Oppimateriaali

Kurssimateraali

Sivusto: OAMK Moodle
Kurssi: K1131TK Organisaation tietoturva
Kirja: Oppimateriaali
Tulostanut: Hakola Janne
Tulostettu: sunnuntai, 2 joulukuu 2012, 07:50

Sisällysluettelo

1 Johdanto

Tietoyhteiskunnan hyödyt on helposti nähtävissä. Arkipäiväinen toiminta on siirtynyt verkkoon: maksaminen, asiointi, viihde, markkinointi ja monet muut asiat ovat saaneet tietotekniikalla toteutettuina aivan uudet ulottuvuudet niin yksityisten henkilöiden kuin erilaisten organisaatioiden toiminnassa. Palvelut ovat paikasta ja ajasta riippumattomia, nopeita, edullisia ja vaivattomia.

Vasta sitten kun toiminnan haitat nousevat esiin alkaa kritiikki ja julkinen keskustelu.

Usein sanotaan, että kun tietoturva paranee, käytettävyys huononee ja toisaalta kun käytettävyys paranee, tietoturva huononee. Esimerkiksi laitteesi ja tietosi ovat paremmassa turvassa jos sinulla ei ole verkkoyhteyttä. Kun laitteen/tiedon siirtää verkkoon, tietoturva heikkenee, mutta ei aina merkittävästi jos ymmärtää siihen liittyvät riskit, osaa suojautua ja noudattaa normaalia varovaisuutta.

Tiedon jakaminen kaikkien ulottuville on filosofisesti ajatellen hyve. Erityisesti yksityisyyden suojan ja yrityssalaisuuksien vuoksi johonkin on välttämätöntä vetää raja.

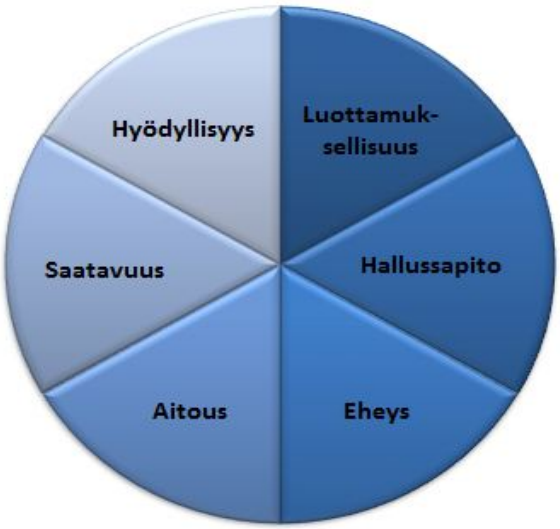
Lisäksi toimintaamme voidaan valvoa ja seurata aivan toisella tasolla kuin koskaan ennen ja kerättyjen tietojen väärinkäyttö voi johtaa ikäviin seurauksiin. Kaikki valvonta ja seuranta eivät kuitenkaan ole pahasta. Monet rikolliset jäävät kiinni matkapuhelimen käytön, valvontakameroiden ja rekistereihin tallentuneiden tietojen perusteella. Valvonta on siis suoranainen välttämättömyys. Kyse on jatkuvasta tasapainoilusta "hyvä ja pahan" välillä.

1.1 Tietoturvan tavoitteet

Tietoturvan määritelmässä sanotaan, että tietoturva on niiden hallinnollisten, teknisten ja fyysisten toimenpiteiden kokonaisuus, jolla tietoturvallisuutta yrityksen, osaston, järjestelmän tai yksittäisen henkilön tiedoille ja niiden käsittelylle rakennetaan ja ylläpidetään. Millaisia "arvoja" siis suojaamme?

Tietoturvan tavoitteet ovat ns. tietoturvallisuuden **peruselementteja tai ulottuvuuksia**. Klassisia ulottuvuuksia ovat luottamuksellisuus, saatavuus ja eheys. Näitä pidetään nykyisin usein riittämättömiä ja siksi myös muita ulottuvuuksia mainitaan monissa lähteissä, mutta ne usein tavalla tai toisella vain täydentävät edellisiä.

Tavoitteenamme on taata organisaation tai yksittäisen ihmisen omistamien tai hallitsemien tietojen:



Luottamuksellisuus: (confidentiality) tarkoittaa sitä, että tiedot ja järjestelmä ovat ainoastaan niiden käyttöön oikeutettujen saatavissa, eikä niitä paljasteta tulostuksen, näytön tai muulla tavalla sivullisten käyttöön. Luottamuksellisuudesta huolehtiminen on siis tietojen suojaamista luvatonta käyttöä vastaan.

Eheys: (integrity) tarkoitetaan sitä, että tietoa ei synny tai häviä, ja että tämä tieto pysyy alkuperäisessä muodossa virheettömänä eri vaiheissa. Tietojen on oltava luotettavia, oikeita ja ajantasaisia niin, että ne eivät ole hallitsemattomasti muuttuneet tai tuhoutuneet. Eheyteen pyritään pääasiassa ohjelmointiteknisin ratkaisuin, mutta eheys voidaan menettää esimerkiksi yrityksen tietojärjestelmän toimintahäiriön, tietokannan vioittumisen, tiedonsiirron aikana tehdyn, luvattomasti suoritetun tietojen muuttamisen, toimintavirheen tai luonnontapahtumien vuoksi.

