Tietoturvaa peruskäyttäjälle

Tämä on kaikille tietokoneen käyttäjille tarkoitettu tietoturvaohjeisto. Käyttäjillä tarkoitetaan tässä kaikkia, jotka tekevät tietokoneella jotain, oli se sitten pelaamista, tekstinkäsittelyä, nettisurffailua, kirjanpitoa tai jotain muuta. Ohjeistoa ei suinkaan ole tarkoitettu kaikenkattavaksi vaan korostamaan tärkeimpiä perusasioita ja antamaan joitakin käytännöllisiä neuvoja. Rakenne on asteittain tarkentuva:

1. Tiivis "huoneentaulu", joka on tarkoitettu muistilistaksi.
2. Huoneentaulun laajempi versio, joka tarkemmin selittää muistilistan sisältöä.
3. Perusteluja sille, miksi tietoturvan takia kannattaa nähdä vaivaa.
4. Varsinainen opasosa, joka on jaoteltu huoneentaulun mukaan:
    a. Selvitä tiedon ja tiedoston alkuperä ennen käyttöä.
    b. Muista, että seinillä on korvat - useammat kuin arvaatkaan.
    c. Lukitse ovesi ja tietokoneesi, kun lähdet muualle.
    d. Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa.
    e. Älä hätäile, äläkä varsinkaan toimi hätiköidysti.
    f. Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu.
    g. Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä.
    h. Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt.
5. Liitteenomainen ohje palvelinten asentamisesta, joka ei toistaiseksi ole tarpeen käyttäjien enemmistölle.
6. Pohdintaa siitä, miksi viruksia ja muita tietoturvaongelmia on.
7. Jälkipuhe (esipuheen asemesta).
8. Linkkejä lisätietoihin.

Tietoturvan huoneentaulu

a. Selvitä tiedon ja tiedoston alkuperä ennen käyttöä.
b. Muista, että seinillä on korvat - useammat kuin arvaatkaan.
c. Lukitse ovesi ja tietokoneesi, kun lähdet muualle.
d. Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa.
e. Älä hätäile, äläkä varsinkaan toimi hätiköidysti.
f. Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu.
g. Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä.
h. Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt.

Tietoturvan huoneentaulu, laajempi versio

1. **Selvitä tiedon ja tiedoston ja muunkin alkuperä ennen käyttöä.** *Viesti*, joka on tullut tuntemattomasta lähteestä, voi sisältää viruksen tai olla väärennetty. Se, mitä on lähettäjän nimen ja osoitteen paikalla, ei takaa mitään, ei myöskään se, miksi lähettäjä esittäytyy. *Ylläpitäjä*, joka soittaa sinulle ja kysyy salasanaasi, on lähes varmasti huijari. *Ohjelmaa* ei pidä

ajatellakaan asentaa, ellei tiedä, mistä se on peräisin. *Tiedostoa*, jonka alkuperää ei tiedä, ei pidä avata ainakaan "napsauttamalla". Ja kun *lähetät* jotain, kerro, mitä se on, äläkä lähetä *liitetiedostoja* varmistumatta ensin siitä, että niitä halutaan ottaa vastaan.

2. **Muista, että seinillä on korvat - useammat kuin arvaatkaan.** Ole tarkkana siinä, mitä kerrot itsestäsi, läheisistäsi ja organisaatiosi asioista. Tämä koskee sekä kirjoittamista Internetissä että puhumista vaikkapa bussissa. Suuri osa tietoturvan murtumisista perustuu vain siihen, että joku kuuntelee, mitä naapuripöydässä puhutaan. Ole myös aina epäluuloinen, kun joku pyytää tietoa, jonka saamiseen hänellä ei ole mitään ilmeistä tarvetta.
3. **Lukitse ovesi ja tietokoneesi, kun lähdet muualle.** Tietomurto saattaa onnistua naurettavan yksinkertaisesti. Joku voi kävellä sisään ja ruveta käyttämään tietokonettasi. Huolehdi ainakin siitä, että *yleisöllä* (siis kenellä tahansa) ei ole vapaata pääsyä työhuoneeseesi, kun olet itse sieltä poissa. Käytä salasanalla suojattua joutonäyttöä ("näytönsäästäjää").
4. **Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa.** Muista, että salasanan vuotaminen ja arvattavuus tekee hyvin suuren määrän teknisiä turvajärjestelyjä tyhjäksi. Järjestelyt, joiden tarkoitus on taata sinunkin tietoturvasi, eivät auta, jos sinun salasanasi on murrettavissa tai jopa jostakin ongittavissa.
5. **Älä hätäile, äläkä varsinkaan toimi hätiköidysti.** Paniikkiin joutuminen vain pahentaa asioita. Erityisesti ei pidä ruveta levittämään virus- tai muita huhuja eikä noudattaa sellaisia ohjeita, joiden alkuperästä ei ole varma. Jos tietokoneesi näyttää olevan aivan sekaisin, niin hätiköity yritys korjata tilannetta voi aiheuttaa paljon vahinkoa. Kysy ajoissa apua asiantuntijalta.
6. **Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu.** Kaikesta tärkeästä aineistosta tulisi olla kaksi toisistaan riippumatonta kopiota, vähintäänkin varmuuskopio levykkeellä. Kaikesta todella tärkeästä on hyvä olla vähintään kolme kopiota, niistä ainakin yksi fyysisesti turvatussa paikassa, mielellään eri rakennuksessa.
7. **Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelyjä.** Koska viruksia tulee koko ajan lisää, on hyvä päivittää torjuntaohjelma ainakin muutaman kuukauden välein ja aina kun tietoon on tullut erityisiä turvariskejä. Selvitä oman organisaatiosi järjestelyt, esim. pitääkö sinun itsesi hoitaa päivitykset ja miten. Muutkin tekniset turvajärjestelmät kuten ns. palomuuri voivat olla tarpeen.
8. **Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt.** Lue tietoturvasäännöt, kysy asiantuntijalta niistä ohjeista, joita et ymmärrä, ja selvitä etukäteen, minne otetaan yhteyttä, kun vahinko on sattunut. Kun isoja ongelmia syntyy, on ratkaisevan tärkeää, miten nopeasti asiantuntijat pääsevät niitä selvittelemään.

Miksi tietoturvan takia kannattaa nähdä vaivaa?

Niin moni asia riippuu tietokoneista ja tietoliikenteestä

Tietoturvassa on kyse tietojen, tietojärjestelmien ja tietoliikenteen suojaamisesta turmeltumista, luvatonta käyttöä, häirintää, urkintaa ja muita uhkia vastaan. Yritysmaailmassa tietoturvan tarve on yleensä ilmeinen, koska tietojenkäsittelyllä on niin keskeinen osa toiminnassa. Tietokoneiden hyväksikäyttö miltei kaikessa on tuonut suuria etuja. Toisaalta siitä johtuu, että vakavat häiriöt tietojenkäsittelyssä aiheuttavat erittäin suuria ongelmia.

Lisäksi tietoihin sisältyy liikesalaisuuksia ja muuta salassa pidettävää. Ja esimerkiksi sosiaali- ja terveysalalla asiakkaiden yksityisyyden turvaaminen on olennaista ja lakisääteinen velvollisuus. Kyse ei ole vain siitä, että tietojen on oltava luotettavasti saatavilla. Lisäksi niiden *ei* pidä olla kenen tahansa saatavilla.

Uhkia on muitakin kuin ilmeisiä

Mutta monissa yhteyksissä tietoturvan tärkeyttä ei tunneta tai ainakaan oteta huomioon, ainakaan käytännön toiminnassa. Esimerkiksi julkisella laitoksella ei ole samanlaista intressiä salata tietojaan kuin yrityksellä. Mutta aina on *joitakin* tietoja, jotka on pidettävä salassa, ja joka tapauksessa on paljon tietoja, jotka on *säilytettävä* ja suojattava asiattomalta muuttamiselta. Kun esimerkiksi yliopiston kaikki opintosuoritukset viedään ATK-rekisteriin, monia asia romahtaa monen ihmisen elämässä, jos se tuhoutuu vaikkapa ohjelmistovian takia, ellei rekisteristä ole ajantasaisia varmuuskopioita.

Yksityinen ihminen ajattelee helposti, ettei hänen kotitietokoneessaan olevista tiedoista kukaan ole kiinnostunut. Ilme voi muuttua, kun huomataan, että koneeseen päässyt virus on lähettänyt yksityisen päiväkirjan Internetiin miljoonien ihmisten naureskeltavaksi.

Eri turvataso eri tilanteisiin

Suhteellisuudentaju on tarpeen, koska tietoturvajärjestelyt aiheuttavat aina jonkin verran lisätyötä sekä rajoituksia ja joskus harmiakin tietokoneiden ja tietoliikenteen asialliselle käytölle. Täydellistä tietoturvaa ei voida saavuttaa, mutta voidaan löytää järkevä turvan taso kuhunkin tilanteeseen.

On syytä miettiä, miten vakavia asioita seuraa, jos tietojärjestelmä tai sen jokin osa lakkaa toimimasta tai se joutuu rikollisen käsiin. Miten olennaisia, korvaamattomia tietoja voi tuhoutua tai tulla väärinkäytetyiksi tai väärennetyiksi? Mihin järjestelmästä voi päästä ja mitä siellä voi tehdä? Voiko joku esimerkiksi sitä kautta esiintyä jossakin muussa järjestelmässä toisena ja tehdä tilauksia ja tilisiirtoja, antaa määräyksiä tms.? Riskien arvioinnin perusteella voidaan sitten järkevästi arvioida, millaiset turvatoimet ovat tarpeen. Jos tietokonetta käytetään vain siihen, että kirjailija kirjoittaa sillä romaania, niin keskeisintä on taata, että käsikirjoituksesta on kunnolliset varmuuskopiot. Jos taas "henkilökohtainen" tietokone on yrityksen maksuliikennettä hoitavan työntekijän työväline, on ennen muuta estettävä se, että asiattomat pääsevät maksuliikennejärjestelmään.

Turva-asiantuntijan ja tavallisen käyttäjän vuorovaikutus

Niitä asioita, joissa tietoturva on äärimmäisen tärkeä, hoitavat toivottavasti kovan luokan asiantuntijat. Mutta tämän lisäksi tarvitaan tavallisten käyttäjien myötävaikutusta. Tämä tarkoittaa muun muassa asiantuntijoiden antamien toimintaohjeiden noudattamista, ja ohjeiden ymmärtäminen puolestaan voi vaatia perustietämystä tietoturvasta. Hyvin toimivassa isossa yrityksessä ei esimerkiksi jätetä tiedostojen varmuuskopiointia jokaisen käyttäjän itse tehtäväksi, mutta jokaisen on kyllä osattava tallentaa tärkeät tiedostonsa sellaisiin paikkoihin, että ne tulevat keskitetyn varmuuskopioinnin piiriin.

Turva-asiantuntijoiden on tärkeää saada ongelmat tietoonsa mahdollisimman nopeasti. Siksikin tavalliset käyttäjät tarvitsevat yleistietoa turvaongelmista, jotta he eivät esimerkiksi luokittelisi kaikenlaisia laitteiden ja ohjelmien käytön arkisia pulmia "viruksiksi" mutta toisaalta tunnistaisivat epäilyttävät tilanteet, joista on syytä ilmoittaa asiantuntijalle.

Kotikonekin voi olla astinlauta isoille tietomurroille

Tietoturvassa on myös kyse kokonaisuudesta, jossa yhden osan turvattomuus voi heijastua laajalle. Vaikka kotikone olisikin enimmäkseen pelikoneena, sillä saatetaan ottaa yhteys työpaikan tietojärjestelmään, ja jos tietoturva ei ole kunnossa, luodaan silloin aukko firman turvamuuriin.

Lisäksi verkon kautta saatetaan tunkeutua kotikoneeseen ja käyttää sitä monenlaisiin asioihin,

apuvälineenä tietorikollisuuteen. Tunkeutujat erittäin yleisesti pyrkivät peittämään jälkensä sillä, että eivät yritä tietomurtoa suoraan omalta koneeltaan vaan hyvinkin pitkien ketjujen kautta.

Turvan minimitaso on kaikille tarpeen

Vaikka tietoturvan tarve ja tavoiteltava turvataso vaihtelevatkin suuresti, käytännössä kaikki tietokoneet ja tietojärjestelmät on syytä suojata ja varmistaa *jollakin* tapaa. Tämän moni oppii katkerasti liian myöhään, kun tietokoneen kovalevy lakkaa toimimasta eikä varmuuskopioita ole. Uuden kovalevyn saa kaupasta, lähes valmista väitöskirjaa tai kymmenen vuoden aikana koottua reseptikokoelmaa ei.

Tietoturvan minimitason järjestäminen ei vaadi kovin suurta vaivaa. Siellä, missä tarvitaan suurta luotettavuutta, on tehtävä enemmän töitä. Se voi merkitä myös asioiden opiskelun tarvetta ja rahanmenoa. Yksi keskeinen kysymys onkin, miten kukin käyttäjä voisi löytää hänelle sopivan tavoitetason, jolla panostus tietoturvaan on järkevässä suhteessa saavutettavaan hyötyyn. Tämä opas pyrkii auttamaan tässäkin, ja siksi eri kohdissa kuvaillaan, keille mitkäkin turvajärjestelyt ovat tarpeellisia.

Kaikkea tietoturvaa ei voi ostaa

Monet yritykset, laitokset ja yhteisöt käyttävät merkittävästi rahaa ostaakseen palveluita, ohjelmia ja laitteita, joilla parannetaan tietoturvaa. On myös saatavilla monipuolisia tietoturvapaketteja.

Niin hyödyllistä kuin tietoturvan ostaminen usein onkin, ei kannata tuudittautua siihen uskoon, että kaikki on sillä hoidettu. Jokaisessa organisaatiossa tarvitaan myös omaa tietoisuutta ja valmiuksia. Kuten tässä oppaassa kuvataan, suuri osa tietoturvaan kohdistuvista uhkista toimii **ihmisten kautta**. Tekniset turvatoimet eivät auta, jos ulkopuolinen saa puhelinsoitolla tietoonsa salasanoja. Sellaista todella tapahtuu.

Selvitä tiedon ja tiedoston alkuperä ennen käyttöä

Tässä osassa:

- Liitetiedostot: kyseenalaisia.
- "Tiedon" levittäminen tai uskominen voi olla vaarallista.
- Tunnista roskaposti (spämmi).
- Älä ole sinisilmäinen: murtautujat ovat kivoja kavereita.
- Netistä löytyy ja levykkeelläkin saa - myös haittaohjelmia.
- Ohjelma on muutakin, kuin miltä näyttää.
- Selainten ongelmia.
- Tietojen lähetys lomakkeelta: avoimina vai salattuina?
- Kenen sivulla *oikeasti* olet? Kenen kanssa olet *oikeasti* tekemisissä?

Liitetiedostot: kyseenalaisia

Kiva tarjous jostain? Seis!

Älä koskaan avaa tuntemattomasta lähteestä tullutta liitetiedostoa. Älä ainakaan napsauttamalla (klikkaamalla), koska siitä voi seurata mitä vain. Kenties se on pelkkä ns. roskaposti, mutta se voi olla paljon pahempaakin. Usein mukaan on piilotettu tuho-ohjelma, ja viestin näennäinen sisältö on vain silmänlumetta.

Jos olet liittynyt jollekin ns. jakelulistalle (postituslistalle) Internetissä, on kaikkea siltä tulevaa syytä pitää tuntemattomasta lähteestä tulevana. Vaikka viesti tulee tutun listan kautta, varsinainen lähettäjä voi yleensä olla kuka vain.

Jos epäilet, että liitetiedosto, jonka lähettäjää et tunne, saattaisi sisältää jotain hyödyllistä, avaa se varovaisesti, vain sellaisilla ohjelmilla, jotka ainoastaan yrittävät näyttää sisältöä. Esimerkiksi MS Word *ei* ole tässä suhteessa turvallinen, jos makrojen suoritus on siinä sallittu. Liitetiedoston tyypin tunnistamisesta yms. kertoo dokumentti *"Sain tiedoston, jonka nimi loppuu `.xyz`; mitähän se sisältää?"*.
<http://www.cs.tut.fi/~jkorpela/softa/ext.html>

Mikä on käytäntö siellä, missä toimit?

Sähköpostin liitetiedostoihin suhtaudutaan eri tahoilla eri tavoin. Liitetiedostot voivat olla (ja yleensä ovat) muuta kuin pelkkää "raakaa" tekstiä, esimerkiksi kuvia, tekstinkäsittelyohjelmalla muotoiltuja tekstejä tai PowerPoint-esityksiä.

Monessa yrityksessä ne ovat olennainen ja hyvin tarpeelliseksi koettu viestinnän muoto. Toisaalla taas niihin saatetaan suhtautua hyvinkin kielteisesti muun muassa tietoturvariskien takia. Jossakin taas on omaksuttu välittävä kanta: liitetiedostoja voidaan lähettää, mutta ei esimerkiksi MS Word -muodossa vaan RTF-muodossa, jossa ei käytännössä ole ollut tietoturvaongelmia enempää kuin pelkässä tekstissä. Selvitä itsellesi, miten niihin suhtaudutaan omassa toimintaympäristössäsi.

On paras olettaa, että liitetiedostoja ei haluta

Olipa oman organisaation sisäinen liitetiedostopolitiikka mikä hyvänsä, organisaation ulkopuolelle ei ole syytä lähettää liitetiedostoja, ellei ole varmistettu, että vastaanottaja voi ja haluaa käsitellä niitä. Yleensä pitää olla jokin erityinen syy, jonka takia lähettäisi liiteaineistoa. Esimerkiksi tekstinkäsittelyohjelmalla tehdyn lyhyen asiakirjan voi hyvin tallentaa pelkkänä tekstinä tiedostoon (toiminnolla *Save as plain text* tms.) ja sieltä sitten leikata ja liimata tai muuten sisällyttää itse sähköpostiviestiin. Tällöin viesti on varmasti luettavissa siitä riippumatta, millaisia laitteita ja ohjelmia vastaanottaja käyttää.

On useita muitakin syitä, joiden takia kannattaa suosia pelkkää tekstiä sähköpostissa: siitä voi lainata tarvittavan osan vastausviestiin; se vie vähemmän tilaa ja siirtyy nopeammin, mikä on tärkeää, jos viesti kääntyy matkapuhelimeen; eikä se herätä turhia epäilyjä siitä, että viestissä voi olla viruksia.

Luonnollisestikin jos vastaanottaja on *pyytänyt* aineiston jossakin määrätyssä muodossa, pyyntöä on syytä noudattaa mahdollisuuksien mukaan. Tällöin on tärkeää, että omassa koneessa on käytössä kunnollinen viruksentorjunta.

Mitä liitteen mukana lähteekään?

Liitetiedostoja lähetettäessä on syytä ottaa huomioon, että esimerkiksi Word saattaa tallentaa tiedostoon sisäisesti muutakin, kuin miltä näyttää, myös tallennettaessa RTF-muotoon. On aika ikävää, jos esimerkiksi tarjouksen sisältävästä dokumentista vastaanottaja pystyy saamaan selville, miten tarjousta on luonnosvaiheessa muuteltu! Seuraava on ote Wordin käyttöohjeesta (suojaus-hakusanan kautta löytyvästä kohdasta, jossa on käsitelty myös muita tietoturvaongelmia ja -ratkaisuja):

> **Poistetut tiedot näkyvät yhä asiakirjassa**
>
> Jos olet tallentanut asiakirjan **Salli pikatallennus** -vaihtoehdolla ja sen jälkeen avannut sen tekstitiedostona, asiakirjassa voi olla aiemmin poistettuja tietoja. Tämä johtuu siitä, että pikatallennus lisää asiakirjaan tehdyt muutokset asiakirjan loppuun sen sijaan, että se tekisi itse asiakirjaan muutokset mukaan lukien poistamiset.
>
> Poista poistetut tiedot pysyvästi sulkemalla tekstitiedosto ja avaamalla asiakirja tavallisena Word-

asiakirjana. Valitse **Tiedosto Tallenna nimellä Tallenna.** Voit myös poistaa pikatallennuksen käytöstä valitsemalla **Työkalut Asetukset** ja poistamalla **Tallenna**-välilehden **Salli pikatallennus** -valintaruudun valinnan.

"Tiedon" levittäminen tai uskominen voi olla vaarallista

Internet on tehokkaimpia tapoja levittää valheita ja huijausta. Tekniikan lisäksi tähän vaikuttaa se, että ihmiset ovat hyvin halukkaita "levittämään tietoa", kun se on heille vaivatonta ja kun kyse on näennäisesti tärkeästä ja hyvästä asiasta, esimerkiksi ihmisten suojelemisesta tietokoneviruksilta.

Kiinnostavaa, liikuttavaa - mutta onko se myös totta?

Ihmiset voidaan aika helposti saada uskomaan erittäin vakuuttavannäköiseen mutta täysin perättömään "uutiseen" ja levittämään sitä. Sama koskee vetoomuksia toimia jonkin hyvän asian puolesta, etenkin, jos siinä on mukana ihmisten sääliin vetoaminen.

