin rinnalla esillä Positif-hanke. Kyseessä oli toimialueen sisäisen politiikan automatisointi. Kun sitä ajatusta yleistetään yhteistyöverkkojen tapaisesti tietynlaisiin päällysverkkoihin, tarvitaan taas uusia mekanismeja. Näitä käsittelee artikkeli *Building and Managing Policy-Based Secure Overlay Networks* (G.M.Pérez ym. 2008). Erityisesti siinä esitetään turvatasosopimuksen (SecLA) laadintaa ja välineenä on tässäkin CIM eli Common Information Model. ¸

Sosiaalinen VPN

Artikkelissa *Social VPNs: Integrating Overlay and Social Networks for Seamless P2P Networking* (R.J. Figueiredo ym. 2008) esitetään uudenlainen arkkitehtuuri ad hoc -tyyppisen VPN-verkon rakenteeksi. Tärkeimmät periaatteet siinä ovat:
1. Kun osapuolilla on alunperin sosiaalisia kytköksiä toisiinsa, IP-verkon päälle konfiguroituu itsekseen kaksisuuntainen virtuaaliverkko.
2. Sosiaalisen verkon infrastruktuurit edistävät luottamussuhteiden muodostumista ja nämä suhteet voidaan integroida olemassaoleviin julkisen avaimen kryptografian toteutuksiin. Niillä puolestaan voidaan toteuttaa päästä-päähän -yhteydet salatusti ja autentikoidusti.
3. Tietoa sosiaalisista kytköksistä voidaan käyttää tehostamaan päällysverkon reititystä. ¸

Kyseinen sosiaalisen VPN:n arkkitehtuuri SVPN yhdistää virtuaaliseen reitittimeen Facebook APIn, virtuaaliset IP-over-P2P -verkot sekä IPsec-rakenteet. Kokeilutoteutus selviää NAT-muunnoksesta ja kykenee tukemaan muuttamattomia TCP/IP-sovelluksia. Tällä on merkitystä silloin, kun halutaan käyttää työpöydän jakamista (esim. VNC tai RDP), audio-streamausta (esim. iTunes), hakemistojen jakoa, audio/video-neuvotteluja tai monen käyttäjän pelejä jne.

Teknisesti SVPN
1) mahdollistaa virtuaalisten nimien ja IPv4-osoitteiden automaattisen sitomisen isäntäkoneisiin tavalla, joka sopii nykyisten verkkojen kanssa yhteen eikä vaadi käyttäjiltä konfigurointia.
2) tukee vertaisolioiden valtuustietojen automaattista generointia, vaihtoa ja löytämistä käyttäen sosiaalisen verkon yhteyksiä. Samalla se tuottaa jo mainitun pasta-päähän –turvan.

Lisätietoa ja koodeja tästä hankkeesta saa sivustolta http://socialvpn.wordpress.com/. **LUE** sivu …/about/. Asiaan liittyy myös wiki.¸

Päällysverkko turvamekanismina

Yksi mahdollisuus DoS-torjunnassa on karsia satunnaisesti ja hyvin vähällä vaivalla liiat paketit. Jotta hyvät paketit pääsisivät kohtuullisella todennäköisyydellä läpi, niitä täytyy vain olla liikkeellä riittävän monena kopiona. Kopioiden lähettäjinä ovat salassa pidettävät solmut päällysverkossa, jonka julkinen osa on sen verran laaja, että se kestää DoS-hyökkäyksen. Tämä on FOSeL-järjestelmän perusidea. **LUE** tarkemmin artikkelista FOSeL: Filtering by helping an Overlay Security Layer to Mitigate DoS Attacks (H. Beitollahi, G. Deconinck, 2008). Se on paikoin kehnoa englantia, mutta tarjoaa silti B-osaan sopivan tieteellisen tutkielman tutustuttavaksi.

FOSeLissa käytetään TTJ:ssä mainintana esillä ollutta päällysverkkoa Chord. FOSeL-järjestelmä ei sovi julkisten palvelujen DoS-suojaksi, vaan se on tarkoitettu suljettuihin verkkoihin, jotka kuitenkin toimivat julkisen verkon puitteissa. Kohdepalvelimet joutuvat siinä tietämään tarkalleen mistä osoitteista tulleet paketit päästetään läpi.¸

Ad hoc -verkot

Maarit Hietalahden lisensiaatintyö Requirements for a security architecture for clustered ad-hoc networks (TKK, 2007) tarjoaa hyvän esityksen ad hoc -verkkojen turvallisuuteen. **LUE** siitä luvut 1–3 ja luku 5 sivuun 35 asti (eli luvun 5.3.5. alkupuoleen asti), yhteensä n. 22 sivua. Työn aiheena ovat tosin klusteroidut verkot, mutta mainituissa jaksoissa ad hoc -verkkoja käsitellään yleisesti. Tarkkoja reititysprotokollien ominaisuuksia ei tarvitse opetella (eikä esim. lukua 2.2.1) . Avaintenhallintaan liittyviä asioita tarkastellaan Kryptoprotokollien kurssilla.