Saatavuus eli käytettävyys (availability), jolloin tiedot ja muut resurssit ovat tarvittaessa niihin oikeutettujen käytettävissä etukäteen määritellyssä vasteajassa. Resurssit ovat tyypillisesti tietojenkäsittelyresurssien, laitteistojen, ohjelmistojen, henkilöstön ja verkkopalvelujen määrä sekä niiden palvelu- ja toimintavarmuus että laatutaso.

Hallussapito (possession): yksittäisen henkilön oikeus käsitellä yrityksen omistamaa tietoa. Hallussapitoa loukataan silloin kun esim. tieto joutuu vääriin käsiin ja/tai ulkopuolinen taho tutustuu sen sisältöön.

Aitous, tarkastettavuus eli auditointi: tieto on alkuperäistä eikä sitä ole väärennetty. Yrityksen tietojen aitous ja alkuperä tulee voida osoittaa tarvittaessa teknisillä tarkistusmenetelmillä. Esimerkiksi mahdollisuus tutkia jonkin muodostuneen aineiston perusteella esiintyykö virheitä tai

epäsäännöllisyyksiä (tapahtumien kirjausketjun hyödyntäminen).

Hyödyllisyys (usability), josta puhutaan silloin, kun tiedot ovat sellaisessa muodossa, että ne ovat käytettävissä vaivattomasti päivittäisessä toiminnassa ilman erityistoimia. Jos tiedot on esimerkiksi suojattu luvattomalta käytöltä salauksen avulla ja käytettävät salaus sekä salauksen purkuavaimet ovat tuhoutuneet tai kadonneet, ei tietoja voida enää käyttää. Tiedot ovat siis saatavilla, mutta niitä ei voi käyttää.

Peruselementteihin luetaan myös:

Pääsynvalvonta (access control) eli todentaminen, jolloin kontrolloidaan tietoihin tai järjestelmiin pääsy esimerkiksi käyttäjän tunnistuksen ja järjestelmään pääsynrajoituksien avulla. Kuulu varsinaisesti luottamuksellisuuden ylläpitoon, mutta sen avulla voidaan estää myös ulkopuolisia tai oman organisaation työntekijöitä käyttämästä laitteita tai tietoliikenneyhteyksiä omiin tarkoituksiinsa. (Luvaton käyttö kuormittaa järjestelmää, heikentää käytettävyyttä ja altistaa järjestelmän haittaohjelmien leviämiselle, mikä taas puolestaan johtaa eheys- ja luottamuksellisuusongelmiin).

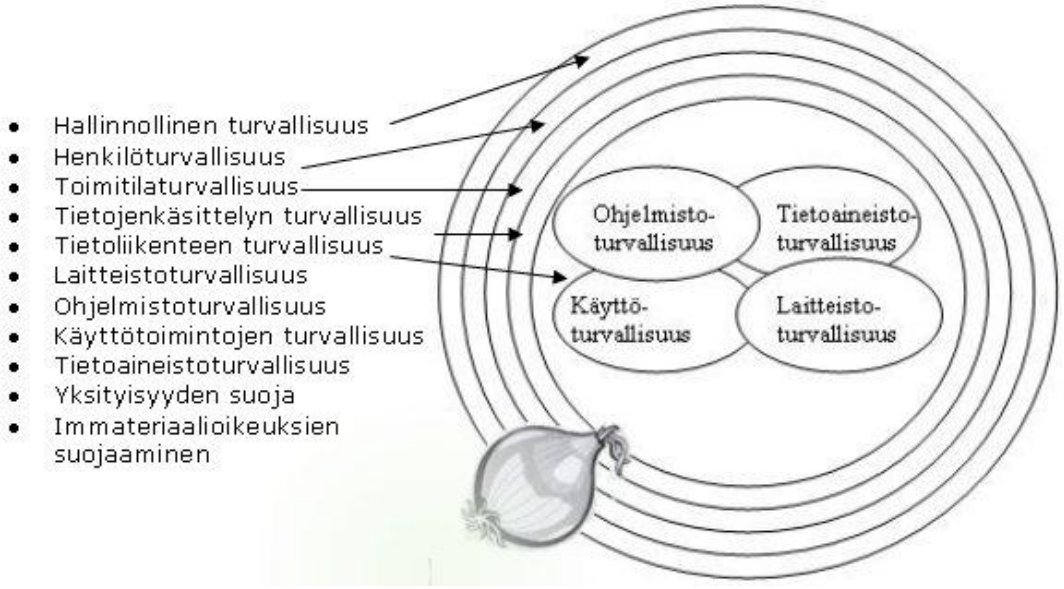
Autenttisuus (authentication) liittyy tunnistamiseen (identification) ja koskee sekä oliota itseään että sen sisältämää alkuperäistä informaatiota. Kahden osapuolen, jotka haluavat kommunikoida keskenään, tulisi autentikoida toisensa. Tietoverkossa siirretyn informaation alkuperä, päivämäärä ja sisältö tulee pystyä tarvittaessa todistamaan oikeelliseksi. Autenttisuus on luottamuksellisuuden ja kiistämättömyyden perusedellytys.