Ota huomioon, että esim. sähköpostin lähettäjätietojen väärentäminen on teknisesti melko helppoa. Erityisesti lähettäjäkenttään (`From`-kenttään) voi lähettäjä useimmissa ohjelmissa kirjoittaa ihan mitä haluaa. Artikkeli, joka näyttää tulevan kansainvälisesti tunnetulta tiedemieheltä tai valtiolliselta organisaatiolta, on voinut tulla ihan mistä hyvänsä.

Ei siis pidä ruveta levittämään "tietoa" vain siksi, että se kuulostaa tärkeältä tai muuten vaikuttavalta. On olemassa valtava määrä sellaisia "tietoja", joita levitetään Internetissä laajamittaisesti, jopa samaa juttua vuodesta toiseen, vaikka niissä ei ole mitään perää tai alkuperäinen asia on vääristynyt täysin. Katso esim. mittavaa kokoelmaa *Urban Legends Archive*. `<http://www.urbanlegends.com/>`

Sano "ei" ketjukirjeille

Ketjukirjeitä ei pidä lähettää, ei varsinkaan, jos niissä uhkaillaan kauheuksilla, joita tapahtuu, jos "katkaisee ketjun". Suuri osa ketjukirjeistä on silkkaa huijausyritystä: jos tarpeeksi monet ihmiset uskovat, että rahaa tulee tyhjästä, niin *joku*, nimittäin ketjun alullepanija, saa rahaa. Sellaiset ketjukirjeet ovat lainvastaisiakin. Jos kyse on pelkästä viestien lähettämisestä eteenpäin, vahinko syntyy toisaalta turhasta verkkoliikenteestä, toisaalta viestien mahdollisesta sisällöstä, esimerkiksi perättömistä tiedoista.

Huijausta ja viestinnän häirintää

Enimmäkseen väärän informaation levittäminen vain tuhlaa aikaa ja muita voimavaroja. Mutta kun kyse on monien ihmisten ajasta, sillä on merkitystä. Lisäksi mukana voi olla kehotuksia toimia tavalla, joka tosiasiassa merkitsee tietoturvariskiä tai muuta vaaraa, esimerkiksi rahojen huijaamista.

Kuluttajaviraston sivuilla on tietoa myös Internet-kaupasta, mm. lomake, jolla voi arvioida kaupan luotettavuutta. `<http://www.kuluttajavirasto.fi>`

Kaikki väärä informaatio on haitaksi sen takia, että mitä suurempi informaation virta on, sitä huonommin oikea ja tärkeä tieto menee perille. Erityisen haitallista on sellainen väärä tieto, joka muistuttaa oikeaa tai näyttää erityisen tärkeältä.

Tunnista roskaposti (spämmi)

Tuntemattomalta lähettäjältä tulevat sähköpostiviestit ovat erittäin usein ns. roskapostia (spämmiä, *spam*) eli aineistoa (useimmiten mainontaa), joka on lähetetty massajakeluna esimerkiksi miljoonalle Internetin käyttäjälle. Hyvin usein asiaan liittyy lisäksi jonkinasteista huijausta.

Roskapostiviestissä on usein mukana linkki, jota seuraamalla käyttäjä tulee kertoneeksi roskapostin lähettäjälle, että osoite toimii. Tästä taas seuraa lisää roskapostia. Pelkkä viestissä olevan kuvan latautuminen voi aiheuttaa saman.

Roskapostin mukana on usein liitetiedosto, joka sisältää viruksen. Tällöin onkin kyse yleensä houkuttelevaksi tarjoukseksi naamioidusta viruksesta.

Roskapostiksi tunnistamisessa voi auttaa *Ryhmän sfnet.viestinta.roskapostit epävirallinen VUKK (FAQ)*. `<http://www.iki.fi/kaip/spam/vukk.html>`

Älä ainakaan vastaa

Älä reagoi roskapostiin, paitsi mahdollisesti tekemällä siitä valituksia asianomaisia kanavia myöten. *Älä* vastaa viestin lähettäjälle äläkä osoitteeseen, jonka väitetään olevan sitä varten, että pääset pois jakelulistalta. Todennäköisesti sellainen reagointi saisi aikaan vain sen, että pääset uusille jakelulistoille ja osoitettasi voidaan myydä "taatusti toimivien osoitteiden" joukossa.

Roskaposti aiheuttaa suuren määränsä takia ongelmia järjestelmien toimivuudelle. Tavallisen käyttäjän kannalta se on pikemminkin inhottava kiusa kuin varsinainen tietoturvauhka; toki voi menettää rahojaan jonkin verran, jos uskoo roskapostien sisältöön.

"Roskapostisuojaus": ratkaisu vai lisää ongelmia?

Roskapostin lähettäjät käyttävät laajoja osoitelistoja, joita on koottu muun muassa verkkosivuilta ja verkon keskusteluryhmistä. Tämän takia ehdotetaan usein, että roskapostia vastaan pitäisi suojautua sillä, että sähköpostiosoitteet jätetään pois tai niihin lisätään jokin merkkijono, joka lähettäjän pitää pois.

Kuitenkin sähköpostiosoitteiden sotkeminen aiheuttaa useita ongelmia. Jos osoitteen `mmx@foo.example` sotkee muotoon `mmx@fooPOISTA.example`, niin ehkä suomalainen päättelee, mitä tarkoitetaan. Mutta entäs sitten, kun viesti tulikin lähetettyä japanilaiselle liikekumppanille? Lisäksi vastaamisen tahallinen vaikeuttaminen voidaan kokea hyvin epäkohteliaaksi.

Yleensä on helppo oppia tunnistamaan selvä roskaposti (MAKE MONEY FAST!!!) roskapostiksi jo otsikon perusteella, itse viestiä edes lukematta. Jos roskapostin määrä käy niin suureksi, että sen hävittäminen aiheuttaa liikaa työtä, tutustu jäljempänä kerrottaviin keinoihin suodattaa roskaposteja pois automaattisesti.

Älä ole sinisilmäinen: murtautujat ovat kivoja kavereita

Ei ole terveellistä epäillä kaikkia ihmisiä kaiken aikaa. Mutta jos joku ehdottaa tai tekee jotain, joka olisi tietoturvan kannalta vaarallista, on syytä ruveta epäluuloiseksi. Olipa hän miten miellyttävä tai arvovaltainen tahansa.

Pehmeä tekniikka toimii usein hyvin

Tietoturvaan liittyy niin paljon teknisiä ja vaikeita asioita, että kovin helposti unohtuu, että useinkaan tietomurtoon ei tarvita mitään "kovaa" tekniikkaa, vaan "pehmeä" tekniikka, pahaa-aavistamattomien ihmisten luottamuksen hyväksikäyttö, riittää mainiosti ja usein sopii paremmin murtautujan tarkoituksiin.

Suomalaisten sanotaan olevan jöröjä ja kömpelöitä, ja luultavasti me olemmekin suhteellisen tottumattomia sulavaan käytökseen. Sellaista kohdatessamme saatamme ihastua siihen tai ylipäänsä

vain kiinnittää huomiomme siihen niin, että huomaamattamme annamme tietoja tai muuta apua ihmiselle, jonka todellisena tavoitteena on jonkinlainen tietomurto.

Kukahan oikeasti on luurin päässä?

Usein tietoja urkitaan puhelimessa. Silloin tietomurtoa yrittävä ei paljasta ulkonäköään, jolloin hän jää tosiasiassa tuntemattomaksi mutta voi esittäytyä vaikkapa konsernin tietoturvapäälliköksi tai suurasiakkaan edustajaksi. *Sähköpostin* käyttöä yritetään myös samoista syistä, mutta se ei ole samalla tavalla vaikuttavaa kuin esimerkiksi asioiden kysyminen puhelimessa, jolloin on sosiaalisista syistä vaikeampi jättää vastaamatta tai ottaa miettimisaikaa. *Henkilökohtainen käynti* vaikuttaa tehokkaimmin. Ja vaikka siihen sisältyy suuri kiinnijäämisen riski, niin taitava tietomurron yrittäjä on jo suunnitellut valmiiksi, mitä tehdä, kun se uhkaa.

Ovelia menettelytapoja

Seuraavassa on joitakin esimerkinomaisia *havaintoja menettelytavoista*:

1. Tunkeutuja voi tekeytyä peruskäyttäjäksi, jolla on hankaluuksia ja joka pyytää apua muilta. Ehkä hän kääntyy suoraan järjestelmän ylläpitäjien puoleen, koska heillä tietysti on eniten hänelle hyödyllistä tietoa. Mutta koska he saattavat olla varuillaan, tunkeutuja voi kääntyä myös muiden peruskäyttäjien puoleen; heidänkin tietonsa (kuten omat salasanat) ovat tunkeutujille hyödyllisempiä kuin he itse useinkaan ymmärtävät. Hän kenties kertoo, että on hukannut salasanansa tai ei muuten pääse sisään järjestelmään ja tarvitsee pääsyä järjestelmään *kiireellisesti*, esittäen jonkin vetoavan syyn siihen.
2. Tunkeutuja saattaa kertoa nimekseen tai asemakseen jotain, joka kertoo kättelyssä, että hän on Tärkeä Henkilö. Peruskäyttäjä tai ylläpitäjä ei ehkä *uskalla* sanoa "ei", kun pääjohtajan tarvitsee heti päästä lukemaan ratkaisevan tärkeä viesti.
3. Tunkeutuja ehkä tarvitsee tietoja, jotka järjestelmän laillisista käyttäjistä tuntuvat tietoturvan kannalta merkityksettömiltä. Monenlaiset käytön järjestelyihin, järjestelmän pieniin yksityiskohtiin yms. liittyvät seikat voivat olla tarpeen tunkeutujalle; koska hän ei ole koskaan käyttänyt järjestelmää ja aikoo esim. tunkeutua verkon kautta, hän joutuu onkimaan tietoja. Niinpä hän esiintyy eksyksissä olevana käyttäjänä; useimmat ihmiset ovat silloin valmiita auttamaan "tyttöä pulassa".
4. Toisaalta tunkeutuja voi *tarjota* apua käyttäjälle saavuttaakseen hänen luottamuksensa. Käyttäjä, joka on turhautunut kohtaamiinsa ongelmiin ja helpdeskin avuttomuuteen, on enemmän kuin onnellinen, kun joku tulee tarjoamaan apua, ja kenties riemusta kirkuen kertoo salasanansa. Etenkin kun toinen vielä esiintyy teknisenä asiantuntijana. Ja sellaisillehan toki on ihan sopivaa paljastaa salaisuuksiakin, eikö totta?
5. Tunkeutuja voi esiintyä myös *ulkopuolisena* asiantuntijana, esimerkiksi tietokoneen korjaajana, verkkoyhteyksien tarkastajana tai ohjelman asentajana. Peruskäyttäjän ei pitäisi päästää sellaista tekemään mitään, paitsi jos on itse tilannut työn tai saanut oman organisaation sisältä asiasta tiedon.
6. Tunkeutuja ehkä kehottaa käyttäjää antamaan komentoja, käynnistämään ohjelmia yms., perusteluna se, että näin käyttäjä antaa apuaan tai selviää omasta pulmatilanteestaan. Kun kehotus esitetään teknisenä kuvauksena, tyyliin "kirjoita `rmdir -r ~`", käyttäjä ei ehkä lainkaan ymmärrä, mitä on tekemässä, eikä osaa epäillä mitään. (Tyypillisessä Unix-järjestelmässä kyseinen komento hävittää käyttäjän kaikki hakemistot tiedostoineen. Tyypillinen Unix-käyttäjä ei tiedä tätä.)

Oikeat ylläpitäjät eivät tarvitse eivätkä kysy salasanaasi, sillä heillä on tekniset keinot tehdä tarvittavat asiat muutenkin.

Netistä löytyy ja levykkeelläkin saa - myös haittaohjelmia

Internetissä on vapaasti saatavilla valtava määrä tekstejä, kuvia, tietokoneohjelmia, videoesityksiä ja paljon muuta. Niitä saa myös levykkeillä ja muilla tietovälineillä tutuilta ja tuntemattomilta, usein kylkiäisinä tai ilmaiseksi. Osa sellaisesta aineistosta on jopa *laillisesti* saatavilla, mutta hyvin iso osa on laittomia ns. piraattikopioita.

Laillinen ohjelma on turvallisempi

Tekijänoikeuskysymykset eivät kuulu tämä oppaan aihepiiriin, mutta yksi huomautus on syytä tehdä: piraattikopioiden käyttö on epäsuora turvariski, koska niiden käyttäjä ei uskalla pyytää apua ongelmiinsa, peläten jäävänsä kiinni laittomuudesta. Lisäksi piraattikopioissa on usein viruksia.

Ns. shareware-ohjelmia käytetään usein maksamatta niitä pienehköjä maksuja, joita pyydetään. Tämä ei välttämättä ole laitonta vaan on ehkä mahdollista esim. tulkitsemalla "kokeilukäytön" käsitettä sopivan väljästi. Mutta tietoturvankin kannalta on hyvä huomata, että maksu usein antaa paremmat mahdollisuudet saada ohjelmaan päivityksiä, ohjelman täydellinen versio (jossa voi olla turvallisuuttakin parantavia lisäpiirteitä), tuotetukea ym. Eri asia sitten on, että shareware-ohjelmien joukko on varsin kirjava, ja mukana on paljon tekeleitä, joissa ei ole tietoturvaa ajateltukaan.

Tekniikoita: Web, FTP

Aineistoja haetaan Internetistä nykyisin enimmäkseen Webin (WWW) kautta, mutta vanhempi "imuroinnin" tapa FTP on myös käytössä. Tietoturvan kannalta molemmat ovat suunnilleen yhtä ongelmallisia teknisesti, mutta Webin käytön *helppous* tekee siitä käytännössä vaarallisemman.

Lisäksi kun Web-selaimella seuraa linkkiä imuroitavaan tiedostoon, niin tyypillinen selain oletusarvoisesti yrittää imuroinnin jälkeen automaattisesti tehdä tiedostolle jotain. Jos se on esimerkiksi Word-dokumentti, selain saattaa tunnistaa tämän ja automaattisesti käynnistää Word-ohjelman näyttämään dokumentin. Tähän taas sisältyy useita riskejä.

Ota talteen tieto alkuperästä

Suhtaudu imuroimiisi tiedostoihin varovaisesti, kuten sähköpostitse tulleisiin liitteisiinkin. Vaikka luulet tietäväsi, mistä imuroit, se voi olla harhaa. Joka tapauksessa huolehdi siitä, että jonnekin tulee talteen tieto siitä, mistä osoitteesta olet imuroinut. Usein sellainen tieto on mukana "paketissa", mutta tarkista asia.

Nimi on voitu valita harhaanjohtavaksi, samoin tyyppi

Älä luota sokeasti tiedoston nimeen äläkä tyyppimerkintään, älä myöskään Web-sivulla oleviin tietoihin tiedostosta. On aika tavallinen mutta tehokas kikka nimetä haittaohjelma niin, että se nimensä perusteella näyttää tekstitiedostolta, kuvalta tms. taikka joltakin yleisesti tunnetulta hyöty- tai hupiohjelmalta.

Windows "piilottaa" sellaiset tiedostonnimien päätteet, jotka kuuluvat Windowsin tunnistamien päätteiden listaan. Tätä käytettiin ensi kerran hyväksi laajalle levinneessä LoveLetter-viruksessa, jossa sähköpostin liitetiedostona tuli tiedosto nimeltä `LOVE-LETTER-FOR-YOU.TXT.vbs`, jonka Windows näyttää muodossa `LOVE-LETTER-FOR-YOU.TXT`, jolloin se näyttää tekstitiedostolta vaikka on tosiasiassa Visual Basic -ohjelmakoodia. Kyseinen Windowsin piirre voidaan kyllä kytkeä pois toiminnasta, ja monissa järjestelmissä niin on valmiiksi tehtykin, ja se voi hiukan auttaa. Esimerkiksi suomenkielisessä Windows 98:ssa menettely on seuraava: kaksoisnapsauta "Oma tietokone" -kuvaketta, sitten levyaseman (C:) kuvaketta, valitse avautuvan ikkunan Näytä-valikosta kohta "Kansion asetukset...", sitten Näkymä-vaihtoehto ja napsauta kohdan "Piilota tunnistettujen tiedostotyyppien tunnisteet" edessä olevaa ruutua, jos siinä ruksi, ottaaksesi kyseisen asetuksen pois.

Ohjelma on muutakin, kuin miltä näyttää

Ohjelmalla on valta koneessa

Ohjelman käynnistäminen tietokoneessa antaa koneen *ohjelman hallintaan* enemmän tai vähemmän kokonaan. Ilmaisu "enemmän tai vähemmän" viittaa siihen, että tietokonejärjestelmissä on suojauksia, joiden tarkoitus on estää ohjelmaa sotkemasta asioita kovin pahasti. Mutta suojaukset ovat aina puutteellisia, ja koko tietokoneen perusideaan kuuluu, että se toimii siihen kulloinkin latautuneen ohjelman mukaisesti, sen kontrollissa.

Tästä seuraa aika pelottavia näkymiä, etenkin kun otetaan huomioon, että ohjelmat ovat tulleet aiempaa paljon suuremmiksi ja monimutkaisemmiksi. Tähän sisältyy paljon mahdollisuuksia mutta myös vaaroja. Mitä isompi kokonaisuus, sitä helpommin käy niin, että jonnekin jää *ohjelmointivirhe*, etenkin, kun virheitä usein syntyy osien vuorovaikutuksesta, jota ei osattu ennakoida, kun kukin ohjelmoija teki omaa osuuttaan.

Ohjelmissa on aina virheitä

Lähes kaikissa ohjelmissa, joilla voi tehdä jotain hyödyllistä tai hauskaa, on virheitä, "bugeja". Jos ohjelma on hyvin tehty ja ylläpidetty, virheet eivät ole kovin vakavia eivätkä ilmene useimmissa käyttötavoissa, koska ohjelmaa on eri tavoin testattu paljon. Ohjelman alkuperän tunteminen auttaa tällaisten asioiden arvioimisessa, etenkin, kun tieto alkuperästä sisältää yleensä tiedon ohjelman "tuoreudesta". Jos ohjelman dokumentaatio kertoo, että ohjelmaa on viimeksi päivitetty vuonna 1996, niin tämä harvoin johtuu siitä, ettei päivittämisen *tarvetta* olisi ollut.

Uusin versio voi olla liiankin uusi

Toisaalta hyvin uudet ohjelmaversiot eivät nekään ole yleensä kovin luotettavia. Tavallisesti kestää muutamia kuukausia, ennen kuin uudesta versiosta on saatu korjatuksi julkaisemisen jälkeen käytössä havaitut virheet ja on saatu levitykseen korjattuja versioita.

Lisäksi on syytä erityisesti varoittaa beetaversioista (beta version), jotka voivat kulkea myös nimellä *evaluation version*: ne ovat kokeiluja, jotka annetaan innokkaiden vapaaehtoisten testattaviksi, yleensä ilman *minkäänlaista* toimivuustakuuta edes etäisesti muistuttavaa lupausta. Yleensä beetaversioita kannattaa kokeilla vain niiden, jotka haluavat enemmänkin antaa panoksensa ohjelman kehitystyöhön kuin käyttää ohjelmaa johonkin käytännölliseen. Ison ohjelmistotalon beetaversio tosin *saattaa* jo olla kohtalaisen toimiva ja sisäisen testauksen läpikäynyt.

Tahallistakin tuhoa

Lisäksi ohjelmiin voidaan tahallisesti piilottaa piirteitä, jotka aiheuttavat tuhoa tai ainakin harmeja. Sitä, miksi niin tehdään, pohditaan jäljempänä. Tosiasia joka tapauksessa on, että sellaista tehdään.

Tässä ei tarkemmin paneuduta siihen, mitä eri haitta- tai haittaohjelmien tyyppejä kuten "viruksia", "matoja", "troijalaisia" jne. on olemassa. Aihetta kuvataan esimerkiksi TKK:n virusoppaan `<http://www.hut.fi/atk/oppaat/virukset/>` kohdassa *Terminologiaa*. Olennaista on, että niitä on monenlaisia eivätkä ne usein ole mitenkään helposti tunnistettavissa haitallisiksi saati lajiltaan luokiteltavissa. Esimerkiksi viruksentorjuntaohjelmat tehoavat vain osaan (joskin merkittävään osaan) haittaohjelmista. On tärkeää käyttää hyvän viruksentorjuntaohjelman tuoreinta versiota säännöllisesti, mutta ei siis pidä tuudittautua ajattelemaan, että se riittäisi suojaamaan kaikelta pahalta.

Pienikin ohjelma voi olla salatie verkkoon

Kun suoritat (ajat) tietokoneessasi jotain ohjelmaa, se muun ohessa ehkä käyttää verkkoa tietämättäsi. Kun tietokone on yhteydessä verkkoon, mikä tahansa ohjelma voi käyttää verkkoa ja voi kertoa tai olla kertomatta siitä sinulle. Ohjelma voidaan tehdä vaikkapa sellaiseksi, että kun käynnistät sen, pääset pelaamaan hauskaa räiskintäpeliä, kokoamaan ruokareseptejä tai katselemaan luontokuvia - mutta todellisuudessa ohjelma sen *lisäksi* esimerkiksi lähettää kaikki tiedostosi, sopivassa tahdissa huomaamattomasti yksi kerrallaan, Internetin kautta jollekulle.

Tai jotain pahempaa. Kiinnostavaan ohjelmaan on ehkä piilotettu ns. takaportti (backdoor) eli pieni ohjelmakoodin pätkä, jonka kautta murtautuja pääsee käyttämään konetta verkon kautta ja voi siten myös käyttää sitä tunkeutuakseen muihin koneisiin.

Nämä ovat todellisia uhkia, mutta on myös todellisia keinoja suojautua niitä vastaan. Asian tärkeys lisääntyy sitä mukaan, kuin kiinteät Internet-yhteydet yleistyvät.

Kehen luotat?

Useimmat tietokoneen käyttäjät eivät tunne ohjelmointia, joten he eivät yksinkertaisen ohjelman koodistakaan osaisi päätellä, mitä se todella tekee, eikä koodia useinkaan ole edes saatavilla ns. lähdekoodina. Joudumme siis käytännössä *luottamaan muiden antamiin tietoihin* siitä, mitä ohjelmat tekevät. Sitä tärkeämpää on katsoa, kehen luottaa missäkin.

Suhteellisuudentaju on syytä säilyttää. Kotikoneeseen voi asentaa ohjelmia melko huolettomasti esimerkiksi luotettavien tietokonelehtien kylkiäisinä tulleilta rompuilta taikka tunnetusta Tucows-jakelusta. `<http://www.tucows.fi/>` Töissä on syytä olla varovaisempi.

Saako koneeseesi edes asentaa ohjelmia?

Monet organisaatiot ovat kokonaan kieltäneet ohjelmien imuroinnin ja ajamisen Internetistä. Se haluttaisiin ehkä *estääkin*, mutta täydellinen estäminen voi olla käytännössä mahdotonta. Jotkin organisaatiot sallivat vain ATK-asiantuntijoiden (ylläpitäjien) asentaa ohjelmia; syynä voi olla paitsi turvallisuus myös se, että sellainen ratkaisu helpottaa ylläpitotyötä. Jos sellaisia ohjeita on annettu, noudata niitä tarkasti.

Selainten ongelmia

Web-selaimet saattavat ladata tiedostoja enemmän tai vähemmän "ohimennen". Et ehkä ole liikkeellä ladataksesi tiedostoja, mutta jotain silti latautuu. Selain ehkä omalla tavallaan kysyy sinulta lupaa, mutta et välttämättä huomaa, mitä on tapahtumassa.

Mitä annat selaimen kytkeä itseensä?

Tyypillistä on, että kun ensi kertaa menet sivulle, jolla on jotain erityistä tekniikkaa käyttävä kehitelmä, esimerkiksi animaatio, selain hakee ja asentaa itseensä lisäosan, "valmisosan" (*plug-in*) sen toteuttamiseksi. Kun siis Web-sivulla oleva teksti tai selaimesi ehdottaa jonkin "valmisosan" lataamista ja asentamista voidaksesi katsoa tai käyttää sivun sisällön jotakin osaa, on hyvä kysyä: Mikä on tämä "valmisosa"? Mitä takeita sen turvallisuudesta on? Mitä erikoisemmasta tekniikasta on kyse, sitä varovaisemmin on suhtauduttava. Voi olla hyvä kysyä asiantuntijalta neuvoa, mieluiten turva-asioiden tuntijalta.

Esimerkkeinä todennäköisesti harmittomista ja usein hyödyllisistäkin lisäosista voidaan mainita Macromedia Flash, joka toteuttaa erilaisia Web-sivun eloisuutta lisääviä asioita, ja RealPlayer, joka esittää määrätynlaisia ääni- ja videoesityksiä. Jos käyt erikielisillä Web-sivuilla ja käytät Windows-konetta, selaimesi saattaa hyvinkin joskus ilmoittaa, että järjestelmääsi on asennettava

"Yleiseurooppalainen näyttötuki". Tämä on aivan asiallista. Jos käytät modeemia, toimenpide voi kestää jonkin aikaa, koska asennustoiminto joutuu todennäköisesti lataamaan tuen Internetistä.

Välimuisti (cache) voi juoruta

Toisen tietoturvaongelman muodostavat selainten välimuistit (caches): kun käyt eri Web-sivuilla, selain tallentaa sivuja (ja niiden osoitteita) väliaikaisesti tietokoneen keskusmuistiin tai levylle tai molempiin. Ja väliaikaisuus voi olla aika pitkääkin, esimerkiksi parikymmentä päivää. Tämä usein olennaisesti nopeuttaa käyttöä silloin, kun käyttäjä siirtyilee sivulta toiselle ja esim. kulkee paljon jonkin hakemistosivun kautta tai palaa joillekin tärkeille sivuille usein. Mutta siinä on myös riskinsä.

Se merkitsee, että seuraava käyttäjä voi yleensä vielä päivienkin kuluttua katsoa selaimen sivuhistoriasta, millä sivuilla on käyty. Tämä on olennaista, jos sivu on esimerkiksi pankin järjestelmän tulostama tiliote. Tosin hyvin tehty pankkisovellus tekee kaikkensa estääkseen sellaisen sivun sisällön automaattisen tallentumisen välimuistiin.

Etenkin **yhteiskäyttöisten** (esim. mikroluokkien ja kirjastojen) tietokoneiden käytössä kannattaa tyhjentää välimuistit, jos sivuhistoriassa on suhteellisen arkaluonteista tietoa. Huomaa, että tämä voi vaatia välimuistin tyhjentämistä sekä keskusmuistista (memory cache) että kovalevyltä (disk cache); se ei ole kovin vaikeaa, mutta se pitää opetella kullekin selaimelle erikseen.

Selain ajamassa ohjelmia

Web-selaimet voivat myös automaattisesti suorittaa sivuilla olevia ohjelmia eli skriptejä, esimerkiksi JavaScript-koodia tai Java-sovelmia. Tällainen ohjelmien suorittaminen voidaan estää selaimen asetuksilla, mutta tavallisimmissa selaimissa asetus on alkutilanteessa se, että suoritus on sallittua. Selvitä itsellesi oman organisaatiosi turvapolitiikka tässä suhteessa. Osa kyseisistä ohjelmista on hyödyllisiä tai ainakin hauskoja Webin käytössä, mutta suurin osa on melko turhanpäiväistä tai häiritsevääkin, esimerkiksi uusien ikkunoiden holtiton availu kuvaruudulle. Lisäksi niihin liittyy tietoturvariskejä. Virusten leviäminen perustuu osittain juuri siihen, että skriptit saattavat tehdä asioita, joita niiden ei pitäisi voida tehdä.

Eräs vaihtoehto varsinkin ns. vakavassa käytössä on, että mm. JavaScript-, ActiveX- ja Java-koodin suorittaminen on normaalisti estettynä mutta se voidaan hetkellisesti ottaa käyttöön sivuilla, joilla se on perusteltua ja joita voidaan pitää luotettavina. Tämän tekeminen eräissä tavallisissa selaimissa on selostettu CERT/CC:n ohjeessa *Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites*. `<http://www.cert.org/tech_tips/malicious_code_FAQ.html>`

Tietojen lähetys lomakkeelta: avoimina vai salattuina?

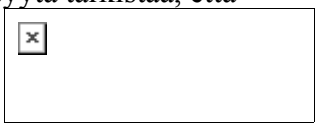
Lomake: yleensä suojaamaton yhteys

Web-sivut sisältävät usein lomakkeita (forms). Kuten sähköpostikin, lomaketiedon lähetys (Web-selaimelta Web-palvelimelle) on lähtökohtaisesti turvatonta, salaamatonta. Tämä koskee myös salasanoja: et itse näe, mitä kirjoitat salasanakenttään, mutta salasana lähtee useinkin muun tiedon mukana salaamattomana verkkoon.

Suojaamaton yhteys on melko vaaraton silloin, kun lomake on esimerkiksi hakulomake, jolla etsitään Web-sivuja tai tietoa jostakin tietokannasta. Mutta jos lomakkeella annetaan henkilötietoja tai tehdään tilauksia, tietojen vuotaminen on todellinen riski. Sen palvelun tarjoaja, jota lomakkeen kautta käytetään, on ehkä luotettava. Mutta lähettämäsi tiedot ovat ulkopuolisten siepattavissa, kun ne kulkevat selaimen ja palvelimen välillä.

Salausta: SSL (`https:`)

Turvattomuuden vähentämiseksi on kehitetty useita mekanismeja, joista merkittävin on nykyisin Secure Sockets Layer (SSL). Sitä käytettäessä tieto kulkee salakirjoitettuna, Useimmat nykyaikaiset selaimet tukevat sitä, mutta se on käytössä vain silloin, kun se on itse sivuilla kytketty toimintaan; merkkinä tästä on, että sivun osoitteen alussa ei ole `http:` vaan `https:`. (Kirjain s johtuu sanasta *secure* 'turvallinen'.) Ainakin käytettäessä Internetiä *maksuliikenteeseen* on syytä tarkistaa, että sellainen tai muu tarpeeksi luotettava suojaus on käytössä! Tyypillinen selain näyttää selainikkunan alapalkissa jonkinlaisen pienen lukon kuvan merkiksi SSL-salauksesta. Kun kursori viedään kuvan päälle, selain yleensä näyttää tiedon siitä, miten vahva salaus on käytössä; luotettavan salauksen miniminä pidetään nykyisin 128-bittistä.



Jos kuitenkin sivu käyttää ns. kehyksiä (frames), niin lukko näkyy hiukan vaihtelevasti silloin, kun osa sivuista tulee suojattuina ja osa ei. Lisäksi lukko sinänsä ei takaa, että lomaketiedot kulkisivat suojatun yhteyden yli.

Kenen sivulla *oikeasti* olet? Kenen kanssa olet *oikeasti* tekemisissä?

Tervetuloa ...:n sivuille! (Tai sitten jonnekin muualle)

On hyvin helppoa tehdä Web-sivusta kopio, joka näyttää aivan alkuperäiseltä mutta jota voi sitten muutella sisällöltään miten haluaa. Sen voi sitten panna Webiin, kenties jopa sentapaiseen osoitteeseen kuin `http://www.suojelupoliisi.org` tai muuten hämäävään osoitteeseen. Oikean osoitteen näkyminen voidaan myös estää eräillä helpoilla tekniikoilla.

Verkkotunnusta `suojelupoliisi.org` ei ainakaan toistaiseksi ole rekisteröity. Mutta erilaisilla .org- ja .com-loppuisilla tunnuksilla on hämätty käyttäjiä paljonkin.

Vaativammilla tekniikoilla voidaan lisäksi usein onnistua osittain sekoittamaan Internetin ns. nimipalvelu (DNS). Tällöin käyttäjä, joka on tottunut vierailemaan vaikkapa jonkin suuryrityksen (oikeilla) sivuilla jonain päivänä niille mennessään törmääkin esimerkiksi pornosivuihin. Vaikeammin havaittavaa olisi, jos sivu *näyttää* aivan oikealta mutta sisältöä on väärennetty jossakin tarkoituksessa.

Aitous joskus varmistettavissa sertifikaatista

Joissakin tapauksissa voidaan varmistaa sivun aitous edellä mainitun SSL:n ansiosta: suojatussa yhteydessä voit katsoa sivun ns. "sertifikaattia". Kussakin Web-selaimessa on oma tapansa tehdä tämä, mutta usein toimii alapalkissa olevan lukon kuvan kaksoisnapsauttaminen. Sertifikaatti ilmoittaa omistajansa ja sen, mikä taho on antanut sen. Voiko siihen tahoon sitten luottaa? Jos sertifiointipolkua taaksepäin seuraamalla päädytään esimerkiksi sellaiseen yritykseen kuin Verisign tai Thawte, niin asiat ovat todennäköisesti kunnossa.

Tavalliset sivut eivät yleensä sisällä mitään sertifikaatteja. Yleisemmin varsinkin jos aikoo käydä kauppaa tai harjoittaa muuta taloudellisesti tai muutoin merkittävää jonkun kanssa, kannattaa katsoa, kenen kanssa on tekemisissä. Täyttä varmuutta on vaikea saada, mutta ainakin kannattaa katsoa, onko sivuilla *mitään* yhteystietoja.

Jos toisesta ei ole helposti saatavilla muuta kuin esimerkiksi sähköpostiosoite, Web-sivun osoite tai postilokero-osoite, on syytä ruveta varsin epäluuloiseksi. Viranomaiset ovat usein varoittaneet, että Internetin välityksellä tapahtuvissa kaupoissa tulisi käyttää vain sellaisia luotettavia maksupaikkoja, joissa palvelun tarjoaja ilmoittaa avoimesti täydelliset yhtiö- ja osoitetietonsa sekä

kontaktihenkilönsä.

Kehittynyt sähköinen allekirjoitus voi auttaa

Sähköposti- ja muihin viesteihin voidaan eräillä tekniikoilla liittää niin sanottu kehittynyt sähköinen allekirjoitus. Tämä tarkoittaa tietoa, joka ei ole suoraan ihmisen luettavissa vaan on sopivilla ohjelmilla avattavissa niin, että käyttäjä voi saada varmistuksen siitä, että lähettäjä on se, joka sanoo olevansa. Menettely on vielä melko vähän käytössä, mutta sen käyttöä pyritään edistämään mm. turvallisen kaupankäynnin ja asioinnin edellytysten parantamiseksi. Suomessa on laki sähköisistä allekirjoituksista, joka mm. antaa kehittyneelle sähköiselle allekirjoitukselle virallisen aseman.

Arkikielessä käytetään usein ilmaisuja "sähköinen allekirjoitus" ja "digitaalinen allekirjoitus" erilaisissa merkityksissä. Lakitekstin muotoilut pyrkivät olemaan riippumattomia kulloinkin käytettävistä tekniikoista, ja siksi niiden suhde teknisiin termeihin voi vaihdella.

Muista, että seinillä on korvat - useammat kuin arvaatkaan

Tässä osassa:

- Ihmisillä on korvat.
- Roskisvakoilu on todellisuutta - ja tehokasta.
- Piuhoilla on korvat.
- Sähköposti vuotaa.
- Etäyhteydet.
- Modeemit.
- Yhteiset tiedostot: joustavuutta - ja riskejä.
- Salakirjoita kaikki, minkä pitää todella pysyä salassa.
- Oma veppipalvelin olis kiva - vai kuinka?

Ihmisillä on korvat

Suuri osa vakoilusta, yritysvakoilusta ja turva-aukkojen etsimisestä perustuu vain siihen, että joku pitää korvansa auki, kun kuulee viereisessä pöydässä tai seuraavalla penkkirivillä juteltavan. Voi myös erityisesti etsiytyä paikkoihin ja tilanteisiin, joissa voisi kuulla jotain kiinnostavaa. Lentoaseman odotustiloissa on usein asiantuntijoita ja johtajia, joilla on paljon aikaa tapettavanaan, ja siitäkös pulinaa syntyy.

Ihmiset ovat usein kummallisen varomattomia silloin, kun olettavat, ettei kuuloetäisyydellä ole ketään, jota asia voisi kiinnostaa. Siinä sitten pahimmillaan kerrotaan hauskoja juttuja oman firman turvajärjestelmien pettämisestä. Mutta viattomankin tuntuinen rupattelu voi antaa ulkopuoliselle tietoa, joka on hänelle tärkeää tietojärjestelmiin tunkeutumiseksi.

Myös varomaton kirjoittelu *netissä* voi aiheuttaa ongelmia. Vaikka esimerkiksi luulet esiintyväsi nimettömänä jossakin nettikeskustelussa ja uskallat siksi kertoa oman organisaatiosi turvaongelmista, on monia tapoja, joilla muut voivat päätellä enemmän kuin uskotkaan.

Yhteiset tulostimet ovat myös ongelma, koska moni voi nähdä tulosteesi vahingossa tai tahallaan. Kannattaa siis hakea tulosteensa pian. Salassa pidettävien asiakirjojen tulostamiseen on syytä käyttää vain valvotussa tilassa olevaa tulostinta. Tämä on myös edellytys kaikille luokitelluille turvajärjestelmille.

Varovaisuutta ei tarvita vain sellaisen tiedon suhteen, jonka salassa pitämiseen on ilmeinen tarve, kuten liikesalaisuuksien. Vaikka tiedot itsessään olisivat jopa julkisia, niitä ei kannata aina joka paikassa levitellä. Itse asiassa hyvin suuri osa yritys- ja muusta "vakoilusta" on vain julkisesti saatavilla olevien tietojen yhdistelemistä, ja jos tietoja on jossakin sopivasti valmiiksi yhdistettyinä, se helpottaa "vakoojan" työtä. Harkitse myös, mitä *henkilötietoja* itsestäsi ja muista annat verkon kautta löydettäväksi. Henkilötietoasioista on neuvoja tietosuojaviranomaisten sivuilla.

Roskisvakoilu on todellisuutta - ja tehokasta

Roskakoreja penkomalla saa selville uskomattoman paljon. Tämä koskee ensinnäkin oikeita roskakoreja, joihin saatetaan heittää muistiinpanoja kokouksista, tietokoneohjelmien listauksia, kirjeenvaihtoa asiakkaiden kanssa ja jopa salaisten suunnitelmien vanhoja versioita. Paperisilppuria tai vastaavaa kannattaa käyttää kaikille pois heitettäville papereille, joiden ei halua joutuvan kilpailijan, lehtimiehen tai vakoojan käsiin.

Mutta myös tietokoneen "roskakorista" löytyy kaikenlaista. Tavallistahan on, että tiedoston hävittämiseksi kutsuttu toimenpide merkitsee vain sen siirtämistä pois näkyvistä, "roskakoriksi" sanottuun hakemistoon. Sieltä se on helposti otettavissa esille. Mutta niin sanottu roskakorin tyhjentäminenkään ei todellisuudessa hävitä tiedoston sisältöä (ainakaan heti) niin, ettei asiantuntija saisi sitä käsiinsä ainakin osittain.

Ei edes kovalevyn formatointi ole kovin tehokas tuhoamistapa. Sopivilla taidoilla ja välineillä on dataa kaivettu esiin. Kaiken kaikkiaan kun esimerkiksi myyt tai muuten luovutat tietokoneesi toiselle, huolehdi siitä, että siihen ei jää mitään aineistoa, jota et halua muiden tietoon. Suhteellisuudentaju on toki hyvä säilyttää. Aineiston poistaminen *todella* varmasti on sen verran työlästä, että on halvempaa olla myymättä kovalevyään.

Myös *sähköposteja* voi jäädä roikkumaan paikkoihin, joista ne ovat nuuskittavissa. Tyypillisesti sähköpostiohjelma tallentaa sekä vastaanotetut viestit että kopiot lähetetyistä joko käyttäjän omaan tietokoneeseen tai Internet-yhteydentarjoajan sähköpostipalvelimeen tai molempiin.

Piuhoilla on korvat

Verkon "salakuuntelu" on helpompaa kuin luuletkaan

Kun tietoa kulkee verkossa, se on näkymätöntä. Voi olla vaikea hahmottaa, että seinään upotetussa kaapelissa kulkeva tieto on "kuunneltavissa" salaa. Mutta todellisuudessa on paljon helpompaa seurata salaa viestintää dataverkoissa kuin esimerkiksi kuunnella salaa puhelinkeskustelua. Tarvitaan toki jonkin verran osaamista ja sopiva laite tai pääsy laitteen luo; sitten onkin *paljon* tietojen virtaa saatavilla. Tietoon sisältyvät tällöin paitsi ihmisten toisilleen lähettämät viestit myös esimerkiksi käyttäjän "keskustelu" jonkin tietojärjestelmän kanssa.

Niin pitkä matka...

Olennaista on, että verkossa tietovirta kulkee monien tietokoneiden kautta. Ennen kuin Suomesta lähetetty sähköpostiviesti päätyy vastaanottajalle Uuteen Seelantiin, se on kulkenut hyvin monen koneen kautta, ensin Suomessa ja sitten muualla. Mutta myös paikallisverkossa viesti kulkee koneesta toiseen: yksi kone ottaa vastaan viestin ja lähettää sen seuraavalle. Yleensä mukana kulkee tieto siitä, mille koneelle viesti on menossa, mutta tämä ei yleisimmissä verkkoratkaisuissa estä sitä, että viesti luetaan jossakin muussa koneessa. Ja eri kerroilla viesti voi hyvin kulkea eri reittejä.

Paikallisverkkokaan ei ole ongelmaton

Jokainen yhteys tietokoneiden välillä voi olla turvaton, ja turvaton voi olla myös jokainen niistä tietokoneista, joiden kautta data kulkee. Kaikkea informaatiota, joka kulkee verkoissa, saatetaan lukea salaa. Erilaiset verkot ovat toki eriasteisesti haavoittuvia sellaiselle. Internet on tässäkin suhteessa aivan toisella tapaa avoin kuin jokin suljettu paikallisverkko, mutta ison organisaation paikallisverkkoonkin voi päästä liittämään laitteen aika helposti. Liittäminen sinänsä voi tapahtua täysin luvallisestikin; tietoturvauhkistahan hyvin suuri osa on organisaation *sisäisiä*. Luvaton liittyminen paikallisverkkoon on erityisen helppoa silloin, kun kyseessä on langaton lähiverkko (WLAN).