Kiistämättömyys (non-repudiation) liittyy siihen, että olio (tieto, tapahtuma, lähettäjä, vastaanottaja) ei pysty kiistämään tapahtuneita sitoumuksia tai toimenpiteitä. Kiistämättömyys tarkoittaa esimerkiksi sitä, että viestin lähetystä tai vastaanottoa ei voida kiistää. Tällä pyritään juridiseen sitovuuteen, jolloin halutaan varmistaa tiedon alkuperä tai olemassa olevien tietojen luvaton käyttö, niissä tilanteissa, joissa tietojärjestelmän omistaja joutuu harkitsemaan oikeudellisia toimia järjestelmän käyttäjää vastaan. Erimielisyystapauksissa voidaan käyttää esimerkiksi ns. luotettavaa kolmatta osapuolta.

Näitä toisiinsa liittyviä peruskomponentteja ja niihin kohdistuvia uhkia tulee hallita kontrolleilla, joilla tähdätään järjestelmän täydellisyyteen ja paikkansapitävyyteen niin normaali- kuin poikkeusoloissa. Kontrolli on menettelytapa, fyysinen suojauskeino tai toimintaprosessi, joka auttaa ei-toivottujen asioiden torjunnassa. Luotujen kontrollien apuna voidaan käyttää mm. lokitietojen analysointia, raportointia ja palautumisen varmistamista. Tietojen suojaaminen ja niihin liittyvä riskienhallinta on koko tietoturvallisuuden hallinnan kannalta tärkeä tekijä.

1.2 Tietoturvallisuuden osa-alueet

Yrityksen tietoturvallisuus kuvataan usein kerroksittaisena kuten sipuli. Kerrokset kuvaavat tietoturvan osa-alueita. Tietoturvatyössä edetään kerros kerrokselta aina tarkemmalle tasolle kohti sipulin sisusta niin, että kaikki osa-alueet tulee lopulta käytyä läpi.



Hallinnollinen turvallisuus on tietoturvan osa-alue, jossa tarkastelun kohteena ovat yrityksessä käytettävät tietoturvan toimintapolitiikat, toiminnan linjaukset ja periaatteet, toiminnan johtaminen, toimintojen organisointi, toimintojen sijoitus yrityksen rakenteeseen, toiminnan resursointi sekä tietoturvaan liittyvien vastuiden määrittelyt. Siihen liittyvät myös yhteydenpito eri turvallisuudesta vastaaviin elimiin organisaation sisällä sekä sen ulkopuolella (esim. viranomaiset). Tärkeässä asemassa ovat lainsäädäntö ja erilaiset yksityisoikeudelliset sopimukset (esim. lisenssisopimukset ja palvelusopimukset). Hallinnollisen turvallisuuden ylläpito kuuluu yleensä organisaation tietohallinnon tehtäviin.

- Yrityksen johdon luomat toimintaedellytykset tietoturvallisuuden ylläpidolle ja kehittämiselle
- Korostetaan tietoturvallisuuden ammattimaisen johtamisen tärkeyttä
- Tietoturvallisuuteen tähtäävä ohjeistus, koulutus ja valvonta

Henkilöturvallisuus on tietoturvan osa-alue, jossa tarkastellaan yrityksen tietojen ja tietojenkäsittelyn suojaaminen ihmisten aiheuttamilta tahallisilta ja tahattomilta uhkilta sekä ihmisten toimiminen yrityksen tietoturvan varmistajina. Tähän kuuluu myös tietojärjestelmien käyttäjien toimintakyvyn varmistaminen (koulutustoiminta).

- Oma henkilökunta, ulkopuoliset työntekijät, vierailijat ja muut henkilöt
- Rekrytointi, toimenkuvat, sijaisuudet ja varamiesjärjestelyt, työsuhteen muutos tai päättyminen
- Taustatietojen tarkistaminen
- Käyttö-, kulku- ja tiedonsaantioikeudet
- Työ- ja yhteistyösopimusten salassapito- ja vaitiolositoumukset
- Ei puhtaasti tietoturvallisuuden osa-alue

Henkilöstöturvallisuudesta vastaa yleensä organisaation henkilöstöhallinto yhdessä tietohallinnon ja muiden turvallisuuselinten kanssa.

Toimitilaturvallisuus osana tietoturvaa tarkoittaa aluetta, jossa tarkastelun kohteena ovat kaikki ne

yrityksen tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyvät asiat, joilla pyritään estämään yrityksen hallussa olevien ja toiminnassaan tarvitsemien tietojen sekä fyysisen ja ei-fyysisen omaisuuden tuhoutuminen, vahingoittuminen tai joutuminen vääriin käsiin.

- Kulunvalvonta ja -hallinta
- Palosuojelu, murtosuojaus, vesivahinkojen estäminen
- Ei puhtaasti tietoturvallisuuden osa-alue

Tietojenkäsittelyn turvallisuus on tietoturvan osa-alue, jossa tarkastelun kohteena on yrityksen automaattisen ja manuaalisen käsittelyn suojaamiseen liittyvät asiat. Atk-turvallisuus on tärkeä osa tietojenkäsittelyn turvallisuutta

Tietoliikenteen turvallisuus on tietoturvan osa-alue, jossa tarkastelun kohteena on yrityksen käyttämien tietoverkkojen ja niissä tapahtuvan tietoliikenteen suojaamiseen liittyvät asiat.

- Tietoliikennettä välittävä dataverkko ja puhelinliikennettä välittävä vaihdeverkko
- Turvataan jatkuva ja häiriötön toiminta
- Suojataan tiedot ulkopuolisilta kun niitä siirretään, varastoidaan ja käsitellään yleisessä televerkossa tai yrityksen yksityisessä suljetussa verkossa

Laitteistoturvallisuudessa tarkastellaan yrityksen tietojenkäsittely- ja tietoliikennelaitteiden suojaamiseen liittyviä asioita. Tähän kuuluvat tietokoneiden ja muiden tietojärjestelmään kytkettyjen laitteiden tarkoituksenmukainen mitoitus, toiminnan testaus, huollon järjestäminen sekä varautuminen laitteiden kulumiseen ja vanhentumiseen.

- Laitteiden rakenteellinen turvallisuus sekä muut turvallisuutta tukevat ominaisuudet
- Tietoturvallisuus on huomioitu laitteiden jo suunnittelu- ja valmistusvaiheessa, komponenttien valmistuksessa, laitteiden kokoonpanossa, varaosien suunnittelussa ja toteutuksessa sekä laitteiden kunnossapitoon liittyvien ominaisuuksien huolto- ja ylläpitorutiinien toteutuksessa.

Ohjelmistoturvallisuudessa tarkastelun kohteena on yrityksen käyttämien tietokoneohjelmien suojaamiseen sekä ohjelmien lisensointiin ja rekisteröintiin liittyvät asiat.

- Testaustoimet joilla varmistetaan sovellusten sopivuus suunniteltuun käyttötarkoitukseen sekä ohjelmistojen keskinäinen yhteensopivuus, toiminnan luotettavuus ja virheettömyys
- Sisäisiä suojausominaisuuksia esim. ohjelmiston pääsynvalvonta, lokitietojen keruu sekä salasanojen automaattien vanheneminen
- Erityisiä suojausominaisuuksia esim. virustentorjunta-, salaus- ja varmuuskopiointiohjelmistot

Käyttötoimintojen turvallisuudessa tarkastellaan yrityksen tietojenkäsittely- ja tietoliikennelaitteiden päivittäisten käyttötoimintojen suojaamiseen liittyviä asioita.

- Laitteiden ja ohjelmistojen ylläpito ja hallinta
- Esim. käyttöoikeuksien hallinta (määrittely, luominen, muuttaminen, poistaminen)
- Tuotanto- ja testiympäristöjen erottaminen
- Käyttötoimintojen valvonta ja dokumentointi

Tietoaineistoturvallisuudessa tarkastellaan eri talletusmuodoissa olevia päivittäisessä toiminnassa tarvittavia tietoja sekä niiden suojaamiseen liittyviä asioita. Näitä ovat tietojen säilyttäminen, varmistaminen ja palauttaminen sekä tietojen tuhoaminen.

- Tieto on tärkeä kaupankäynnin kohde
- Tietoon liittyy merkittäviä taloudellisia, oikeudellisia ja yhteiskunnallisia arvoja
- Väärinkäytösten aiheuttama vahinko?
- Tärkeää tietojen tunnistaminen:
  -strategiset tiedot
  -asiakastiedot
  - henkilöstötiedot
  -talous- ja hallintotiedot
  -tuotekehitystiedot
  -tuote- ja palvelutiedot
  -turvajärjestelyihin liittyvät tiedot

- Tietojen turvaluokituskäytäntö:
  -tärkeysluokat ja käsittelysäännöt
  -tiedon sisällöllinen arvo (kaikkea ei tarvitse luokitella)
  -koskee kaikkia talletusmuotoja
  -peruskäsitteitä: tiedon omistaja - tiedon haltija
  -esim. turvaluokitusmallista: julkiset tiedot, sisäiset tiedot, luottamukselliset tiedot, salaiset tiedot

Yksityisyyden suoja (=tietosuoja) on tietoturvallisuuden osa-alue, jossa tarkastelun kohteena on yrityksen toimintaan liittyvien ihmisten henkilötietoihin liittyvät asiat.

- Henkilötieto- ja tietosuojalainsäädäntö
- Oma henkilöstö, yksityishenkilö- ja yritysasiakkaat
- Arkaluonteisia tietoja esim. palkka, ammattijärjestötieto, terveys, kotiosoite, kotipuhelinnumero, ammatillinen osaamisprofiili ja erityisosaaminen

Immateriaalioikeuksien suojaaminen tarkoittaa sitä, että yritys tai yksityishenkilö hyödyntää lainsäädännön mahdollisuuksia kohteen omistus- ja hallintaoikeuden suojaamisessa muiden menetelmien lisäksi.

- Tavoitteena erottuminen kilpailijoista
- Luvaton kopiointi ja jäljentäminen
- Korvaus käyttöoikeudesta
- Esim. patentti, hyödyllisyysmalli, mallisuoja, tuotemerkki, tekijänoikeus ja liikesalaisuus, yrityksen toiminimi, Internet domain -toiminimi

Yrityksen tietoturva (sisältö ja laatu) on verkottuneessa maailmassa liiketoiminnan edellytys. Vahingon sattuessa yrityksen julkinen kuva kärsii, yritys ei ehkä saa sopimuksia, menettää asiakkaita, voi joutua maksamaan vahingonkorvauksia tai sopimussakkoja…

Tietoturvasta huolehtiminen on yrityksen johdon vastuulla: johdon tulee osoittaa riittävät resurssit tietoturvatyölle, määritellä vastuut ja johtaa tietoturvatyötä. Tietoturvan parantamisen tulisi olla jatkuva, koko yrityksen läpäisevä prosessi, jossa suunta on ylhäältä alas - eli tietoturvan ja tietoturvatietoisuuden tulee ulottua koko yrityksen kaikille tasoille ja jokaiseen henkilöön.