Salasana ei kulje salattuna! (Yleensä)

Jos yhteydenotto toiseen tietokoneeseen tai toisessa koneessa olevaan palveluun vaatii salasanaa, niin myös salasana kulkee verkossa ja voidaan siis siepata. Jos kyse on vaikkapa ilmaispalvelusta, johon on saanut salasanan, kun on antanut vähän henkilötietojaan, tähän ei yleensä sisälly suurta riskiä. Tosin se, että joku pääsee esimerkiksi kirjoittelemaan julkisuuteen sinun tunnuksellasi, voi olla vähintäänkin noloa.

Mutta jos salasana antaa pääsyn esimerkiksi pankkipalveluihin, sillä ehkä voi tyhjentää tilisi käden käänteessä. On siis olennaista, kulkeeko salasana salakirjoitettuna. Tämän ohella on merkitystä sillä, liittyykö pankkipalvelun käyttöön *lisäksi* kertakäyttösalasanoja, jotka antavat merkittävän lisäturvan.

Jos aiot maksaa luottokortilla netissä, perehdy luottokorttiyhtiön antamiin ohjeisiin, sellaisiin kuin Luottokunnan ohje *Asioi turvallisesi verkossa*.

Sähköposti vuotaa

Kuin postikortti?

Sähköpostikin kulkee Internetin kautta tietokoneesta toiseen ja on siten siepattavissa eri tavoin kuten muukin Internet-tietoliikenne. *Lisäksi* se tallentuu saapuvien viestien "laatikkoon" (ns. mailbox), ja siellä se saattaa olla muiden nähtävissä. Tosin yleensä vain järjestelmän ylläpitäjien, mutta voiko kaikkiin ylläpitäjiinkään kaikissa tilanteissa luottaa?

Huomaa, että töissä lähetetty tai vastaanotettu sähköposti ei ehkä ole yksityinen kaikkialla; asia riippuu kunkin maan lainsäädännöstä ja sen tulkinnoista. Suomessa tilanne on periaatteessa selvä (sähköposti on viestintäsalaisuuden alaista), käytännössä ei niinkään, vaan monin paikoin tulkitaan, että esimerkiksi työnantajalla sittenkin olisi oikeus joillakin perusteilla lukea työntekijöiden sähköposteja. Käytännössä tietoturvan kannalta on olennaista, että toisten sähköpostien lukemisen *tekniset* esteet ovat monien murrettavissa.

Älä siis lähetä hyvin luottamuksellista tai henkilökohtaista informaatiota sähköpostitse ainakaan suojaamattomana (salaamattomana).

Luotettavalla menetelmällä salakirjoitettuna sähköposti on turvallinen urkintayrityksiä vastaan (joskaan ei sellaista häirintää vastaan, joka estää sen perillemenon). Valitettavasti vain luotettava salakirjoitus on vielä melko työlästä ottaa käyttöön ja opetella käyttämään, ja luonnollisestikin vastaanottajan tulee myös osata purkaa se.

Uudelleenohjaus... turvattoman yhteyden kautta?

Sähköpostin uudelleenohjaus (forwardointi) on usein kätevältä tuntuva palvelu ja monissa järjestelmissä helppo toteuttaa, mutta siihen liittyy riskejä. Ajatellaanpa seuraavaa tilannetta: Käytät työssäsi suhteellisen turvallista, suojattua järjestelmää. Haluat kuitenkin ohjata työosoitteeseesi

tulevan sähköpostin sellaiselle tunnukselle, jota käytät kotoasi käsin yksityisen Internet-yhteydentarjoajan kautta, muun muassa voidaksesi tehdä töitä kotonakin. Tuntuuko asialta, josta työnantajasi olisi iloinen? Ehkä, jos ei ajatella sitä, että kaikki sinulle tuleva sähköposti, myös työasioita koskeva, kulkee tällöin Internetissä ja lisäksi tallentuu yhteydentarjoajan palvelimeen. Se on tällöin urkittavissa siitä riippumatta, miten hyvin suojattu työpaikan oma verkko on.

Etäyhteydet

Monet verkon hyväksikäyttömahdollisuudet perustuvat etäyhteyksiin (remote connections), joissa tietokonetta käytetään matkan päästä, usein niin, että käyttäjä ikään kuin tekee tietokoneestaan toisen koneen päätteen. Tällöin siis kyse on tietokoneiden välisestä tietoliikenteestä, jota koskevat edellä esitetyt turvaongelmat.

Riskejä voidaan merkittävästi vähentää käyttämällä etäyhteyksiin *salaavia* yhteysohjelmia kuten SSH-tekniikkaan perustuvia. Esimerkiksi Windowsin tai Unixin mukana tulevaa Telnet-ohjelmaa *ei* yleensä pidä käyttää, koska se lähettää tiedot täysin salaamattomina.

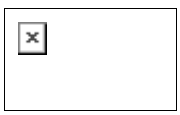
Modeemit

Modeemeja käytetään yhä tietoliikenneyhteyksiin, ja niillä onkin oma käyttöalueensa, koska ne mahdollistavat tietoliikenteen tavallisen puhelinverkon ja -liittymän kautta.

Kotikäyttäjälle modeemit eivät yleensä tuo isoja ylimääräisiä turvariskejä, yllättävän isoja laskuja kylläkin, ellei tunneta laskutusperusteita. Lähinnä kannattaa mainita, että on olemassa haittaohjelmia, jotka muuttavat järjestelmää siten, että puhelinyhteys huomaamattomasti vaihtuu toiseen. Ja kun se toinen onkin maksullinen numero ulkomailla, tulee iso lasku. Tätä vastaan auttaa lähinnä se, että ei hanki ohjelmia epämääräisistä lähteistä.

Muualla, siis lähinnä työpaikoilla, modeemit sen sijaan ovat erityinen riski. Joku ehkä keksii kytkeä työhuoneessaan olevaan tietokoneeseen modeemin ja jättää koneen ja modeemin toimintaan voidakseen sitten kotoa ottaa siihen yhteyden. Niin ei pidä tehdä, ei ainakaan keskustelematta työpaikan tietoturva-asiantuntijan kanssa. Vaikka työpaikan tietoliikenneverkko olisi miten hyvin suojattu, niin tuollainen järjestelmä mahdollistaa sen, että tavallista puhelinlinjaa pitkin päästään siihen käsiksi. Sama voi koskea tilannetta, jossa otat työpaikkasi koneesta yhteyden modeemin kautta muualle. Tietokoneesihan on yleensä kytkettynä paikallisverkkoon, joten modeemi muodostaa sen ja puhelinverkon välille yhteyden, ikään kuin turvamuurin ali kaivetun käytävän.

Yhteiset tiedostot: joustavuutta – ja riskejä



Erilaisten paikallisten tietoliikenneverkkojen keskeisiä etuja on resurssien yhteiskäyttö. Voidaan käyttää samoja tulostimia, tiedostopalvelimia ym. Ja voidaan saada esimerkiksi yhteiskäytössä oleva kovalevy näkymään eri käyttäjien tietokoneissa ikään kuin paikallisena levynä niin, että käyttäjä ehkä ei edes tiedä, milloin hän tallentaa tiedoston oman koneensa levylle ja milloin jonnekin muualle.

Tähän sisältyy kuitenkin ongelmiakin. Jos suojaukset eivät ole kunnossa, voivat käyttäjät ehkä lukea sellaisiakin muiden käyttäjien tiedostoja, joita heidän ei ole tarkoitus nähdä, ja kenties muuttaa ja tuhotakin niitä. Etenkin jos useat käyttäjät voivat *kirjoittaa* samoihin tiedostoihin, pitää huolehtia siitä, ettei kaksi ihmistä muuttele samaan aikaan samaa tiedostoa, jolloin ainakin toisen työ yleensä menee hukkaan.

Jos siis käytössäsi on mainitunlainen yhteiskäyttöinen järjestelmä, perehdy huolella sen toimintaan ja sitä koskeviin ohjeisiin.

Harkitse salakirjoittamista

Mikä on tarpeen salata?

Viestit ja tiedostot ovat erilaisia sen suhteen, miten tärkeää niiden julkisuus tai yksityisyys on. Joidenkin ehkä erityisesti haluat tulevan mahdollisimman monen tietoon. Jotkin taas ovat täysin henkilökohtaisia muistiinpanojasi, joita et halua *kenenkään* muun näkevän missään oloissa. Valtaosa on jostain siltä väliltä.

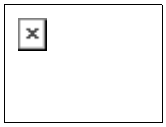
Tietojen erityinen salaaminen salakirjoittamalla (kryptaaminen, *encryption*) vaatii erityisiä välineitä ja lisätyötä, joten sitä on syytä käyttää vain tarvittaessa. Toisaalta tarvittaessa sitä *on* syytä käyttää.

Kaikista suojauksista huolimatta joku voi päästä käsiksi aineistoihisi. Vaikka esimerkiksi firman sisäinen verkko olisi miten hyvin suojattu, *jollakulla* pitää olla tekniset mahdollisuudet päästä käsiksi suojattuihin tietoihin. Tätä henkilöä voidaan kutsua ylläpitäjäksi tai mikrotukihenkilöksi tai jollakin muulla nimikkeellä. Vaikka häntä pitäisi miten luotettavana tahansa, kaikenlaista voi sattua. Hän ei ehkä mistään hinnasta eikä minkään kiristyksen takia rupeaisi ulkopuolisen palvelukseen vakoojaksi, eikä hän ehkä tule hulluksi eikä toheloi eikä kostaisi, jos häntä kohdellaan huonosti. Tosin eräiden selvitysten mukaan organisaation *sisältä* tulevat tietoturvahyökkäykset ovat yleisempiä kuin ulkopuoliset. Mutta uhkan muodostaa pelkästään se, että ylläpitäjä saattaa *vahingossa* paljastaa tietoja, vaikka toimisi huolellisesti.

Salakirjoitus: viimeinen puolustusmuuri

Kaikessa, missä on ihminen mukana, on myös mahdollisuus, että tämän ihmisen osalta tietoturva *jollain tapaa* pettää. Joudumme paljon luottamaan muihin, mutta on hyvä olla viimeinen puolustusmuuri *jokaista* ulkopuolista vastaan. Ja itse asiassa myös itseäsi. Sinä saatat unohtaa tärkeimmän ja luottamuksellisimman tiedostosi jonnekin, mistä joku muu saa sen käsiinsä. Eikö silloin ole hyvä, että se onkin salakirjoitettu, niin että se on pelkkä mieletön merkkijono, ellei ole menetelmää ja avainta, joilla se saadaan selväkieliseksi?

```
qANQR1DBwU4DrPtn1RrPI2EQCACVPL...
```



Tärkeimpien aineistojen salakirjoittaminen on erityisen tärkeää, jos jaat tietokoneesi muiden kanssa. Esimerkiksi kotitietokonetta saattavat käyttää huonetoverit, jotka ovat ystävyksiä mutta pitävät parempana pitää sähköpostinsa ja raha-asioita koskevat tietonsa yksityisinä. Salakirjoittaminen mahdollistaa yksityisyyden säilyttämisen yhteiskäytössä.

Joissakin maissa (mutta ei Suomessa) on salakirjoitusta lailla rajoitettu. Toimiessasi ulkomailla selvitä tällaiset asiat. Apua voi olla koosteesta *Crypto Law Survey*. <http://rechten.kub.nl/koops/cryptolaw/>

Jos hukkaat salasanan, hukkaat kaiken

Salakirjoittamisessa käytettyjen sanasanojen tai avainten suhteen pitää tietysti olla erityisen huolellinen. Jos hukkaat tiedon, joka tarvitaan salakirjoittamasi aineiston avaamiseen, olet tietysti tehnyt paljon vahinkoa itsellesi: et enää mitenkään pääse käsiksi mihinkään, mikä sinulla on vain salatussa muodossa. Jos voisit päästä, valitsemasi salakirjoitusjärjestelmä olisi kelvoton!

Jos taas salasana vuotaa ulkopuolisille, vahinko voi olla vielä suurempikin. Voi olla, että salattu aineisto ei enää olekaan sinulle tarpeen, mutta ulkopuolinen voi saada siitä sellaista tietoa, mitä hänen ei pitäisi missään nimessä saada.

Turvakopio salasanasta?

Voi olla viisasta panna talteen useampia kuin yksi kopio, mutta kaikkien kopioiden pitää sitten olla todella turvallisessa paikassa. Organisaatiossasi saattaa olla käytössä periaate, jonka mukaan mainitunlainen tieto on annettava myös esimerkiksi tietoturvasta vastaavalle henkilölle. Tämä on tietysti tärkeää, koska työasioita koskevia, salakirjoittamiasi tietoja saatetaan tarvita juuri silloin, kun olet yllättäen joutunut leikkaukseen tai lomalla jossain erämaassa ilman puhelinta. Mutta tällöin on syytä muistaa, että henkilökohtaisimmat asiat on syytä turvata ja salata muilla keinoin.

Eräissä maissa on käytössä sellainen vara-avainjärjestelmä (key escrow), jossa salausavainten turvatalletus on säädetty pakolliseksi ja turvatalletuksessa oleva avain on tietyissä tilanteissa tai oikeuden päätöksellä luovutettava sitä vaativalle viranomaiselle. Suomessa näin *ei* ole, ja Euroopan unionissa sellaiset järjestelyt on kielletty sähköisiä allekirjoituksia koskevassa direktiivissä (1999/93/EY).

Erilaisia salaustekniikoita

Vaikka salakirjoitusohjelmia on helposti saatavilla, niiden laatu voi vaihdella suuresti. Moniin tavallisiin sovellusohjelmiin sisältyy mahdollisuus salakirjoittaa dataa, mutta niiden salakirjoitustekniikat voivat olla hyvin heikkoja.

Yleisimmin käytettyjä salakirjoitusmenetelmiä on PGP. Menetelmää käyttäviä ohjelmistoja on saatavilla myös maksuttomina useimpiin käyttöympäristöihin. Kerran käyttöön otettuna PGP on teknisesti aika helppo käyttää. Asia riippuu mm. käyttöympäristöstä, mutta melko tyypillisessä PGP:n asennuksessa ilmestyy sähköpostiohjelman valikoihin vaihtoehtoja, joilla voi salata lähtevän viestin tai allekirjoittaa sen sähköisesti tai avata salattuna saapuneen viestin. PGP:tä voi käyttää muutenkin kuin viestinnässä, esimerkiksi omien tiedostojen salaamiseen.

PGP:n suurimpia ongelmia ovat se, että se on sittenkin melko vähän tunnettu, ja se, että useissa sen käyttömuodoissa on olennaista varmistua viestinnän toisen osapuolen henkilöllisyydestä. Lähtevän sähköpostin PGP-salaukseen nimittäin käytetään vastaanottajan ns. julkista avainta (public key), joka voidaan kyllä panna vaikka julkisesti näkyville, mutta lähettäjän on olennaista varmistua, että kyseessä on oikean vastaanottajan julkinen avain. Toisaalta esimerkiksi PGP:n käytössä omalla kovalevyllä olevien tiedostojen salaamiseen ei näitä ongelmia ole.

Kaikessa PGP:n käytössä on aivan keskeistä huolehtia oman PGP-salasanansa (passphrase) muistamisesta ja salassa pitämisestä. Jos esimerkiksi unohdat PGP-salasanan, jolla olet salakirjoittanut omia tiedostojasi, et itsekään enää mitenkään saa niitä avatuiksi.

Tavallisen PC:n käyttäjälle riittänee PGP:n käytön alkuun pääsemiseksi ohje *PGP:n käyttö Windowsissa*. <http://www.cs.tut.fi/~jkorpela/softa/pgp.html> Unix-käyttäjälle taas voi sopia, soveltuvin osin, Tampereen yliopistossa tehty suomenkielinen ohje *PGP - Pretty Good Privacy*. <http://www.uta.fi/laitokset/tkk/ohjeet/unix/pgp.shtml>

PGP:n kanssa kilpailevista tekniikoista merkittävin on S/MIME. Se on ns. MIME-sähköpostin laajennus, joka sisältää sanakirjoituksen ja sähköisen allekirjoituksen.

Oma veppipalvelin olis kiva – vai kuinka?

Tietokoneiden tehon ja ennen muuta Internet-yhteyksien parantuessa on ruvettu pystyttämään palvelimia (servers) jopa henkilökohtaisiin kotitietokoneisiin. Tavallisinta on ehkä asentaa kotikoneeseen Web-palvelin esimerkiksi omiin Web-sivuihin liittyvää testausta varten, ennen siirtoa "oikeaan" palvelimeen.

Vaikka palvelimesta voi olla monenlaista hyötyä ja hupia, niin palvelin omassa koneessa aiheuttaa

runsaasti tietoturvariskejä. Siihen kannattaa ryhtyä vasta, kun hallitsee tietoturvan perusteet hyvin ja on valmis perehtymään niihin lisäongelmiin, joita on itselleen hankkimassa. Palvelimen asentaminen on usein teknisesti helppoa, mutta sen tekeminen oikein on jo vaativampaa. Aihetta käsitellään jäljempänä ohjeessa palvelinten asentamisesta.

Vaikka et aio asentaa koneeseesi palvelinta, on hyvä tietää tämä: Jotkin ohjelmat saattavat käynnistää koneeseesi palvelimia, tietämättäsi tai esitettyään hämärän kysymyksen. Tähän ei voi yleisesti sanoa muuta kuin kehottaa yleiseen varovaisuuteen sitä suuremmassa määrin, mitä epämääräisemmästä lähteestä ohjelma on. On myös hyvä tietää, että sanan "server" asemesta voidaan palvelimista käyttää muutakin yleisnimitystä, esim. Unixissa *daemon* (tai *demon*) ja Windowsissa *System Agent* tai *service*.

Lukitse ovesi ja tietokoneesi, kun lähdet muualle

Tietokone kiinni

Älä jätä tietokonetta "auki", kun lähdet muualle, älä ainakaan niin, että olet kirjautuneena verkkoon tai johonkin palveluun. *Tietokoneen käyttäjän turvaoppaassa* on aiheesta havainnollinen esimerkki:

> Niin ilkeältä kuin se tuntuukin, ei ole epätavallista, että joku tulee ja tuhoaa työsi. Jos pysyisit sisäänkirjautuneena, kuka tahansa voi poiketa käymään ja tehdä vahinkoa, josta sinua saatetaan pitää vastuullisena. Kuvittele esimerkiksi niitä vaikeuksia, joissa voisit olla, jos siivoton sähköpostiviesti lähetettäisiin työpaikkasi ylimmälle johtajalle tai tunnustasi käytettäisiin laittoman pornografian siirtämiseen.

Ainakin työpaikoilla ja julkisissa tiloissa tulisi huolehtia siitä, että kun lähtee tietokoneen äärestä, se jää tilaan, jossa sitä ei pysty ainakaan helposti käyttämään kuka tahansa paikalle osuva. Tämä merkitsee ennen muuta ohjelmien käyttöä koskevia menettelyjä, joita kuvataan jäljempänä.

Kotioloissakin voi sattua monenlaista. Vaikka perheen sisällä olisi sovittu menettelytavoista ja niitä noudatettaisiin, niin jonkun perheenjäsenen vieras saattaa ymmärtämättömyyttään räplätä tietokonetta ja aiheuttaa vahinkoa.

Poistu ohjelmista ja palveluista

On hyvä opetella poistumaan ohjelmasta tai palvelusta, kun sitä ei enää tarvita. Kun rupeaa käyttämään uutta ohjelmaa, kannattaa heti aluksi selvittää, miten sen käyttö lopetetaan eli "miten täältä pääsee ulos". Siitä nimittäin on monia erilaisia kehitelmiä; yhdessä ohjelmassa toimii käsky `quit`, toisessa `exit`, kolmannessa jokin muu. Lisäksi ohjelma lopetuksen yhteydessä usein vaatii tai kehottaa käyttäjää tekemään joitakin erityisiä lopetustoimia, kuten kertomaan, haluaako hän tallentaa tiedostoon tehdyt muutokset.

Usein palveluita on lisäksi "sisäkkäin": omasta koneesta on esimerkiksi yhteys verkkoon, jonka kautta ollaan suorassa yhteydessä toiseen koneeseen, jossa käytetään jotain ohjelmaa, jonka sisällä mennään johonkin erityiseen palveluun jne. Tällaiset ketjut on sitten hyvä aikanaan purkaa vaihe vaiheelta, jotta ei jää minnekään roikkumaan ja jotta kaikki tarvittavat tietokantojen päivittymiset yms. tapahtuvat. Mutta vaikka olisit mielestäsi poistunut kaikista palveluista, jotain voi silti jäädä käyttöön, ja joka tapauksessa sekin, että muualle lähtiessäsi vain oma koneesi jää "auki", muodostaa riskin.

Kun olet lopettamassa tietokoneen käyttöä, on syytä ensin lopettaa kaikki ohjelmat ja vasta sitten

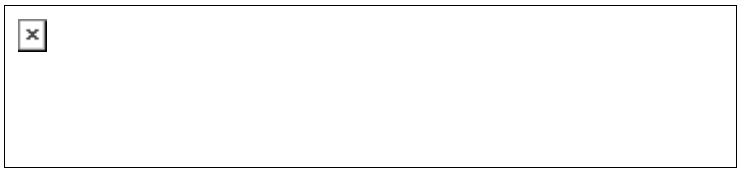
käyttää tietokoneen sammutustoimintoa. Jos kyse on Windowsista, napsauta vuorollaan kutakin ruudun alareunassa näkyvää ohjelman ikkunan kuvaketta avataksesi itse ikkunan ja käytä sitten ohjelman omaa lopetustoimintoa. Vasta sitten valitse Käynnistä- eli Start-valikosta koneen sammutus. Tämä suojaa myös sitä vastaan, että olet unohtanut tallentaa jotakin tärkeää, ja lisää todennäköisyyttä sillä, että Windows sammuu "siististi" ja käynnistyy ongelmitta seuraavalla kerralla.