Edellä lueteltu jaottelu on paljolti keinotekoinen, koska kaikki osa-alueet yleensä vaikuttavat toisiinsa ja niissä on runsaasti yhteisiä tekijöitä. Jaottelu kuitenkin helpottaa tietoturvasuunnittelua yhdessä tietoturvallisuuden peruselementtien (luottamuksellisuus, eheys, saatavuus, jne.) kanssa.

2 Yritystoiminnan turvallisuus

Johdanto yritystoiminnan turvallisuuteen

Tietojenkäsittely on muuttunut koko yhteiskunnan läpi tapahtuvaksi, kaikkien kansalaisten hyväksymäksi toiminnaksi muutaman viimeisen vuosikymmenen aikana. Tärkein kehitys on tapahtunut aluksi mikrotietokoneiden ja myöhemmin mm. erilaisten tablettien ja älypuhelimien ympärillä. Monesti koko yritysten olemassaolo on riippuvainen erilaisilla laitteistoilla olevasta tietoaineistosta, ja sen käytettävyydestä, luotettavuudesta ja salassa pysymisestä asiattomilta. Tämä on tapahduttava erilaisten laitteiden, ohjelmistojen ja verkkojen 'sekamelskassa'.

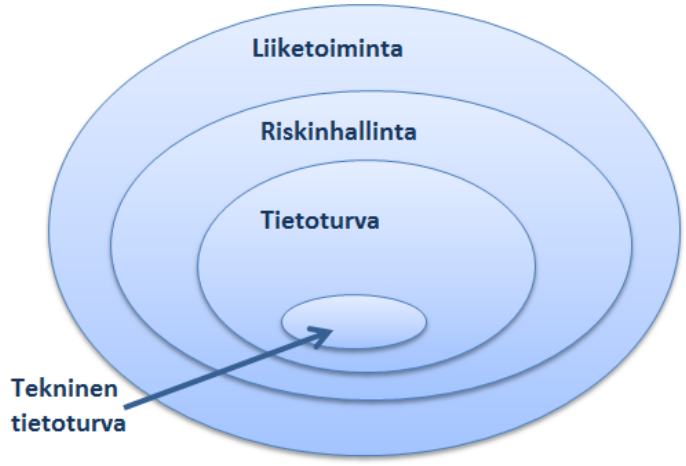
Tietoturva on niiden hallinnollisten, teknisten ja fyysisten toimenpiteiden kokonaisuus, jolla tietoturvallisuutta yrityksen, osaston, järjestelmän tai yksittäisen henkilön tiedoille ja niiden käsittelylle rakennetaan ja ylläpidetään. Tietoturvallisuuden vaatimukset riippuvat suojattavasta tietoaineistoista, toiminnan osapuolista ja normituksesta.

Tietoturvallisuus on osa yritystoiminnan turvallisuutta ja liittyy moniin yrityksen eri osa-alueisiin. Tietoturvan osa-alueet muodostava kokonaisuuden, joka määrittelee sen ympäristön, jossa tietoa yrityksen sisällä siirretään prosessista toiseen ja jonka heikoin lenkki määrää koko järjestelmän turvallisuuden.

Monimutkaisilla teknisillä ratkaisuilla ei voida saavuttaa hyvää turvallisuuden tasoa, jos samalla unohdetaan usein halvat ja yksinkertaiset perustoimenpiteet. Esimerkiksi kulunvalvonta on yksi perustoimenpide, jonka on oltava kunnossa ennen kuin kannattaa lähteä kehittämään verkon turvallisuutta.

Usein jonkun yrityksen tai yksittäisen henkilön tietokoneessa saattaa olla useiden viikkojen tai jopa vuosien työn tulokset, joiden menettäminen tietovarkauden, haittaohjemien tai laitteen rikkoontumisen ja puutteellisten varmuuskopioiden vuoksi on suuri vahinko. Kun luottamukselliset tai salassa pidettävät tiedot päätyvät julkisuuteen on vahinko vieläkin suurempi.

Tietoturvallisuuden taso riippuu yrityksen osaamisesta sekä arvoista ja arvostuksista. Riskinhallinta auttaa meitä vastaamaan kysymykseen mm. kustannuksista. Kuinka paljon rahaa meidän tulisi käyttää esim. Internet-liittymän suojaamiseen? Tietoturvassa kysymys ei yleensä ole riskin poistamisesta, koska 100 % tietoturvaa ei ole olemassakaan. Paremminkin pyritään tehokkaaseen riskinhallintaan. Yrityksen riskinhallinnassa tietoturvallisuus on oma alueensa ja tästä vain pieni osa on teknistä tietoturvallisuutta.



Tietoturva on vaativa ja moniulotteinen tehtävä ja tähän tehtävään osallistuminen kuuluu kaikille. Erilaisten tietoturvaratkaisujen tulisikin olla luonnollinen osa kaikkea toimintaa yhteiskunnassamme. Tietoturvan suunnittelussa, toteutuksessa ja ylläpidossa on muistettava, että tietoturva on yhtä vahva kuin sen heikoin lenkki. Teknisesti ei koskaan voida luottaa ainoastaan yhteen turvatasoon tai turvajärjestelmään. Yksikään ihmisen tekemä järjestelmä ei ole täydellinen. Vaikka tietoturvassa tulisi epäillä kaikkia ja kaikkea, täytyy käytännössä yleensä luottaa johonkin, muuten käytettävyys ja tietoturvan kustannukset karkaavat helposti käsistä.

Yritystoiminnan turvallisuus

Tietoturvallisuus on hyvin laaja käsite ja siihen lähestyminen yritysturvallisuuden ja tietoturvan osa-alueiden kautta auttaa ymmärtämään, mistä siinä on oikeastaan kyse. Tietoturvan luonteen ymmärtämiseksi on siis tarkasteltava ensin organisaation yritysturvallisuutta. Tietoturvallisuus muodostaa tästä vain osan.

Turvallisuusjohtaminen

Turvallisuusjohtaminen ohjaa kaikkea yritysturvallisuuteen liittyvää toimintaa. Turvallisuusjohtaminen koostuu mm. seuraavista asiakokonaisuuksista:

    - Turvallisuustoiminnan organisointi
    - Turvallisuusanalyysit
    - Turvallisuuslainsäädäntö
    - Turvallisuustoiminnan standardit, laatu ja mittarit
    - Tapaturma-, onnettomuus- ja vahinkotilastot
    - Turvallisuustietoisuuden lisääminen, johon liittyy perehdyttäminen, koulutus ja käytännön harjoitukset
    - Sidosryhmäyhteistyö (viranomaiset, asiantuntijat, muut turvallisuustahot)
    - Riskienhallinnan menetelmät
    - Turvallisuusriskien seuranta ja tarkastukset
    - Turvallisuuden osa-alueiden auditoinnit
    - Benchmarking
    - Turvallisuusohjeistuksen kehittäminen
    - Vakuutukset

- eri osa-alueet ja niiden keskinäiset suhteet
- yritystoimintaan kohdistuvia riskejä ja uhkia vastaan suojautuminen (suojataan mm. henkilöstö, asiakkaat, muut sidosryhmät, tiedot, omaisuus ja toimintaympäristö vahingoilta,

väärinkäytöksiltä ja rikolliselta toiminnalta)

- suojauskeinot (tekniset ja ei-tekniset keinot)
- suojattavat kohteet (esim. asia, esine, toiminto, ihminen, tieto, prosessi)
- liiketoiminnan ydin (pidettävä mielessä perimmäinen syy)

Yritysturvallisuuden osa-alueet

1. Kiinteistö- ja toimitilaturvallisuus
    - Tilojen tärkeysluokittelu (esim. toimisto-, varasto-, tuotantotilat: perus-, erityis-, täyssuojaus)
    - Kerroksittainen suojaaminen (esim. aluesuojaus - tontti; kuorisuojaus - kiinteistö; tilasuojaus - huone; kohdesuojaus - kassakaappi)
    - Rakenteellinen suojaus (lukitukset, murtosuojaus, ovet)
    - Turvallisuusvalvonta (rikosilmoitinjärjestelmä, vartiointi, avainten ja kulkuoikeuksien hallinta)
    - muita: energiansaannin varmistaminen, tilojen äänieristys)
2. Henkilöturvallisuus
    - Henkilöturvallisuuden huomioiminen henkilöstöpolitiikassa (henkilöstösuunnittelu, -hankinta, -kehittäminen, työsuhde ja palkka-asiat, yhteistoimintamenettely)
    - Henkilöiden taustatietojen tarkistus (viranomaistarkistus, työhistoria, koulutustausta, luottotiedot ja maksuhäiriöt, yrityskytkennät, suosittelijat, julkaisutoiminta, terveydentila)
    - Toimenpiteet työ- tai sopimussuhteen alkaessa ja päättyessä (tietojärjestelmien ja puhelinliittymien käyttöoikeuksien poisto, yrityksen tietoaineiston palautus, kulkuoikeuksien poisto ja avaimien palautus, rahankäyttövaltuuksien poisto)
    - Uhkaustilanteiden käsittely (vaikeat asiakaspalvelutilanteet, pommi- tai tappouhka)
    - Henkilösuojaus (edellisten tilanteiden johdosta fyysinen suojaaminen)
    - Avainhenkilöt (osaaminen, sitouttaminen, varahenkilö, henkilön sidosryhmäsuhteet, muut henkilön ominaisuudet)
    - Sopimukset henkilöturvallisuuden varmistajina (salassapitosopimus tai -sitoumus; henkilökohtainen, yritysten välinen, työnantaja ja työntekijä)
3. Paloturvallisuus ja pelastustoiminta
    - Paloturvallisuus (lait, tekniset rakennemääräykset, paloilmoitin ja sammutusjärjestelmät, vastuumäärittelyt)
    - Pelastustoiminta (väestönsuojelu, evakuointi, ensiapu)