"Näytönsäästäjä" ei säästä näyttöä mutta antaa suojaa

Käytä salasanan suojaamia joutonäyttöjä aina kun mahdollista. Sellainen voidaan asettaa käynnistymään itsestään, kun tietokone on ollut joutilaana jonkin aikaa. Kymmenen minuuttia lienee sopiva aika. Tietysti on hyvä käynnistää joutonäyttö "käsin", kun lähtee koneen äärestä, mutta automaattikäynnistys antaa lisäsuojaa unohduksia vastaan.

Joutonäyttöjä sanotaan usein näytönsäästäjiksi (screen saver). Alkuperäinen käyttötarkoitus on käytännössä menettänyt merkityksensä laitetekniikan kehittyessä, mutta *väärinkäytöltä suojautuminen* on uusi, tärkeä hyöty, kunhan käytetään salasanasuojausta. Toki jotkin joutonäytöt ovat kivan näköisiäkin.

Tyypillisessä suomenkielisessä Windowsissa päästään "näytönsäästäjän" asetuksiin valitsemalla Käynnistä-valikosta Asetukset-kohta ja sitten Ohjauspaneeli, napsauttamalla Näyttö-kuvaketta ja sitten valitsemalla Näytönsäästäjä-vaihtoehto.



Yleiset koneet - erityinen riski

Varsinkin kirjastoissa, oppilaitoksissa ja muualla, missä on monien ihmisten yhteiskäytössä olevia tietokoneita, sattuu aika usein, että käyttäjä lähtee muualle hetkeksi tai kokonaan ja jättää koneen tilaan, jossa hän on kirjautuneena yhteen tai useampaan palveluun. Se on suorastaan vaikeuksien kerjäämistä. Sen lisäksi, että joku voi tehdä jäynää, hän voi tehdä todellista vahinkoa joko ilkeyttään tai ymmärtämättömyyttään.

Kahvitauolle tai vastaavalle lähdettäessä voi riittää ohjelmallisesti lukita kone (salasanalla suojatulla joutonäytöllä). Tarkista kuitenkin, mitä paikallisissa ohjeissa sanotaan; koneen varaaminen sillä tavoin saattaa olla kiellettyä. Muutoin on syytä yksinkertaisesti katkaista kaikki yhteydet, myös kirjautuminen lähiverkkoon ja itse koneeseen. Odota ja tarkista, että kaikki varmasti katkeaa.

Työskentelyä koneen ääressä on syytä ruveta lopettelemaan muutamaa minuuttia *ennen* kuin pitää lähteä luennolle tai bussille, sillä on varauduttava siihen, että jotain meneekin pieleen eikä lopettelu suju ihan ongelmitta.

Ovikin lukkoon, jos mahdollista

Tietokoneen sulkemisen *lisäksi* on työpaikalla syytä lukita ovi, jos mahdollista. Erityisesti tämä koskee sellaisia virastoja ja muita tiloja, joiden auloihin, käytäviin yms. yleisöllä on vapaa pääsy. Yleisön ei tietenkään pidä päästä työhuoneisiin silloin, kun siellä ei ole ketään työntekijää. Ulkopuolista ei pidä jättää huoneeseen yksin.

Käytännössä joudutaan tekemään kompromisseja, jotta asiat sujuisivat joustavasti, mutta mitä useammin jätät oven auki, sitä tärkeämpää on huolehtia *muista* turvakeinoista.

... mutta älä luota lukkoihin

Vanha totuus on, että lukot eivät ole varkaita vaan rehellisiä ihmisiä varten. Lukko ei kauaa ammattivarasta pidättele, mutta melko rehellistä ihmistä se auttaa pysymään kaidalla tiellä. Osittain sama koskee erilaisia teknisiä suojauksia kuten salasanasuojauksia, salakirjoitusta jne. Ei siis pidä tuudittautua siihen, että mitään pahaa ei voi tapahtua, kunhan ovi on lukossa ja tietokoneessa jonkinlainen suojaus.

Mitä tärkeämpiä tietoja ja käyttömahdollisuuksia koneessasi on, sitä tärkeämpää on rakentaa lisäsuojauksia, esimerkiksi salakirjoittaa kovalevyllä olevat tiedot ainakin tärkeimmältä osaltaan. Tässä, kuten yleensäkin tietoturvassa, joudutaan etsimään kohtuullisia ratkaisuja täydellisen suojan asemesta. Kotitietokone, jota käytetään lähinnä pelaamiseen, nettisivujen katseluun ja henkilökohtaisten mutta ei arkaluonteisten tekstien kirjoittamiseen, ei ole sellaisen suojan tarpeessa kuin kone, jossa on tärkeää liikekirjeenvaihtoa, lähes valmis patenttihakemus tai sairaalan potilasrekisteri.

Kätevä kantaa - varkaankin

Mitä kevyempi ja pienempi tietokone, sitä mukavampi se on kantaa mukana - varkaankin. Siksi kannettavan tietokoneen (tai taskutietokoneen tms.) suojaaminen ohjelmallisilla lukoilla ja muilla keinoin (esim. tärkeimpien tietojen salakirjoittamisella) on erityisen tärkeää mutta ei toisaalta riittävää. Rikollisen on paljon helpompi murtaa koneen ja sen ohjelmien suojauksia, kun kone on hänen hallussaan eikä laillinen omistaja edes tiedä, missä se on.

Kannettavan tietokoneen *fyysisestä* turvallisuudestakin on siis huolehdittava. Ainakaan sitä ei pidä jättää esimerkiksi näkyviin auton takaistuimelle, josta "tavallinen varas" saattaa varastaa sen ihan vain sen aineellisen jälleenmyyntiarvon takia. Ja varsinkin matkoilla oudoissa oloissa on muunlaisen varkauden tai rikkoutumisen tai unohtumisen vaara huomattava.

Jos kannettavaa tietokonetta käytetään olennaisesti vain matkakirjoituskoneena, yksi menettelytapa voisi olla seuraava: Kaikki sillä tuotetut dokumentit salakirjoitetaan, ja näistä salakirjoitetuista tiedostoista otetaan saman tien varmuuskopiot levykkeille. Levykkeet pidetään eri paikassa kuin kone ja sopivissa koteloissa, jotka suojaavat niitä ulkonaisilta vaurioilta kuten murtumiselta tai roskaantumiselta. Tällöin koneen tuhoutuminen tai varastaminen aiheuttaa vain aineellisen vahingon, ja vakuutus ehkä osittain korvaa sen. Käytännössä koneeseen yleensä halutaan ottaa mukaan erilaisia tietoaineistoja, joiden halutaan olevan käytettävissä matkalla. Tällöin pitää harkita siihen sisältyviä tietoturvariskejä, koska kaikkea ei ehkä ole käytännöllistä salakirjoittaa, ja etsiä sopiva kompromissi.

Käytä salasanoja, joissa on muitakin merkkejä kuin kirjaimia, ja pidä ne salassa

"Salasana" ei saa olla mikään kielen sana. Mutta salainen sen pitää olla.

Mistä salasanoissa on kyse?

Salasanoja joka paikassa

Tietokoneita, ohjelmia, palveluita ym. suojataan usein salasanoilla: merkkijonolla, jonka oletetaan olevan vain laillisen käyttäjän tiedossa. Usein joudut antamaan eri salasanoja peräkkäin eri yhteyksissä, esimerkiksi ensin käynnistäessäsi koneesi, sitten ehkä heti perään ottaessasi verkkoyhteyden, sen jälkeen kenties mennessäsi johonkin palveluun jne.

Salasanojen laatu ja salassapito eivät ole tärkeitä niinkään siksi, että salasanasuojaus olisi erityisen hyvä suojakeino, vaan siksi, että se niin usein on käytännössä lähes *ainoa* turva-aita sinun ja

luvattoman käyttäjän välillä.

Salasana yleensä liittyy tunnukseen

Käytännössä salasanaan usein liittyy *käyttäjätunnus* (user id, user name, account name), kun on kyse järjestelmästä, jolla voi olla useita laillisia käyttäjiä. Tällöin käyttäjätunnus on usein jotain yksinkertaista, esimerkiksi oikeasta nimestä muodostettu tai sähköpostiosoite, kun taas salasana on tunnistetiedon salainen osa.

Logataanpa sisään - mutta myös ulos

Usein järjestelmän käyttö on aloitettava erityisellä *kirjautumisella* (login), jossa annetaan käyttäjätunnus ja salasana, tai joskus vain salasana. (Toinen, harvinaisempi tilanne on se, että kutakin toimenpidettä varten pitää erikseen antaa salasana.) Tämän jälkeen järjestelmä on käytettävissä kyseistä tunnusta vastaavilla käyttöoikeuksilla. Käytön lopuksi on tällöin **kirjauduttava ulos** (logout, logoff) erillisellä komennolla tai näppäilyllä tms., koska muutoin yhteys järjestelmään jää auki. Uloskirjautuminen voi olla olennaista muistakin syistä, mutta sen välttämättömyys tietoturvan kannalta lienee ilmeistä. - Järjestelmiin saattaa sisältyä automaattikatkaisuja esimerkiksi 15 minuutin hiljaisuuden jälkeen, mutta niihin ei pidä luottaa.

Salasana: annettu tai valittu

Järjestelmästä riippuu, onko salasana käyttäjän valittavissa vai annetaanko se hänelle valmiina. Usein tilanne on muodollisesti jälkimmäinen mutta asiallisesti edellinen: käyttäjälle annetaan käyttöluvan yhteydessä jokin salasana ja kehotetaan häntä heti vaihtamaan se itse. Tällaista kehotusta kannattaa todella noudattaa, varsinkin kun alkuperäinen salasana on usein hyvin alkeellinen. Varsin tavallinen välimuoto on, että käyttäjä voi valita salasanansa, mutta sen on täytettävä jonkinlaiset tekniset laatuvaatimukset, jotka salasananvaihto-ohjelma hänelle antaa.

Millainen salasana on hyvä?

Salasana ei saa olla sana

Jos sana "salasana" ja sen englanninkielinen esikuva "password" vielä voitaisiin poistaa kielestä, se pitäisi ehdottomasti tehdä. Tämä sana on omiaan vahvistamaan harhakäsitystä, joka on suurimpia uhkia tietoturvalle. Salasanaa on syytä pitää **salakoodina**. Salasana ei saa olla sana millään kielellä, ei myöskään mikään tavallinen lyhenne, ei auton rekisterinumero, ei syntymäaika eikä ylipäänsä mitään luonnollista!

Luonnollinen salasana on kyllä helppo muistaa. Mutta se on myös usein helppo ihan arvata, varsinkin, jos se on jotain niin yksinkertaista kuin oma tai vaimon nimi tai rakkaan harrastuksen nimi. Mutta arvaamista suurempi riski on *järjestelmällisten murtomenetelmien* vaikutus. On helppo ohjelmoida tietokone ottamaan esimerkiksi miljoona sanaa sisältävä luettelo ja kokeilemaan sana sanalta, pääsisikö sitä salasanana käyttämällä sisään johonkin palveluun. Ja mikään kovin yksinkertainen muuntelu ei paljoakaan suojaa tämäntapaisilta murtoyrityksiltä. Esimerkiksi jonkin numeron lisääminen sanan perään (kuten "jukka2") on ehkä ilmeinen tapa suojautua murroilta, mutta sepä onkin niin ilmeinen, että murto-ohjelman tekijäkin sen keksii ja ottaa huomioon ohjelmassaan.

Tee salasanasta koodimainen

Salasanan tulisi siis sisältää sekaisin numeroita, isoja ja pieniä kirjaimia ja erikoismerkkejä. Toisaalta sen pitäisi olla käyttäjän itsensä muistettavissa!

Vältä kuitenkin sellaisia merkkejä, joita et ehkä pysty kovin helposti kirjoittamaan oudolla näppäimistöllä, jollaista voit joutua käyttämään. Esimerkiksi ä:tä ja ö:tä ei kannata käyttää. Sen sijaan esimerkiksi piste, pilkku ja kysymysmerkki ovat sopivia, koska ne löytyvät kaikista näppäimistöistä.

Usein suositeltu menetelmä on ottaa jokin lause, joka pysyy mielessä, ja muodostaa sekavahko merkkijono siitä muuntamalla, tavalla, jonka itse muistaa. Esimerkiksi lauseenalusta "Vaka vanha Väinämöinen" saisi välilyönnit vinoviivoilla korvaamalla ja ä:n ja ö:n pisteet kaksoispisteillä korvaamalla merkkijonon "Vaka/vanha/Va:ina:mo:inen", joka lienee vielä muistettavissa mutta jonka arvaaminen tai murtaminen on epätodennäköistä. *Tietenkään* ei pidä käyttää mitään tällaisissa salasanaohjeiden esimerkeissä esitettyä salasanaa sellaisenaan!

Paina se mieleesi, juuri sellaisena kuin se on

Salasanaa ei pitäisi kirjoittaa paperilapulle eikä tiedostoon, mutta varmista, että muistat sen. Isojen ja pienten kirjainten ero on yleensä merkitsevä salasanoissa! Yksi menettely on kirjoittaa uusi salasana paperilapulle, jota sitten pidetään koko ajan mukana, kunnes se painuu mieleen, kun salasanaa muutamia kertoja käytetään ja lappu voidaan repiä. Tietenkin on mieletöntä jättää salasanaa teipattuna kuvaruutuun tai pöydän alapinnalle tms. Se on vähän kuin kirjoittaisi pankkiautomaattikortin tunnusluvun korttiin itseensä.

Salasanan oikea käyttö

Ei toisten nähden

Yhteydenottoa salasanaa vaativaan palveluun ei pidä tehdä toisten nähden. Vaikka käyttöliittymät ovat tyypillisesti sellaisia, että salasanaa näpytellessäsi kirjoittamasi merkit eivät näy vaan tilalla näkyy esimerkiksi tähtiä (*), niin näppäilyistäsi voidaan yleensä aika helposti nähdä, mikä salasana on. Itse asiassa tästä käyttöliittymien piirteestä on siis ehkä enemmän harmia kuin hyötyä! Se luo harhakuvaa turvallisuudesta mutta vaikeuttaa salasanan kirjoittamista. Ja mitä useammin joudut sen kirjoittamaan, sitä isompi on riski, että joku näkee.

Salasanan tallennus tuo käyttömukavuutta - myös väärinkäyttäjälle

Usein on mahdollista tallentaa salasanoja esim. erilaisiin yhteydenotto-ohjelmiin niin, että ne tarvitsee kirjoittaa vain kerran, ja seuraavalla käyttökerralla ohjelma osaa sitten lähettää ne omia aikojaan. Vaikka tällainen kiistatta parantaa käyttömukavuutta, siihen on syytä suhtautua *erittäin* varauksellisesti, etenkin, jos talletus on sellainen, että salasana säilyy, vaikka kone sammutetaan.

Eri salasanat eri järjestelmiin

Yleensä ei pidä käyttää eri järjestelmissä samaa salasanaa. Syynä on muun muassa se, että tällöin yhden murtuminen ei anna murtajille pääsyä kaikkiin järjestelmiin. Onhan aika ilmeistä, että murtaja saattaa ruveta kokeilemaan löytämäänsä "avainta" muihinkin lukkoihin.

Salasanojen vaihtaminen

Salasana pitäisi vaihtaa säännöllisesti, muutaman kuukauden välein, tai useamminkin, jos asiasta on annettu sellaiset ohjeet. Tunnusta ja salasanaa saadessaan kannattaa etsiä ohjeet siitä, miten vaihtaminen tehdään.

Vaihtamisen yksi syy on se, että murtautujat usein hankkivat käyttöönsä tunnuksia "varastoon" tai käyttävät murtamiaan tunnuksia vain vähän, jottei murto tulisi ilmi. Kun salasanaa vaihdetaan silloin

tällöin, rajoitetaan murtojen vaikutuksia, Lisäksi jos joku pyrkii murtamaan jonkin erityisen tunnuksen järjestelmällisellä, hyvin pitkään jatkuvalla salasanojen kokeilulla tai vastaavalla menetelmällä, niin salasanan vaihtaminen kesken kaiken haittaa puuhaa melkoisesti.

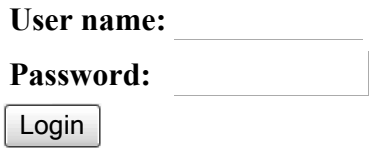
Miten selvitä kymmenien salasanojen kanssa?

Yllä esitetty voi tuntua epärealistiselta: pitäisi olla luonnottomia salasanoja, aina eri salasana eri järjestelmissä, ja salasana pitäisi vaihtaa usein, mutta mitään ei saisi kirjoittaa muistiin. Se koskeekin ensisijaisesti "oikeita" salasanoja kuten tietokonejärjestelmän tai paikallisverkon salasanaa, sähköpostin salasanaa, tietokantajärjestelmän käyttäjän salasanaa, maksullisen palvelun salasanaa tms.

Suhteellisuudentajua tarvitaan: salasanojen tärkeys vaihtelee suuresti sen mukaan, mitä salasanalla voi tehdä. Nykyisin on myös monia järjestelmiä, jotka vaativat käyttäjäksi ilmoittautumisen ja salasanan, jotta pääsisi vaikkapa lukemaan verkossa olevaa sanomalehteä. Jos kyseisen oikeuden saa kuka hyvänsä, kunhan ilmoittaa omat tietonsa, ei tällaisen salasanan vuotaminen ole ollenkaan niin vakava asia kuin "oikean" salasanan vuotaminen. Niinpä voidaankin ehkä tyytyä alempaan tietoturvan tasoon niiden kohdalta.

Esimerkiksi saman salasanan käyttö eri ilmaispalveluissa voi olla käytännöllinen ratkaisu, joka antaa enemmän voimavaroja turvata salasanojen laatu siellä, missä se on olennaisinta. Sellaisen salasanan ei tietenkään pidä olla sama kuin jokin "oikea" salasanasi! Tämä on tärkeää senkin takia, että sellaisten palveluiden ylläpitäjät eivät aina suhtaudu kovin vakavasti palveluidensa salasanoihin vaan saattavat esimerkiksi lähettää niitä suojaamattomassa sähköpostissa tai kertoa niitä kenelle tahansa, joka vähänkin vakuuttavasti kertoo unohtaneensa oman salasanansa.

Mikä ohjelma kysyy salasanaasi?



Kun ruudulle ilmestyy pyyntö kirjoittaa salasanasi, varmista, että olet todella kirjautumassa *oikeaan järjestelmään*. Halusitko todella käyttää sitä vai hyppäsikö se omia aikojaan silmille? Etenkin jälkimmäisessä tapauksessa se voi olla huijausta. Ehkä sinut vain yritetään saada antamaan jokin tärkeä tunnus ja salasana niin, että luulet meneväsi johonkin tuttuun järjestelmään mutta todellisuudessa vain annat ne niitä keräilevälle ohjelmalle.

On helppoa rakentaa ohjelma, jonka käyttö *näyttää* yhteydenotolta johonkin järjestelmään pieniä yksityiskohtia myöten mutta joka onkin vain huijarin kehitelmä salasanojen keräämiseksi. Vältä epätavallisia yhteydenottokehotteita ja ilmoita niistä heti lähimmälle turva-asiantuntijalle. Jos huomaat mitä tahansa outoa kirjautuessasi johonkin järjestelmään, vaihda salasanasi.

Pidä salasanasi omanasi

Salasanojen tulisi olla henkilökohtaisia, ei esimerkiksi työryhmäkohtaisia. Jos suinkin mahdollista, älä suostu järjestelyihin, joissa joutuisit käyttämään samaa tunnusta ja salasanaa kuin joku toinen. Siitä seuraa tietoturvariskien lisäksi muitakin ongelmia. Joudutaan ehkä kuluttamaan aikaa sen selvittämiseen, kuka on jonkin asian tehnyt, ja seuraa sotkuja, jos joku vaihtaa tunnuksen salasanan kertomatta siitä muille.

Salasanan antaminen "pikku hommaan" voi olla iso ongelma

Salasanaa ei pidä antaa *tilapäisestikään* tai yhtä "pikku hommaa" varten toisen käyttöön. Jos annat tavallisen käyttäjätunnuksen salasanasi toiselle, jotta hän voisi lukaista yhden tiedostosi sisällön, annat hänelle mahdollisuuden lukea myös kaikki muut ynnä hävittää ne. Vaikka hän ei ehkä missään tapauksessa haluaisi tehdä niin, vahinkoja voi sattua. Monissa järjestelmissä on aivan liian helppoa hävittää tai turmella suuri määrä tietoja, ja varsinkin järjestelmää tuntematon saattaa tehdä niin tietämättään.

Älä hätäile, äläkä varsinkaan toimi hätiköidysti

Huolestu kummallisuuksista, mutta älä hätäänny

Jos huomaat, että tiedostosi ovat muuttuneet oudosti, tai on ilmestynyt omituisia tiedostoja tai levytilaa on salaperäisesti kadonnut tai on aihetta epäillä, että joku on luvatta käyttänyt konettasi tai käyttäjätunnustasi, tai jotain näyttäisi muutoin olevan hullusti, on syytä *huolestua*. Mutta ei hätääntyä.

Hätäily voi tehdä pienestä tietoturvaongelmasta ison. Se voi esimerkiksi hävittää murtojälkiä, tuhota vioittuneen tiedoston lopullisesti tai avata kokonaan uusia aukkoja turvallisuuteen.

Etsi apua

Kun vakavia tietoturvaongelmia tai sellaisiin viittaavia oireita on ilmennyt, pyri ensi tilassa ottamaan *yhteys asiantuntijaan*, ja yritä rauhallisesti selvittää, mistä on kyse. Normaaleista tietokoneen käytön pulmista kannattaa toki yrittää itse selvitä ohjeiden ja käsikirjojen avulla. Jos tekstinkäsittelyohjelmassasi kaikki teksti näkyy lihavana, syynä on luultavammin jokin näppäilyvirhe tai vastaava ongelma ohjelman käytössä, ei tietomurto tai virus.

Kirjoita muistiin, mitä tapahtui

Ellet saa asiantuntijaa ihan saman tien paikalle, kirjoita muistiin, mitä olit tehnyt (mm. mitä ohjelmaa käyttänyt ja miten) ja mitä tapahtui. Ongelmien selittäminen on muutenkin vaikeaa, mutta sitten kun on unohtanut olennaisia asioita, se alkaakin olla mahdotonta.

Ota järjestelmän mahdollisen virhe- yms. ilmoituksen teksti talteen *sanatarkasti*. Usein asiantuntijakin joutuu tekemään hakuja tietokannoista löytääkseen selityksen, ja silloin pienikin kirjoitusvirhe merkitsee. (Järjestelmän joissakin tilanteissa virheilmoitustekstin jälkeen tulostamat monen rivin mittaiset ns. vedokset, jotka ovat täynnä numerotietoa, eivät sen sijaan useinkaan ole hyödyksi.)

Hanki tietoa

Perustiedot tietotekniikasta auttavat monessa asiassa. Tietoturvaakin parantaa merkittävästi se, että tuntee tietotekniikkaa yleisesti, jolloin on parempi perusta, jolle tietoturvatiedotkin voi rakentaa. Hätiköinti ja hämääntyminen johtuvat paljolti siitä, ettei ymmärretä, mitä on tapahtunut tai tapahtumassa, ja silloin helposti kuvitellaan, että kunhan tekee *jotakin* ja äkkiä, se auttaa.

Monellakin on kyllä paljon tietoja tietotekniikasta, mutta jotkin osa-alueet ovat saattaneet jäädä tuntemattomiksi tai, mikä pahempaa, harhakuvien varaan. Kannattaakin harkita mm. *Tietokoneen ajokortin* suorittamista. `<http://www.tieke.fi/ajokortti/>` Sen oppisisältöihin voi tutustua ja niitä voi kerrata *ATK-ajokorttikoulun* sivuilta. `<http://www.atk-ajokorttikoulu.net>`

Varo vääriä varoituksia ja huijausta

Pelkät *aiheettomat varoituksetkin* aiheuttavat vahinkoa. Jos olet kuullut jostakin uhkasta ja rupeat levittämään siitä tietoa, voi käydä, ettei se olekaan tietoa vaan luuloa tai suorastaan sumutusta, ja muut ihmiset sitten hätääntyvät ja tekevät hätiköidessään vahinkoa. Lisäksi jokainen turhaksi osoittautuva varoitus turruttaa ihmisiä: kun sitten susi oikeasti tulee, sitä pidetäänkin taas yhtenä turhana varoituksena.

Älä levitä virusvaroituksia

Jos saat virusvaroituksen, jossa kehotetaan levittämään sanaa kaikille tuntemillesi, älä tee niin. Jätä viruksista varoittaminen tietoturva-asiantuntijoiden tehtäväksi. Liikkeellä on hyvin paljon vääriä varoituksia. Useimmiten voit tarkistaa ns. hoax warnings -listasta, että kyse on sellaisesta. `<http://www.f-secure.com/news/hoax/>` Jos et, ota yhteys lähimpään turva-asiantuntijaan, joka pystyy. Muista myös yleisemmin, että paljon ihmisiä erehdytetään levittämään väärää tietoa hyvässä tarkoituksessa.

Huijaukset

Erilaiset huijausyritykset, joita edellä 1. luvussa käsiteltiin melko laajasti, perustuvat usein siihen, että viestin vastaanottaja yritetään saada toimimaan *heti*. "Toimi saman tien, tarjous on voimassa vain hetken!" "Soita heti, vain 50 ensimmäistä pääsee mukaan!" "Noudata neuvoa heti, muuten tiedostosi tuhoutuvat!" Voidaan siis hyvinkin vedota tietoturvaan, kun tosiasiallinen tarkoitus on murtaa se.

Muista, että *vähänkin epämääräisestä* lähteestä tuleva viesti on hyvin epäilyttävä varsinkin, jos siinä kehotetaan *pikaisuuteen*.

Ota talteen kaikki tarpeellinen, ennen kuin vahinko sattuu

Tallentele

Kun käytät esimerkiksi tekstinkäsittely- tai taulukkolaskentaohjelmaa, tallenna välillä työsi levylle. Sama koskee myös esimerkiksi pitkän sähköpostiviestin kirjoittamista. Muutoin saattaa sähkökatkos, järjestelmävirhe, verkkoyhteyden katkeaminen tai muu syy hävittää tekemäsi työn. Useimmat ohjelmat nimittäin pitävät käsiteltävää aineistoa vain tietokoneen keskusmuistissa, josta se täysin tuhoutuu, jos vaikkapa vain joku vahingossa kiskaisee töpselin irti. Tallennustoiminto, nimeltään usein "Save", ottaa aineiston talteen myös kovalevylle. Esimerkiksi ruokatunnille lähdettäessä kannattaa ehdottomasti "seivata" kaikki aineistot, joita on tekemässä tai muokkaamassa jossakin ohjelmassa.

Useissa ohjelmissa on mahdollisuus myös *automaattisiin* tallennuksiin esimerkiksi kymmenen minuutin välein. Ominaisuus kulkee usein nimellä "auto-save", ja se on ehkä erikseen kytkettävä toimintaan ohjelman asetuksista. Sellaisia mahdollisuuksia kannattaa yleensä käyttää hyväksi etenkin ohjelmissa, joita käyttää paljon. Esimerkiksi MS Wordissä automaattinen tallennus saattaa valmiiksi olla käytössä, mutta on hyvä tarkistaa asia, ja samalla voi valita omaan työtyyliinsä sopivan tallennusvälin. Esim. suomenkielisessä versiossa asetus voi olla seuraavien valintojen takana: Työkalut > Asetukset... > Tallenna.

Teknisesti sanottuna aineisto on ohjelman käytön aikana *sähköilmiöihin* perustuvassa muodossa tietokoneen keskusmuistissa, ja siksi se katoaa, kun sähkö katkeaa. Levyllä tai levykkeellä se on *magnetoitumiseen* perustuvassa muodossa ja säilyy siksi paremmin.

Kannattaisiko turvata sähkönsaanti?

Sähkökatkoja ja -häiriöitä vastaan voidaan suojautua ns. UPS-laitteilla, joilla pyritään takaamaan jatkuva, häiriötön sähkövirran saanti. Sellainen laite kytketään tietokonelaitteiden ja sähköverkon väliin eli sähkövirta tulee UPS:n läpi. Laitteessa on akusto, josta se antaa virtaa jonkin aikaa sähköjen katkettua. Tämä voi antaa mahdollisuudet siihen, että verkkovirran katkettua ehditään tallentaa tiedot ja sammuttaa tietokone hallitusti. UPS-laitteita on erilaisia, ja monet niistä on rakennettu lisäksi huolehtimaan virran tasaisuudesta, etenkin estämään "piikkejä", jotka saattavat aiheuttaa pahoja häiriöitä tietolaitteistoille. Pienen UPS:n saa alle tuhannella markalla, ja se saattaa olla tarpeellinen hankinta myös kotiin ja pienyritykseen etenkin alueilla, joilla sähkösyötössä esiintyy usein häiriöitä. Lisätietoja on esim. *Haamuraja*-sivuston jutussa *Suojaa ukkoselta*. <http://www.haamuraja.com/artikkelit/ups/>

Kannattaisiko pitää vanhakin versio tallessa?

Usein on syytä ottaa talteen useita versioita aineistoista, esimerkiksi tekemällä aineistosta kopion eri nimelle, ennen kuin rupeaa muokkaamaan sitä. Näin varsinkin silloin, kun on aihetta epäillä, että muutos ehkä joudutaan perumaan. Voi olla, että loistava idea jonkin asiakirjan sisällön uusimiseksi osoittautuukin huonoksi.

Varmuuskopiointi auttaa

Varmuuskopiointi vähentää tuhojen vaikutusta

Vaikka tiedot normaalisti säilyvätkin kovalevyllä, on syytä lisäksi tehdä varmistuksia eli kopioida tärkeimmät aineistot kovalevyltä esimerkiksi levykkeille. Varmuuskopioinnin yksi tarkoitus on huolehtia siitä, ettet menetä työsi tuloksia, jos kovalevy lakkaa toimimasta tai jos vahingossa hävität tiedoston. Nykyisin levytila on halpaa mutta ei kovin luotettavaa. Kovalevyn meneminen jumiin niin, että sieltä ei voi normaalein keinoin pelastaa tiedostoja, ei valitettavasti ole kovinkaan harvinaista. Itse asiassa on lähes jokaiselle tietokonetta säännöllisesti käyttävälle käy niin jossain vaiheessa vuosien saatossa.

Varmuuskopiointi on myös olennaista tietomurtoihin ja haittaohjelmiin varautumiseksi. Yksi haittaohjelmien tavallisimmista tihutöistä on juuri tietokoneen kovalevyn sisällön hävittäminen, koska se on erityisen vahingollista ja toisaalta helppoa ohjelmoida.

Varmuuskopioi ennen muuta omat tietosi

Ota lisäksi varmuuskopioita *omista tietoaineistoistasi*, esimerkiksi itse kirjoittamistasi asiakirjoista, eli tallenna ne kovalevyn lisäksi esimerkiksi levykkeille. Hanki tarpeeksi levykkeitä tai muita tietovälineitä. Uutta tietokonetta ostettaessa kannattaa ehkä sijoittaa vähän ylimääräistä, jotta saa siihen kirjoittavan CD-rom-aseman tai vastaavan, jolla isonkin tietomäärän saa kopioiduksi kohtuullisessa ajassa.

Jos kovalevystä on täydellinen varmuuskopio, niin esimerkiksi levyrikon jälkeen on paljon helpompi toimia. Mutta yleensä ei kannata yrittää kopioida koko kovalevyn sisältöä, koska sitä on niin paljon siellä on paljon sellaista, joka voidaan asentaa uudestaan alkuperäisiltä tietovälineiltä tai hakea uudestaan Internetistä.

Varmista varmuuskopioinnin säilyvyys

Varmuuskopiot on hyvä *suojata* vahingossa tapahtuvalta hävittämiseltä tai päällekirjoittamiselta. Varmuuskopiolevyke kannattaa kirjoitussuojata napsauttamalla tähän tarkoitettu nipsu levykkeessä

oikeaan asentoon. Kovalevylle tehdyn varmuuskopion voi yleensä suojata käyttöjärjestelmäkohtaisella tavalla niin, että lukeminen on mahdollista, kirjoittaminen (ja hävittäminen) ei. Tällaisen suojauksen voi tiedoston "omistaja" ohittaa, mutta sen asettaminen suojaa *vahingossa* tapahtuvalta hävittämiseltä.

Palvelinvarmistus

Usein kätevä keino on tallentaa aineisto paitsi omaan tietokoneeseen myös johonkin *palvelimeen*, esimerkiksi lähiverkon tiedostopalvelimeen taikka Web-palvelimeen. Muista toisaalta, että silloin aineistot voivat joutua muidenkin tietoon kuin on tarkoitus. Erityisesti Web-palvelimeen tallentaminen tulee kyseeseen lähinnä vain silloin, kun erityisesti haluat aineiston julkiseksi.

Kaksi kopioita tärkeästä, kolme tärkeimmästä

Kaikesta tärkeästä aineistosta tulisi olla *kaksi* toisistaan riippumatonta kopiota. Varmuuskopio levykkeellä (kovalevyllä olevan varsinaisen tiedoston lisäksi) täyttää tämän vaatimuksen niukin naukin. Tällöin on erityisen tärkeää *säilyttää* levykkeet hyvin, sillä pöly, lika, magneettikentät, lämpö ja kuluminen voivat tehdä levykkeen vähitellen käyttökelvottomaksi.

Paperituloste voi olla hyödyllinen lisävarmistus. Tietojen palauttaminen paperilta tietokoneella luettavaan muotoon on kuitenkin työlästä, vaikka tuloste olisikin hyvin säilynyt.

Kaikesta todella tärkeästä on hyvä olla vähintään kolme kopiota, niistä ainakin yksi fyysisesti turvatussa paikassa, mielellään eri rakennuksessa.

Tee oma varmuuskopiointipolitiikkasi

Mieti oma varmuuskopiointisuunnitelmasi. Selvitä aluksi, onko toimintaympäristössäsi jokin yleinen automaattinen varmuuskopiointi, joka huolehtii *osasta* varmistustarpeita. Isossa yrityksessä näin todennäköisesti on, mutta varmuuskopiointi koskee todennäköisesti vain niitä tiedostoja, jotka on sijoitettu määrättyihin palvelimiin tai hakemistoihin.

Harkitse, miten usein teet laajan varmuuskopion (tai ehkä jopa täydellisen, jos se on mielekästä) ja miten usein otat talteen vain erityisen tärkeät tai usein muuttuvat tiedostot. Tilanne on verrattavissa *vakuutuksen ottamiseen*: maksamalla vakuutusmaksun (huolehtimalla varmuuskopioinnista) hyväksyt varman rahanmenon (vaivannäön), jotta välttäisit suhteellisen epätodennäköisen mutta *ison* menetyksen tai saisit sen jotenkin korvatuksi. Asiaa voi miettiä näin päin: kuinka suuren osan tekemästäsi työstä haluat tuhoutuvan, *kun* vahinko sattuu? Jos et halua menettää yli viikon työn tuloksia, ota varmuuskopio vähintään kerran viikossa.

Mitä vakuutuksiin tulee, niin mikään vakuutus ei yleensä korvaa tiedostojen tuhoutumista, jos tietokone varastetaan, vaurioituu tulipalossa tms. Esimerkiksi kotikäyttäjän kannattaa huolehtia siitä, että tietokonelaitteet ovat kotivakuutuksen piirissä, mutta sellainen vakuutus korvaa vain aineellisia vahinkoja ja nekin yleensä laskennalliset kuoletukset huomioon ottaen.

Käytä ajantasaisia viruksentorjuntaohjelmia ja muita turvajärjestelmiä

Edellä kohdassa *Ohjelma on muutakin, kuin miltä näyttää* mainittiin lyhyesti virukset ja muut haittaohjelmat. Tässä käsitellään virusten torjunnan käytäntöä sekä muita turvajärjestelmiä.

Viruksentorjunta

Helpompaa kuin moni luulee

Virusten torjuntaan on saatavilla ohjelmia osittain maksutta, osittain kohtuulliseen hintaan tai esimerkiksi tietokonepaketin osana. Ne ovat melko helppoja ja vaivattomia käyttää. Ongelmana on lähinnä se, että käyttäjät eivät useinkaan huolehdi ohjelman pitämisestä ajan tasalla tai eivät *käytä* viruksentorjuntaohjelmaa.

Monissa tapauksissa päivityksistä ei tarvitsekaan huolehtia, jos ohjelma on valittu ja asennettu hyvin ja käytössä on kiinteä Internet-yhteys, jonka kautta ohjelma ehkä automaattisesti käy hakemassa päivitykset tietokantoihinsa esimerkiksi viikoittain.

Jos kiinteää yhteyttä ei ole eli käytännössä jos ollaan tavallisen modeemiyhteyden varassa, on käyttäjän itsensä huolehdittava päivityksistä. Huolehtiminen tarkoittaa esimerkiksi sitä, että aina kuun alussa ja muulloinkin, kun on kuullut uusia viruksia olevan liikkeellä, käynnistää viruksentorjuntaohjelmansa toiminnon, jolla se päivittää tietokantansa verkosta.

Vastaavasti voidaan viruksentorjuntaohjelma ehkä asettaa käynnistymään automaattisesti koneen käynnistyessä ja toimimaan koko ajan taustalla. Kuitenkin on syytä automaattitarkistusten lisäksi erikseen tarkistaa "käsin" (manual check) ainakin *ohjelmatiedostot* ennen ohjelman asentamista.

Selvitä, miten viruksentorjunta on järjestetty

Selvitä, mitä periaatteita ja käytäntöjä viruksentorjunnassa sovelletaan työpaikallasi, oppilaitoksessa tai muussa organisaatiossa, jossa toimit. Parhaassa tapauksessa saat täsmälliset toimintaohjeet, joiden noudattaminen ei paljoa vaadi. Käytäntöihin voi sisältyä keskitetty viruksentorjuntaohjelmien päivittäminen taikka se, että tarvittavista päivityksistä tiedotetaan paikallisesti. Tämä voi ratkaisevasti helpottaa tietoturvaasi sekä auttaa sinua antamaan oma panoksesi yhteiseen tietoturvaan.

Joudut ehkä itse järjestämään viruksilta suojautumisesi, esimerkiksi kun kyse on kotikoneestasi. Huomaa kuitenkin, että organisaation solmima yhteislisenssi viruksentorjuntaohjelmasta kattaa usein myös käytön henkilöstön kotikoneissa, ja tällöin voit siis käyttää samoja ohjelmia ja osittain samoja menettelytapojakin.

Torjuntaohjelma tunnistaa viruksia, mutta ei kaikkia niistä

Viruksentorjuntaohjelmien toiminta perustuu monessa suhteessa virusten tunnistamiseen erilaisilla menetelmillä, jotka on kehitetty viruksista saatujen käytännön kokemusten perusteella. Tästä seuraa, että kun tulee uusi virus, torjuntaohjelmat eivät ehkä heti havaitse sitä.

Ohjelmia kehittävät yritykset kyllä toimivat nopeasti ja panevat jakeluun uuden version, joka osaa tunnistaa ja hoidella uudenkin viruksen. Mutta tästä ei ole mitään hyötyä niille, jotka eivät sitä versiota itselleen hanki ja ota käyttöön. Lisäksi viruksen tuoma uhka on suurin alkuvaiheessa, kun se tuntemattomuutensa ansiosta leviää nopeasti. Siksi torjuntaohjelmien tietokantojen päivittäminen on niin tärkeää.

Jos virus havaitaan, kerro siitä - harkitusti

Jos viruksentorjuntaohjelma ilmoittaa, että järjestelmässäsi on ongelma, kerro asiasta sekä lähimmälle tietoturvahenkilölle organisaatiossasi että niille ihmisille, jotka ovat saattaneet tietämättään välittää viruksen sinulle - he nimittäin muuten luultavasti levittävät sitä edelleen. On tärkeää pysyä rauhallisena. Se, että ihmiset säikähtävät viruksia ja sen takia toimivat hätiköidysti, voi aiheuttaa enemmän viivästystä ja sekaannusta kuin itse viruksen hyökkäys.

Ota huomioon, että viruksen havaitsemisen hetki voi olla aivan toinen kuin virustartunnan saamisen hetki. Eroa voi olla kuukausia, jos ei käytetä ajantasaisia viruksentorjuntaohjelmia. Jotkin virukset ovat "aikapommeja", jotka rupeavat toimimaan esimerkiksi määräpäivänä tai määrätyn ohjelman käynnistyessä. Virus voi myös tehdä tihutöitään hitaasti, niin että sen vaikutusta esimerkiksi levytilan vähittäisenä syöjänä on vaikea erottaa tilan normaalista täyttymisestä. Ovela virus voi yksinkertaisesti muuttaa järjestelmän asetuksia ja sitten piiloutua.

Jos on aihetta epäillä, että tietokoneessasi on virus tai muu haittaohjelma, on syytä ensin irrottaa se kaikista verkoista paitsi sähköverkosta. Muussa tapauksessa on vaara, että haittaohjelma levittää itseään verkon kautta muihin koneisiin, ennen kuin ehdit paikantaa ja poistaa sen.

Haittaohjelmia on muitakin kuin viruksia

Alun perin viruksiksi kutsuttiin vain pieniä ohjelmanpätkiä, jotka kopioivat itseään "isäntäohjelmasta" toiseen. Taustalla oli rinnastus biologiasta tuttuihin viruksiin. Sittemmin on tietokoneviruksiksi ruvettu kutsumaan hyvinkin monenlaisia haitallisia tai ainakin harmillisia ohjelmia. Nekin saattavat levitä nopeasti mutta eivät varsinaisten tietokonevirusten tapaan vaan esimerkiksi vain siten, että ihmiset lähettelevät niitä toisilleen ymmärtämättä, mitä ne todella tekevät.