4. Ympäristönsuojelu
    - Ympäristöpolitiikka
    - Ympäristöasianhallintajärjestelmä EMAS
    - ISO 14000–ympäristöstandardisarja
    - Ympäristömerkit
    - Jätehuolto (materiaalit, kuljetukset, aineisto (esim. käytöstä poistettava tuhottava luottamuksellinen tietoaineisto ei ole jätettä))
    - Keräys- ja kierrätystoiminta (katso edellinen)
5. Ulkomaan toimintojen yritysturvallisuus
    - Toiminta ulkomailla (paikalliset erityispiirteet (vartiointi, suojelurahat, jokamiehen oikeudet))
    - Kriisitilanteet ja henkilöstön evakuointi
6. Matkustusturvallisuus
    - Ennakkotietojen hankinta matkakohteesta
    - Matkustusturvallisuus (esim. atk-laitteet käsimatkatavarana)
7. Rikosturvallisuus
    - Yrityksen toimintaan kohdistuva rikollisuus (varkaus, ryöstö, murto, ilkivalta ja vahingonteko, kiristys)
    - Rikosriskien hallinta (ennaltaehkäisy, rajoittavat suojaus-toimenpiteet, korjaavat toimenpiteet)
    - Yhteistoiminta viranomaisten kanssa (valvovat ja ohjaavat viranomaiset, vero-, tietosuoja-, tulli- ja rajavartiosto viranomaiset, poliisi)
    - Toiminta rikostilanteessa (etukäteisohjeistus, esto- ja rajoittamis- ja jatkotoimenpiteet)
8. Työsuojelu
    - Työsuojeluvastuut, -henkilöstö ja -valvonta
    - Työsuojelun toimintaohjelma
    - Työturvallisuus (työn henkinen kuormittavuus)
    - Työterveyshuolto
9. Tuotannon ja toiminnan yritysturvallisuus

- Tuotevastuu (tuotteen aiheuttamien vahinkojen korvaaminen)
- Tuoteturvallisuus
- Kuljetusturvallisuus
- Arvo-omaisuuden suojaaminen (materiaalinen, immateriaalinen (mm. tieto ja tietokoneohjelmat))
- Varainhoidon ja maksuliikenteen turvallisuus (perustana kunnossa oleva henkilö-, toimitila- ja tietoturvallisuus)
- Sopimusriskien hallinta

10. Vakuuttaminen
    - Vakuutuslajit (pakolliset ja vapaaehtoiset (esim. keskeytysvakuutus))
    - Vakuuttajan valinta (vakuuttajan vakavaraisuus, vakuutusten kattavuus)
11. Poikkeusoloihin varautuminen
    - Varautumisen päämäärä ja tarkoitus (pidetään yllä ja kohotetaan kriisinkestokykyä) Normaalitilanne; poikkeustilanne (vakava häiriö); poikkeusolo.
    - Varautumisen taustalla olevat tilannemallit (kiristynyt kansainvälinen tilanne, vieraiden maiden välinen sota, sodan-uhka, sodan jälkitila, suuronnettomuus, taloudellinen kriisi)
    - Varautumisen toteutus (lainsäädäntö, varautumistoimien suorittaminen jo normaaliaikana)
    - Yhteistoiminta viranomaisten kanssa (puolustusvoimat, palo-, pelastus-, poliisi- yms. viranomaiset)
    - Liiketoiminnan jatkuvuussuunnitelma (Kriittisten prosessien ja resurssien tunnistaminen, kuvaus ja priorisointi; riskit, kriisiorganisaation määrittely, aktivointi)
    - Vapaaehtoinen maanpuolustustyö
12. Tietoturvallisuus
    Tietoturvallisuuden osa-alueet käsiteltiin jo luvussa 1 omana kokonaisuutenaan.

2.1 Tarkastelukulmat

Hyvin hoidetulla yrityksellä on oltava selkeästi ja asianmukaisesti kuvattu tietoturvallisuuden suunnittelun, ylläpidon sekä kehittämisen toimintamalli, jota kehitetään järjestelmällisesti kuten muitakin yrityksen toimintoja. Mallista käytetään nimeä yrityksen tietoturvallisuusarkkitehtuuri. Malli muodostuu useista loogisesti erillisistä tarkastelukulmista, jotka kattavat kaikki yrityksen toiminnan oleelliset tietoturvallisuusasiat.

1. Liiketoiminnallinen tarkastelukulma

- Johdon näkökulma
- Tämän avulla pyritään määrittelemään yrityksen tietoturvallisuusasioiden kehittämisen ja ylläpidon lyhyen ja pitkän ajan tavoitteet sekä niiden yhteys yrityksen päivittäiseen toimintaan
- Tietoturvallisuutta katsotaan ylhäältä alaspäin päivittäisen liiketoiminnan osana
- MIKSI tietoturvallisuus on tärkeää yritykselle!

Voit hahmottaa sitä seuraavilla kysymyksillä:

- mitä tietoja yritys tarvitsee toiminnassaan?
- mitkä yrityksen tiedoista ovat kaikkein tärkeimmät?
- kuinka pitkään yrityksen toiminta voi jatkua ilman tärkeitä tietoja?
- mitä tapahtuu, jos yrityksen tärkeät tiedot eivät ole käytettävissä?
- mitä tapahtuu, jos yrityksen tärkeät tiedot joutuvat ulkopuolisten haltuun tai ne tuhoutuvat?