Haittaohjelmien luokittelu ja ominaisuuksien erittely on tärkeää torjuntaohjelmien tekijöille, mutta tavallista käyttäjää se lähinnä hämmentää. Hämmennystä voi aiheuttaa myös tässä käytetty yleisnimitys "haittaohjelma", sillä kaikki haittaohjelmat eivät suinkaan tee haittaa tai eivät ainakaan näytä tekevän, ja toisaalta jotkin tekevät niin paljon tuhoa, että haitta-sana tuntuu vähättelyltä.

Olennaista on ensinnäkin se, että niin sanotut viruksentorjuntaohjelmat tehoavat hyvin monenlaisia haittaohjelmia vastaan, eivät vain varsinaisia viruksia. Toiseksi on olennaista, että mitkään niistä eivät tehoa *kaikenlaisia* haittaohjelmia vastaan. Kuka tahansa ohjelmoinnin alkeiskurssin suorittanut voi tehdä ohjelman, joka saa aikaan vahinkoa tai ainakin harmia; itse asiassa niin usein käy yrittämättäkin. Jos sitten sellaista ohjelmaa levitetään, niin tuskin mikään viruksentorjuntaohjelma huomaa mitään erikoista. Jos ohjelmaa levitetään laajasti, niin sitten joku torjuntaohjelman tekijä ehkä lisää ohjelmaansa koodin, jolla haittaohjelma tunnistetaan.

Viruksentorjuntaohjelmien käyttö on siis välttämätöntä, mutta ei riittävää.

Kaikki ongelmat eivät ole haittaohjelmien aiheuttamia

Kun tietoisuus tietokoneviruksista on levinnyt, on samalla syntynyt harhakäsityksiä siitä, mitkä kaikki ongelmat ovat virusten tai muiden haittaohjelmien aiheuttamia. Suurin osa kaikista ongelmista tietokoneiden käytössä johtuu jostakin muusta. Käyttäjä on ehkä huomaamattaan muuttanut jonkin ohjelman asetuksia niin, että se toimii oudosti. Tai kun kone tuntuu olevan "tukossa", syynä on ehkä vain se, että ollaan tekemässä jotain Internet-yhteydessä ja yhteys tai toisessa päässä oleva palvelin on ruuhkainen.

Palomuurit

Palomuuri rajoittaa vahinkoja

Peruskäyttäjänkin saattaa olla aiheellista asentaa ja ottaa käyttöön muitakin tietoturvaa parantavia ohjelmia ja järjestelmiä. Tavallisimmin tulee kyseeseen ns. palomuuri (firewall) eli järjestelmä, joka pyrkii rajaamaan Internetin ja oman koneen tai paikallisverkon väliset yhteydet turvallisiksi ja valvotuiksi. Ensisijaisesti tämä tarkoittaa, että mitä tahansa Internetistä päin tulevaa tietoliikennettä ei oteta vastaan. Tyypillinen henkilökohtainen tietokone sisältää monenlaisia tietoturva-aukkoja tässä suhteessa, ellei niitä erikseen tukita.

Palomuureilla ei ole mitään tekemistä tulipalojen kanssa. Sana on käännöslaina, ja nimityksen taustalla on vain ajatus jostakin, joka rajoittaa vahinkojen leviämistä.

Riskit ovat sitä suurempia, mitä kiinteämpi Internet-yhteys koneessa on. Esimerkiksi ADSL-yhteyden tai kaapelimodeemin käyttäjän on syytä olla enemmän varuillaan kuin tavallisen modeemin käyttäjän. Yhteydentarjoaja ehkä kertoo, että se on toteuttanut palomuurin niin, ettei käyttäjien tarvitse asiasta huolehtia, mutta todellisuudessa sellainen palomuuri ei välttämättä tarjoa riittävää turvaa.

Kotikäyttäjäkin voi tarvita

Isoissa organisaatioissa palomuuri toteutetaan usein niin, että lähiverkon ja Internetin välinen liikenne kulkee erillisen palomuuritietokoneen kautta. Kotikäyttäjälle realistinen vaihtoehto on omaan koneeseen asennettava palomuuriohjelmisto. Jos harkitaan fyysistä palomuuria, on syytä tarkistaa, sallivatko yhteydentarjoajan sopimusehdot sen.

Palomuuriohjelmistoja on useisiin tilanteisiin (yksityiskäyttöön) saatavissa maksuttominakin, mm. seuraavat:

- ZoneAlarm `<http://www.zonelabs.com>`
- Tiny Personal Firewall `<http://www.tinysoftware.com/>`
- Sygate Personal Firewall `<http://www.sygate.com/products/shield_ov.htm>`

Palomuuriohjelma toimii ikäänkuin oman koneesi ja Internetin välisenä portinvartijana molempiin suuntiin. Sillä voi estää sen, että järjestelmääsi päässeet haittaohjelmat ottavat omia aikojaan yhteyden verkkoon. Sillä voi myös torjua niin kutsutun porttiskannauksen (port scanning), jossa vakoilevat koneet etsivät järjestelmällisesti mahdollisuuksia päästä sisään verkossa oleviin koneisiin.

Windows XP sisältää itsessään palomuuriohjelmiston, mutta se ei tarjoa yhtä kattavaa suojaa kuin edellä mainitut.

Palomuuri vaatii osaamista mutta ei ruudin keksimistä

Palomuuriohjelman asentaminen ja käyttö vaatii jonkin verran teknistä osaamista. Asioita tuntematon helposti asettaa turva-asetukset liiankin tiukoiksi ja sitten ihmettelee suurta määrää aiheettomia hälytyksiä. Lisäksi palomuurin ideaan kuuluu, että kun jokin omassa koneessa käynnistettävä ohjelma yrittää ottaa yhteyden Internetiin, palomuuri kysyy käyttäjältä lupaa tähän. Käyttäjän pitää silloin osata arvioida, mistä on kysymys, ja sallia yhteydet tarvittaessa. Tämä ei ole niin työlästä kuin voisi luulla, sillä sellaisen oikeuden voi antaa pysyvästi joillekin ohjelmille. Ymmärrettävästi ainakin Web-selaimelle on syytä antaa oikeus verkkoyhteyksiin!

Palomuuriohjelman mukana tulee yleensä melko hyvä englanninkielinen ohjeisto. Jos kieli tuottaa vaikeuksia tai tulee muita ongelmia, saat ehkä apua asiantuntevalta, luotettavalta tuttavalta.

Roskapostin suodatus

Roskaposti (spämmi, *spam*) koetaan usein niin vakavaksi ongelmaksi, että sitä vastaan pyritään suojautumaan ns. suodattimilla (*filters*). Ne yritetään tehdä sellaisiksi, että ne automaattisesti heittävät roskat pois eli hävittävät roskapostin tai (tavallisemmin) siirtävät sen normaalista saapuneiden viestien kansiosta erilliseen kansioon, jolloin vastaanottajan ei tarvitse nähdä roskapostia.

Roskaposti sinänsä ei yleensä ole varsinainen tietoturvaongelma, mutta virheelliset yritykset torjua

sitä voivat horjuttaa tietoturvaa! Roskapostin mukana saattaa tulla viruksia, mutta niitä vastaan auttaa normaali viruksentorjunta. Ja roskapostin runsaus voi aiheuttaa sen, että asiallisiakin viestejä luullaan roskapostiksi ja jätetään siis käsittelemättä. Mutta roskapostin suodatus saattaa pahentaa ongelmia, jos se tehdään väärin: jopa yhden merkin virhe suodatusta määriteltäessä jopa aiheuttaa sen, että suodatus toimii tasan väärin päin, eli roskiin menevätkin asialliset viestit. Kannattaa siis harkita, missä määrin roskapostista on niin paljon todellista kiusaa, että kannattaa ottaa käyttöön automaattipuolustus sitä vastaan.

Jos roskaposti on sinulle iso ongelma, kannattaa ehkä kääntyä luotettavan asiantuntijan puoleen, jotta hän rakentaisi sinulle suodatuksen. Lisäksi isoissa organisaatioissa on käytössä yleinen suodatus, joka joillakin teknisillä perusteilla suodattaa pois roskapostia. Mutta omienkin suodattimien tekeminen on kyllä mahdollista.

Roskapostia ja muita vastaavia ongelmia sekä ratkaisuja niihin käsittelee Kai Puolamäen sivusto *Ei-toivottu viestintä Internetissä*. `<http://www.iki.fi/kaip/spam/>`

Selvitä itsellesi oman organisaatiosi tietoturvajärjestelyt

Organisaatioita on monenlaisia

"Organisaatio" voi tässä tarkoittaa erilaisia asioita tilanteen mukaan: työnantajaasi, jos käytät tietokonetta työssäsi; oppilaitostasi, jos käytät sen tietokoneita; Internet-yhteydentarjoajaasi, jos esim. olet kotikäyttäjä. Ota huomioon, että osa sellaisen organisaation tietoturvajärjestelyistä saattaa olla sinua *virallisestikin velvoittavia* esimerkiksi työsuhteen tai muun tekemäsi sopimuksen perusteella. Jos esimerkiksi käytät kotitietokonettasi työasioihin, niin sinun on otettava huomioon sekä työpaikkasi että Internet-yhteydentarjoajan tietoturvajärjestelyt - tai niiden puute.

On realistista lähteä siitä, että Internet-yhteydentarjoajalta ei ole paljoakaan apua saatavissa, ainakaan asioissa, jotka eivät suoranaisesti liity yhteyden teknisiin kysymyksiin. Yhteydentarjoajat mahdolliset tietoturvasivut kannattaa kuitenkin etsiä ja ainakin vilkaista läpi.

Millaiset turva-asiat on syytä selvittää itselleen?

Tietoturvajärjestelyt voivat koskea *esimerkiksi* seuraavia asioita:

1. kehen on otettava yhteys, kun ilmenee tietoturvaongelmia
2. millaisia *salasanojen* tulee olla ja miten usein ne on vaihdettava
3. mitä ohjelmia (esim. viruksentorjuntaohjelmia ja salakirjoitusohjelmia) *pitää* käyttää ja miten
4. mitä ohjelmia *ei saa* käyttää niiden tietoturvariskien takia
5. millaisia *asetuksia* (konfigurointeja, *settings*) ohjelmissa pitää käyttää
6. mihin tarkoituksiin tietokonetta ja sen eri käyttömuotoja ylipäänsä saa käyttää, esim. millaisia tietoja ei saa lähettää yleisen verkon kuten Internetin kautta
7. mitä *tiedostomuotoja* saa käyttää sähköpostissa
8. millaisia *säännöllisiä tarkistuksia* ja muita turvatoimia (esim. varmuuskopiointeja) käyttäjien pitää tehdä
9. minne käyttäjien tulee tallentaa omat tiedostonsa
10. onko yleinen varmuuskopiointi järjestetty ja miten.

Järjestelyt vaihtelevat, osa voi olla salaista

Turvajärjestelyjen luonne ja yksityiskohtaisuus vaihtelee suuresti. Esimerkkinä osittain varsin

yksityiskohtaisista ohjeista voidaan mainita Turun yliopiston tietoturvasivut, joilla on mm. tarkkoja ohjeita suojatoimenpiteistä tietomurtotapauksissa. <http://www.cc.utu.fi/tietoturva/>

Etenkin kaupallisissa yrityksissä tietoturvaan liittyy usein seikkoja, joiden takia sen järjestelyjä ei haluta kertoa julkisesti. Organisaatiosi *julkisesti* esittämä ei yleensä kerro kaikkea, mikä sen sisällä toimivien tulisi tietää. Sinun on luonnollisestikin varottava kertomasta ulkopuolisille oman organisaatiosi tietoturva-asioista seikkoja, jotka voisivat murtautujan korviin kantauduttuaan olla vaarallisia. Yleensä tämä merkitsee, ettei tavallisen käyttäjän ole syytä kertoa ulkopuolisille niistä mitään; jätä asiantuntijoiden ratkaistavaksi, mitä ulospäin kerrotaan.

Uutena työntekijänä on syytä olla aktiivinen

Parhaassa tapauksessa sinulle kerrotaan tietoturvajärjestelyistä heti aluksi, esimerkiksi työsuhteen alkaessa. Mutta yleisesti ottaen pitää varautua itse selvittämään tällaisia asioita. Jos yhtenäistä kirjoitettua tietoturvapolitiikkaa ohjeineen ei ole, joudut itse etsiskelemään ja kyselemään ohjeita. "Taloon tuleminen" voi olla juuri oikea tilaisuus tehdä aloite tietoturvaohjeiden kokoamisesta. Mutta ainakin kannattaa esittää esimerkiksi edellä oleva kymmenen kysymyksen lista paikan mikrotukihenkilölle tai vastaavalle ja kirjoittaa vastaukset muistiin.

Noudata niitäkin ohjeita, joiden syitä et (vielä) ymmärrä

Noudata ohjeita, vaikka et aina ymmärtäisi niiden perusteita. Ohjeita ei yleensä tehdä tiukoiksi kiusaamisen tarkoituksessa, vaan niille on omat tekniset perusteensa. Jos sinusta jokin sääntö tuntuu tarpeettomalta, on hyvin mahdollista, että sille silti on painavat perusteet organisaation kannalta.

Paikalliset ohjeet: kaavamainen esimerkki

Paikalliset tietoturvaohjeet voivat olla hyvin lyhyet ja aika tekniset. Ajatuksena ehkä on, että sinun oletetaan tuntevan tietoturvan *yleiset* perusteet, ja siksi kerrotaan vain *paikalliset erityisjärjestelyt* niitä täydentämään, ja kenties joitakin yleissääntöjä, joita paikallisen tilanteen takia halutaan erityisesti korostaa.

Paikalliset ohjeet voisivat olla *esimerkiksi* seuraavanlaiset:

1. Organisaation sisällä voidaan asiakirjoja lähettää liitetiedostoina, mutta vain RTF-muodossa. Lähettämistä varten tulee siis tallentaa Wordillä tehty asiakirja "Tallenna nimellä..." -toiminnon kautta RTF-muotoon.
2. Organisaatiosta ei lähetetä ulospäin sähköpostia missään muussa muodossa kuin pelkkänä tekstinä, ellei vastaanottajien kanssa ole sovittu muusta.
3. Omat tiedostot tehdään levyasemaan *Z*, jolle on käytössä automaattinen varmuuskopiointi (muutokset tallentuvat vähintään kerran vuorokaudessa). Tiedostot, joiden halutaan näkyvän muille lähiverkossa, tehdään asemaan *Y*. Levyasemaan C ei pidä tallentaa mitään, mikä ei ole korvattavissa.
4. Kaikkiin henkilökohtaisiin tietokoneisiin on valmiiksi asennettuna ja automaattisesti käynnissä viruksentorjuntaohjelma. Päivitykset tehdään keskitetysti. Torjuntaohjelmaa ei tietenkään saa poistaa käytöstä.
5. Henkilökohtainen tietokone sammutetaan työpäivän päätteeksi.
6. Tietoturvaan liittyvissä ongelmissa otetaan yhteys ensisijaisesti NN_1:een; varamiehenä toimii NN_2.

Tee myös "oma" politiikkasi

Laadi omaa toimintaasi varten oma turvallisuuspolitiikkasi, joka ottaa kantaa asioihin tarkemmin kuin yleiset tai organisaatiokohtaiset ohjeet. Tämä ei tarkoita esimerkiksi työnantajan ohjeet ohittavaa sooloilua vaan sen miettimistä, miten niiden mukainen vähimmäisturva toteutetaan omassa tilanteessa ja mitä turvajärjestelyjä ehkä tarvitaan niiden lisäksi.

Mieti, mitkä riskit ovat hyväksyttäviä, ja noudata sitten linjaasi, ainakin niin, ettet liu'u lepsumpaan suuntaan. Aika ajoin ja etenkin uusien uhkien ilmettyä kannattaa miettiä päätöksiä uudestaan.

Jos tietokonetta käytetään arkaluonteisen tiedon käsittelyyn, voi olla viisasta yksinkertaisesti olla asentamatta *mitään* tuntemattomasta lähteestä tulevaa ohjelmistoa siihen. "Ilmainen" ohjelma voi osoittautua kovin kalliiksi!

Jos toisaalta järjestelmää käytetään sekalaisiin tarkoituksiin, esimerkiksi viihteeseen, kirjeenvaihtoon ja kodin kirjanpitoon, voi suhtautua asioihin kevyemmin, mutta toivottavasti ei holtittomasti. Joustavuuden tai mukavuuden takia haluat ehkä ottaa pieniä riskejä siitä, että hankit koneeseen jotain, joka ei ihan ole sitä, miltä se näyttää.

Jos tietokoneella on useita käyttäjiä, on ehkä syytä tehdä järjestelyjä, jotka suojaavat kunkin käyttäjän omat tiedot muilta. Vaikka kyse olisi perheenjäsenistä, ei ehkä kannata ihan kaikessa täysin luottaa kaikkiin. Ja vahinkoja voi aina sattua: joku voi poistaa tärkeän tiedostosi luullen sitä omaksi tarpeettomaksi tiedostokseen, koska sillä oli sama nimi.

Selvitä ennalta, keneltä kysyä apua

Selvitä etukäteen, kehen ottaa yhteyttä, kun tulee isoja turvaongelmia. Kuka on työpaikkasi tai oppilaitoksesi sinua lähin tietoturvahenkilö? Tiedätkö, miten häneen saa *nopeimmin* yhteyden esimerkiksi matkapuhelimella? Jos käytät yksityistä Internet-yhteydentarjoajaa, selvitä *etukäteen*, mikä on turva-asioiden kontaktipiste tai neuvontapäivystys.

Kun vahinko on sattunut, sinulla on muutakin tekemistä kuin haeskella oikeaa paperia. Pidä siis yhteystiedot sekä verkossa että paikallisesti tallessa niin, että löydät ne helposti.

Kannattaa myös yrittää esimerkiksi muilta käyttäjiltä kyselemällä selvittää, millaista palvelun tasoa voi odottaa. Usein palvelut ovat hyvin ruuhkaisia. Ainakin työpaikalla on hyvä tietää myös toiseksi lähin tietoturvahenkilö ja koko organisaation tietoturvavastaava.

Vastaa *nyt* mielessäsi seuraavaan kysymykseen: Jos *juuri nyt* sattuisi jokin todella vakava tietoturvaongelma, tietäisitkö heti, kehen otat yhteyttä ja miten? Muista, että olisi ehkä mahdotonta tai erittäin riskialtista käyttää yhteydenottoon normaalia sähköpostin lähettämisen tapaasi. Entä tiedätkö, mitä tehdä, jos kyseinen henkilö ei nyt olekaan tavattavissa ja tiedostosi tuhoutuvat yksi kerrallaan tai haittaohjelma lähettää itseään kaikille osoiteluettelossasi oleville?

Kohti parempaa tietoturvaa

Tietoturvan tavoitteena on tila, jossa nykyaikaista tekniikkaa voidaan käyttää tietojen keräämiseen, käsittelyyn ja siirtämiseen niin, että tiedot säilyvät ja pysyvät oikeina ja ovat käytettävissä silloin kun tarvitaan, mutta vain niihin oikeutettujen saatavilla. Erityisen tärkeää on huolehtia tästä sellaisten tietojen osalta, joita käytetään päätöksentekoon tai erilaisten järjestelmien toiminnan ohjaamiseen.

Tietoturvaan tarvitaan hyvin monenlaisia järjestelyjä ja tekniikoita, mutta myös laajaa yhteistyötä ihmisten ja organisaatioiden kesken. Ketju on yhtä heikko kuin sen heikoin lenkki, ja heikoin lenkki on hyvin usein niin sanottu tavallinen käyttäjä, jolle kukaan ei ole kertonut, mitä hänen pitäisi tehdä. Siksi se, että tavallinen käyttäjä hoitaa oman osuutensa ja ehkä vielä opastaa kaveriaankin, on usein suurin tehtävissä oleva parannus tietoturvaan.

Palvelimien asentaminen

Monenlaisia palvelimia

Tietokoneiden tehon ja ennen muuta Internet-yhteyksien parantuessa on ruvettu pystyttämään palvelimia (servers) jopa henkilökohtaisiin kotitietokoneisiin. Tavallisinta on ehkä asentaa kotikoneeseen Web-palvelin (HTTP-palvelin). Palvelimia ovat Web-palvelimien lisäksi esimerkiksi FTP-palvelimet, Irc-palvelimet, sähköpostipalvelimet ja ns. news-palvelimet (NNTP servers).

Yhteydentarjoajan sopimusehdot tai määräykset voivat kieltää palvelimien asentamisen. Tämä johtuu muun muassa siitä, että palvelin voi aiheuttaa paljon sellaista verkkoliikennettä, johon ei ole varauduttu.

Usein pettävän helppoa

Palvelimen asentamisen pystyy usein tekemään melko vähinkin tiedoin; kohtalainen kyky lukea ja noudattaa asennusohjeita voi riittää. Tässä onkin perusongelma: sen voi tehdä ymmärtämättä, mitä oikeastaan tulee tehneeksi.

Palvelin omassa koneessa on usein mielenkiintoinen mahdollisuus, mutta siihen liittyy myös riskejä. Palvelin nimittäin antaa **tietokoneesi muiden käyttöön verkon yli**. Tarkoituksena on antaa se tarkoin rajattuun käyttöön, mutta tässä voi monta asiaa mennä pieleen. On syytä varautua jopa siihen, että lähtötilanteessa rajoituksia ei ole kytketty toimintaan. Lisäksi ne saattavat pettää.

Monet vahinkoa tekevät ohjelmat pyrkivät erityisesti etsimään ja käyttämään hyväksi Web-palvelinohjelmistojen turva-aukkoja. Usein ne siinä myös onnistuvat.

"Asiakkaat" ja palvelimet

Aluksi hiukan käsitteiden selvennystä. *Web-selain* kuten Internet Explorer tai Netscape on ohjelma, joka ottaa yhteyksiä eri puolilla oleviin tietokoneisiin, *Web-palvelimiin*, ja hakee niistä tietoja sekä voi mahdollisesti tallentaakin tietoa niihin eli muuttaa palvelimessa olevia tiedostoja. Vaikka selaimeen liittyy monenlaisia turvariskejä, niin selain ei normaalisti anna koko Internetin luettavaksi sen koneen tiedostoja, jossa selain toimii. Sen sijaan Web-palvelimen keskeinen *tarkoitus* ja idea on juuri sellainen avoimeen käyttöön saattaminen. Tosin sen pitäisi antaa vain määrätty osa koneen tiedostoista maailman saataville.

Vastaavasti on yleisemmin erotettava toisistaan "tavalliset" ohjelmat, jotka toimivat vain "asiakkaina" (asiakasohjelmina, *client*, *user agent*), ja palvelimet (*servers*), jotka vastaavat "asiakkaiden" esittämiin pyyntöihin. Pyyntö voi olla esimerkiksi "annapa tiedosto se-ja-se" tai "tallennapa tämä tieto sen-ja-sen nimiseen tiedostoon" tai "päivitä tietokantaasi näin-ja-näin" tai "laukaise ydinohjus maaliin se-ja-se", esitettynä erityisellä koodikielellä ("protokollalla"). - Viimeksi mainittu esimerkki ei (toivottavasti) vastaa todellisuutta, mutta se on mukana korostamassa sitä, että palvelin *voidaan* ohjelmoida ohjaamaan tosiaikaisesti todellista järjestelmää, muutakin kuin "vain" tietojenkäsittelyä.

Normaalisti "asiakkaat" on etenkin nykyisin tehty helppokäyttöisiksi niin, että käyttäjä ei näe, mitä teknisellä tasolla, koodikielellä, tapahtuu. Käyttäjä vain esimerkiksi kirjoittaa Web-selaimensa osoitekenttään `www.ficora.fi/suomi/tietoturva/` ja painaa Enteriä; selain, joka siis toimii "asiakkaana", tällöin ottaa yhteyden palvelimeen `www.ficora.fi` lähettäen sille esim. koodikielisen pyynnön `GET /suomi/tietoturva/ HTTP/1.0`. Tähän palvelin normaalisti vastaa hakemalla omasta tiedostojärjestelmästään tiedoston, jonka osoite vastaa pyyntöä, ja lähettämällä kopion sen sisällöstä selaimelle, joka sitten sitten näyttää sen ikkunassaan.

Palvelin kotona

Aiemmin tilanne oli sellainen, että palvelimia toimi vain keskustietokoneissa tai erikseen palvelinkäyttöön varatuissa tietokoneissa. Nykyisin siis tavallinen työ- tai kotikäytössä oleva henkilökohtainen tietokonekin voi toimia muun ohessa palvelimena. Tämä saattaa esimerkiksi mahdollistaa sen, että tietokoneen käyttäjä hakee siitä tietoja tai tallentaa siihen jotain verkon kautta vaikkapa ollessaan matkoilla Australiassa. Ja vaarana sitten on, että joku muu kuin tietokoneen laillinen käyttäjä voi tehdä saman, jos onnistuu murtautumaan salasana- ja muiden suojausten läpi. Ja kuten edellä on kuvailtu, murtamiseen ei ehkä tarvita sen kummempaa kuin että joku katsoo olkasi yli, kun kirjoitat salasanaasi.

Aina valmiina! Mutta mihin?

Mutta palvelimeen liittyy myös erityisiä ongelmia sen takia, että palvelinohjelmiston luonteensa takia *pitää* olla avoin ottamaan vastaan pyyntöjä. Mitä tapahtuukaan, kun joku tekee ohjelman, joka lähettää palvelimelle pyynnön esimerkiksi tuhat kertaa sekunnissa jatkuvasti? Kone, jossa palvelin toimii, voi täysin hyytyä tällaiseen ns. palvelunestohyökkäykseen (Denial of Service).

Lisäksi voidaan tehdä ohjelmia, jotka lähettävät palvelimelle koodikielisiä pyyntöjä, jotka käyttävät hyväkseen turvallisuusaukkoja. Tyypillisesti ne ujuttavat palvelinohjelmiston suoritettavaksi pienen ohjelmanpätkän. Palvelinohjelmiston on toimittava tietokoneessa melko laajoin valtuuksin, ja siksi on olennaista, ettei se ota vastaan käskyjä mistä vain. Mutta rajoitusten toteuttamisessa on siis usein aukkoja.

Ensimmäiseksi lue ohjeet

On siis tärkeää perehtyä palvelinohjelmiston dokumentaatioon huolellisesti etenkin turvallisuuteen liittyvien asioiden osalta. Siinä voi olla vaikeita asioita, mutta silloin on syytä hankkia perustietoja, ennen kuin jatkaa. Voit tarvita yleisiä oppikirjoja, kursseja jne. etenkin tietoliikenteen ja koneesi käyttöjärjestelmän osalta. Yksittäisten vaikeiden kohtien selvittämisessä voi olla apua melko yleistajuisesta englanninkielisestä Webopedia-tietosanakirjasta ja muista verkossa olevista tietotekniikan sanastoista. `<http://www.cs.tut.fi/~jkorpela/dt.html8>`

Palvelinohjelmiston asetuksissa (konfiguroinnissa) voidaan yleensä rajoittaa sitä, mistä kaikkialta palvelin ottaa pyyntöjä vastaan, mitä kaikkea se saa koneessa tehdä jne. Asetukset on syytä käydä huolella läpi, luottamatta siihen, että oletusasetukset olisivat sopivat.

Toiseksi lue lisää ohjeita: seuraa uutisia

On myös syytä seurata jotakin tiedotus- ja keskustelukanavaa, josta saa tietoja kyseisessä palvelinohjelmistossa ilmenevistä turva-aukoista ja niiden tukkimisesta. Tällainen kanava, joka voi olla esimerkiksi Web-sivu tai sähköpostin kautta toimiva jakelulista (mailing list) toivottavasti mainitaan ohjelmiston asennus- ja käyttöohjeissa. Jos ei, on syytä ruveta epäluuloiseksi. Muutenkin dokumentaation puutteellisuus on aina huolestuttavaa; vaikka ohjelman ehkä saisikin jotenkin toimimaan arvailun, yrityksen ja erehdyksen menetelmällä, tulos ei ehkä ole kovin turvallinen!

Tuki turva-aukot

Ilmenevät turva-aukot pitää tietysti tukkia niin pian kuin mahdollista. Usein on syytä harkita palvelun *välitöntä* sulkemista (palvelinohjelmiston pysäyttämistä), kun merkittävä sitä koskeva turvaongelma on tullut tietoon. Väärinkäyttöä yrittävät saavat usein hyvin nopeasti tiedon turvaongelmista, ja "pommitus" on tavallisesti suurinta heti aukon tultua tietoon. Siksi on parempi aluksi sulkea palvelu ja odottaa ehkä muutama päivä, että luotettava korjaus löytyy ja ehditään

toteuttaa. Mutta jos kyseessä on merkittävä julkinen tai kaupallinen palvelu, on syytä asiantuntijoiden arvioida tilannetta; muuten hätiköinnillä helposti aiheutetaan varma haitta, joka on suhteeton riskiin nähden eikä ehkä edes lainkaan auta vaaran torjumisessa.

Tapahtumatiedot talteen, mutta turvallisesti

Tyypillisesti palvelinohjelmisto tarjoaa mahdollisuuden kerätä *tapahtumatiedostoa* eli lokitiedostoa (log file), joka sisältää ehkä hyvinkin yksityiskohtaisen tiedon kaikesta, mitä jokin "asiakas" on palvelimelta pyytänyt ja miten palvelin on siihen vastannut. Tästä voi olla suurta apua ongelmien havaitsemisessa ja selvittelemisessä.

Mutta toisaalta on huomattava, että lokitiedostot usein kasvavat hyvin isokokoisiksi. Ne voivat huomaamattasi täyttää koko kovalevysi (ja siten aiheuttaa pahoja ongelmia) varsinkin, jos kone joutuu palvelunestohyökkäyksen kohteeksi! Tarkista siis, voidaanko ohjelmiston asetuksissa asettaa rajoja tiedostojen koolle ja missä määrin tietojen keruun laajuutta voidaan ja kannattaa rajoittaa. Mahdollisesti joudut aika ajoin "käsin" poistamaan vanhoja lokitietoja.

Asiantuntijaksi kasvaminen

Kaiken kaikkiaan sinun on syytä siirtyä peruskäyttäjän tasolta tehokäyttäjän ja teknisen asiantuntijankin tasolle, jos aiot ottaa käyttöön palvelimen. Tällöin *Site Security Handbook* (RFC 2196) on hyödyllistä peruslukemista, vaikka onkin jo melko vanha.
<http://asg.web.cmu.edu/rfc/rfc2196.html>

Englannin kieli pitää käytännössä osata aika hyvin, koska mitä enemmän mennään turva-asioiden tekniikkaan, sitä enemmän niistä puhutaan vain englanniksi.

Tämän oppaan lopussa olevien linkkien kautta löytyy lisää aineistoa.

Miksi viruksia ja muita tietoturvaongelmia on?

Usein ihmiset kysyvät, ainakin mielessään, miksi tietokoneviruksia tehdään ja miksi ylipäänsä on olemassa kaikenlaisia haittaohjelmia ja muita uhkia. Lyhyt vastaus on, että lyhyttä vastausta ei ole.

Nörtit vauhdissa?

Suuri osa tietokoneviruksista, tietomurroista yms. on tehty poikamaisen kujeilun tarkoituksessa. Monista tietokoneharrastajista on *haastavaa* tehdä virus taitavasti tai murtautua turvajärjestelyn läpi. Usein tähän liittyy *näyttämisen halu*: jätetään jälkiä, niin kuin jotkut maalaavat seiniin tägejä.

Asialla saattaa olla myös *turhautunut* tietokonealan osaaja, jolle ei ehkä ole kunnollisia töitä omassa maassaan tai joka vain haluaa *kostaa* jotakin jotenkin.

Kun tällaisiin seikkoihin vielä yhdistyy usein nuoruuden ajattelemattomuus ja tietojen puutteellisuus, tulee ehkä tehdyksi paljon suurempaa vahinkoa, kuin oli tarkoitus.

Kaikki ei riipu ihmisistä

Mutta ei pidä tuudittautua luulemaan, että tietoturvaa uhkaavat vain hairahtuneet nörtit. Ensinnäkin monet tietoturvaongelmat ovat riippumattomia ihmisten tahdosta. Fyysiset uhkat ovat ilmeisin esimerkki: kovalevy voi mennä rikki kenenkään sitä mitenkään tahtomatta ja tarkoittamatta. Edellä lyhyesti käsitelty ohjelmien ja järjestelmien yleinen *monimutkaistuminen* synnyttää myös uhkia. Jos

ohjelma tekee tuhojaan, ei paljoa lohduta se, ettei se ollut vähimmässäkään määrin kenenkään tarkoitus; ohjelmointivirheestä voi seurata yhtä pahaa jälkeä kuin tahallisesti tehdystä haittaohjelmasta.

Tietotekniikka aseena

Tietotekniikkaa voidaan myös käyttää todellisen terrorin ja muun rikollisuuden ja sodankäynninkin välineenä. Laajamittainen sotilasoperaatio alkaa nykyisin vihollisen tietoliikenteen ja tietojenkäsittelyn lamauttamisella, jos siihen suinkin on mahdollisuuksia. Ja jos ei ole, yritetään edes häiritä. Tai sitten yritetään ottaa vihollisen tietoliikenneverkko omaan käyttöön tai syöttää siihen väärää tietoa.

Tämän lisäksi voidaan suhteellisen rauhallisissakin oloissa pyrkiä *eriasteiseen häirintään*, joskus vain julkisuuden saavuttamiseksi jollekin asialle, joskus vain vastustajan hermostuttamiseksi, mutta mahdollisesti laajemminkin tavoittein. Kenties tavoitteena on "vain" kaapata jotakin taloudellisesti merkittävää tietoa, vaikkapa kilpailijan salaiset tiedot tuotteistaan taikka kansalaisten luottokorttien numeroita. Iso osa hyökkäyksistä tietoturvaa vastaan on *tunnusteluhyökkäyksiä* heikkojen kohtien selvittämiseksi, ilman pyrkimystä *sillä kertaa* tehdä vahinkoa.

Jälkipuhe

Yleistä taustaa

Tätä opasta ruvettiin laatimaan syksyllä 2001, koska tietoturvasta oli kyllä laadittu runsaasti ohjeita, mutta suhteellisen pieni osa niistä oli kirjoitettu peruskäyttäjille (end users) käytännöllisestä näkökulmasta. Useimmat tietoturvaan tähtäävät, peruskäyttäjille tarkoitetut toimintaohjeet olivat organisaatiokohtaisia, jos niitä oli lainkaan koottu yhteen. Usein ne olivat erillisinä kohtina tietoturvaohjeiden viidakossa, jossa on paljon sellaista, mikä on liian teknistä ja liian vaativaa peruskäyttäjälle.

Oppaan luonne

Tähän oppaaseen pyrittiin valitsemaan kaikkein keskeisimpiä tietoturvaneuvoja ja muotoilemaan ne lyhyesti, "huoneentauluksi", sitten selittämään niitä tarkemmin.

Vaikka nyttemmin on laadittu myös monia muita yleistajuisia ohjeita, on peruskäyttäjille sopivan tietoturvaohjeistuksen laatimiseen ja ajan tasalla pitämiseen kiinnitettävä jatkuvasti huomiota. Erityisen tärkeää on muistuttaa keskeisistä perusasioista ja tuoda niitä myös uusien käyttäjien tietoon.

Kyse on tietenkin **yleisluonteisesta** oppaasta. Eri organisaatioissa ja tilanteissa on erityisiä tietoturva-asioita, joita on painotettava, ja kuten tässä oppaassakin korostetaan, paikallisten ohjeiden tunteminen ja noudattaminen on hyvin keskeistä. Parasta olisi, jos niin huoneentaulu kuin tarkempi ohjeistokin voitaisiin laatia organisaatio-, toimintayksikkö- tai jopa henkilökohtaiseksi, mutta käytännössä joudutaan usein tyytymään yleisempään aineistoon. Kovin useinhan tilanne on, että niin tietoturvassa kuin monessa muussakin asiassa monen kotikäyttäjän ja pienen organisaation työntekijän ainoa ATK-tukihenkilö on hän itse.

Kohderyhmänä on siis peruskäyttäjä, tai yleisemmin sanottuna ihminen tietokoneen peruskäyttäjän ominaisuudessa. Esimerkiksi johtajan tai ATK-ylläpitäjän tulee ymmärtää tietoturvasta paljon enemmän, mutta heidän on syytä myös omassa tietokoneen hyväksikäytössään ottaa tietoturva huomioon. Olisi ikävää, jos yrityksen turvasuunnitelman salaiset osat vuotaisivat ulkopuoliselle vain siksi, että turvasuunnitelman laatija ei huolehtinut henkilökohtaisen koneensa turvallisuudesta.

Tätä opasta laadittaessa käytettiin hyväksi monia niistä aineistoista, jotka on mainittu lisätiedoissa. Lisäksi erityisesti RFC 2504:nä julkaistu *Users' Security Handbook*, joka on suomennettu nimellä *Tietokoneen käyttäjän turvaopas*, oli paljolti inspiraationa ja esikuvana.

Tietoturvan käsite

Aihepiirinä tässä ohjeistossa on tietoturva sellaisena kuin se laajassa mielessä käsitetään, siis sisältäen mm. fyysisen turvallisuuden, tietoaineistojen varmistamisen ym. asioita, jotka ovat jääneet julkisuudessa jossain määrin varjoon, koska mm. virusten leviäminen on saavuttanut suuren yleisön huomion. Tietoturva on pyritty ymmärtämään suunnilleen valtionhallinnon tietoturvasanastossa olevan tietoturvan (tietoturvallisuuden) määritelmän mukaisesti:

1. Asiaintila, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää riskiä.
2. Keinojen ja toimenpiteiden kokonaisuus, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissa.

   Huom. Tietoturvallisuuden toteuttamisessa erotetaan kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Päivitys

Oppaan sisältö on tarkistettu tammikuussa 2004. Erityisesti on tarkistettu ja täydennetty linkkejä.

Liite: Lisää tietoturva-aineistoa

Tietoturvasta on niin paljon aineistoa, että runsaus saattaa hämmentää. Seuraavaan on pyritty kokoamaan muutamia keskeisiä aineistoja ja erityisesti sellaisia, joiden kautta löytyy lisää yksityiskohtaista aineistoa ja joiden voi toivoa olevan ylläpidettyjä.

Suomenkielistä perusaineistoa

1. Kansallisissa tietoturvatalkoissa 2004 tehty tietoturvaopas (julk. 9.2.2004). Se on laajennettu versio suomalaisiin koteihin jaetusta *Joka kodin tietoturvaoppaasta*. Siinä mm. kerrotaan mahdollisimman selkeästi Internetin turvallisen käytön perusteista sekä neuvotaan tietokoneiden käyttöjärjestelmän sekä virustorjunta- ja palomuuriohjelmistojen päivittämisessä. <http://www.tietoturvaopas.fi>
2. *Käyttäjän tietoturvaohje*, jonka on laatinut Valtionhallinnon tietoturvallisuuden johtoryhmä. PDF-muodossa. <http://www.vm.fi/tiedostot/pdf/fi/51024.pdf>
3. Viestintäviraston tietoturvasivut. Viestintävirasto (ent. Telehallintokeskus, THK) on Suomessa se viranomainen, joka on vastuussa tietoturvaloukkausten havainnoinnista ja ratkaisemisesta. Sen puitteissa toimii CERT-FI, joka tiedottaa ajankohtaisista tietoturvaongelmista. <http://www.ficora.fi/suomi/tietoturva/index.htm>

Muuta suomenkielistä aineistoa

1. Ilpo Kuivanen: *Johdatus tietoturvaan*. <http://cs.stadia.fi/~kuivanen/tietoturva/index.php>
2. Internetixin opiskeluaineisto *Tietoturvallisuuden perusteita*.

<http://www.internetix.fi/atk-tuki/opinnot/tietoturva/>

3. Microsoftin tietoturvasivut, joilla on useita erityyppisiä tietoturvaohjeita. <http://www.microsoft.com/finland/security/>
4. PK-yritysten tietoturvaopas. Käytännöllinen ohjeisto pienille ja keskisuurille yrityksille. PDF-muodossa. <http://www.ytnk.fi/tietoturva.pdf>
5. *Ostoksilla verkkokaupassa*. TIEKEn opas, joka antaa neuvoja verkosta ostamiseen, myös sen erityisten tietoturvaongelmien osalta. <http://www.tieke.fi/kauppa/ostoksilla>
6. Valtiovarainministeriön sivuston osio *Hallinnon kehittäminen* sisältää erilaisia valtionhallinnon tietoturvaohjeita ja niihin liittyvää aineistoa, mm. tietoturvakäsitteistön. <http://www.vm.fi>
7. TTY:n kurssin *Tietoturvallisuuden perusteet* aineisto, jossa on tietoa tietoturvan tekniikoista; mukana on hyvä aakkosellinen hakemisto. <http://www.cs.tut.fi/kurssit/8306000/>
8. TKK:n virusoppaat. <http://www.hut.fi/atk/oppaat/virukset/>
9. Digitoday-uutissivuston osio *tietoturva*. <http://www.digitoday.fi>
10. Suomen tietosuojaviranomaisten sivusto. <http://www.tietosuoja.fi>
11. *Makupalat*-linkkikirjaston osa *tietoturva*. <http://www.makupalat.fi/teknika3.htm#tietoturva>

Englanninkielistä aineistoa

1. FBI:n National Infrastructure Protectin *Seven Simple Computer Security Tips for Small Business and Home Computer Users*. <http://www.nipc.gov/warnings/computertips.htm>
2. SANS Instituten *The Twenty Most Critical Internet Security Vulnerabilities*. Sen alussa oleva yleinen osuus on sellainen, että siitä on hyötyä peruskäyttäjällekin, kun taas Windows- ja Unix-spesifiset asiat ovat lähinnä ylläpitäjille tarpeen. <http://www.sans.org/top20.htm>
3. dmoz: Computers: Security. Laaja luokiteltu linkkilista. <http://dmoz.org/Computers/Security/>

Osa edellä mainitusta aineistosta on saatavilla vain PDF-muodossa, jonka katsomiseen tai tulostamiseen tarvitaan sopiva ohjelma. Verkosta maksutta saatavia ohjelmia ovat mm. Adobe Acrobat Reader ja GhostScript.

Tämän oppaan Web-version osoite on http://www.tieke.fi/tietoturvaopas/
Jukka K. Korpela