2. Prosessitason tarkastelukulma

- Haetaan vastausta siihen, MITÄ suojattavaa yrityksessä on!
- Voidaan tarkastella erilaisten toimintaprosessien sekä niihin liittyvien omaisuuserien kautta
- Suojattava omaisuus voi olla luonteeltaan ei-fyysistä ja fyysistä

- Toimintaprosesseja ovat esim. laskutus-, tuote-, kehitys- ja markkinointiprosessit
- Fyysisiä omaisuuseriä ovat esim. atk- ja tietokonelaitteet, koneet ja yrityksen toimitilat
- Yrityksen tietokoneohjelmat ja tiedot ovat esimerkkejä ei-fyysisistä omaisuuseristä
- Tarkastelukulman kautta pyritään löytämään suojaamista vaativat kohteet
- Kokonaisvastuu prosessin omistajalla (vrt. tiedon omistaja)
- Jos suojattavia kohteita ei tunnisteta, ei yritys myöskään pysty suojautumaan tehokkaasti sen toimintaan kohdistuvilta uhkilta
- Kohteet tunnistettava tarkasti, koska yli- tai alisuojaus ei ole kustannustehokasta

3. Toteutustekninen tarkastelukulma

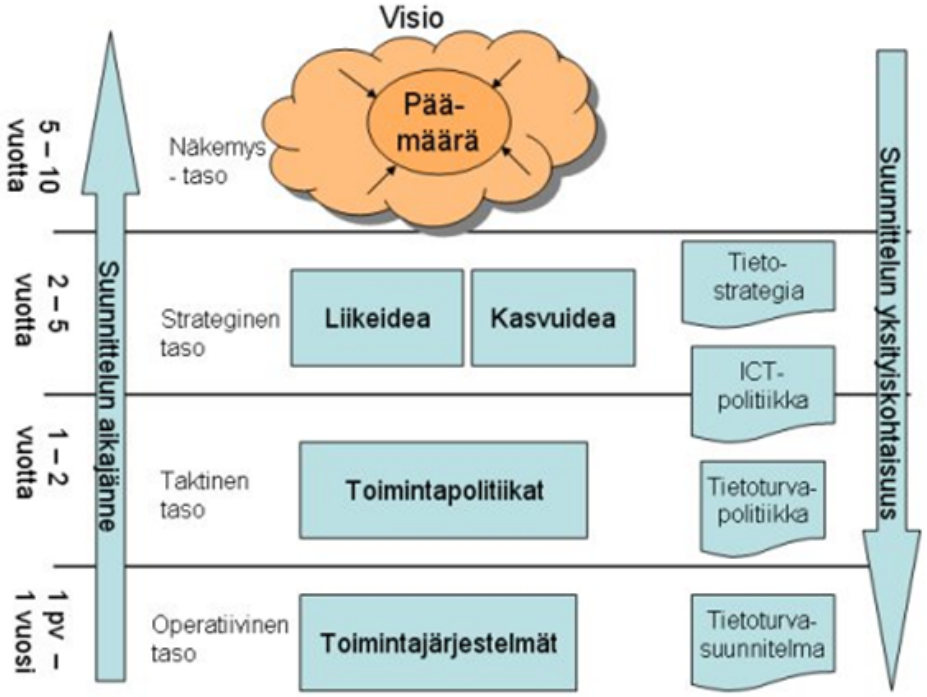
- Tällä etsitään vastausta siihen, MITEN yrityksen tarvitsemat suojaukset toteutetaan käytännössä!
- Suojausmenetelmien ylläpitäjien ja kehittäjien tarkastelukulma
- Usein yritykset aloittavat tietoturvallisuuden kehittämisen erilaisilla teknisillä suojausmenetelmillä miettimättä tarpeeksi MIKSI ja MITÄ
- Teknisiä tai ei-teknisiä menetelmiä
- Kokonaisvastuu tietoturvallisuusalan asiantuntijoilla

2.2 Tietoturvallisuuden johtaminen

Tietoturva koskee koko organisaatiota ja sen suunta on ylhäältä alas - johdosta loppukäyttäjiin asti. Tällöin ylin johto (yrityksen koosta riippuen johtaja / tietoturvallisuusasioiden ohjausryhmä / neuvottelukunta) määrittää turvallisuusmallin, jossa esitetään tietojen ja informaation käsittelyturvallisuus, lakisääteiset turvakysymykset, organisaatioon mahdollisesti kohdistuvat rikolliset toimenpiteet ja organisaation eri ryhmittymien välinen yhteistyö.

Juha E. Miettisen (1999) mukaan tietoturvallisuuden johtamisen päävaiheet ovat riskien tunnistus, suojaustason määrittely, suojausten suunnittelu, suojausten toteutus, suojausten valvonta, suojaustason kehittäminen ja suojaustason mittaaminen. Tietoturvallisuuden kehittäminen on jatkuva prosessi, jossa eri päävaiheet seuraavat toisiaan.

Hakala & al. 'Suunnittelun tasot ja aikajänteet' kuvaa asiaa seuraavasti:



Lähde: Hakala, Vainio, Vuorinen. 2006 Tietoturvallisuuden käsikirja

Tietoturvavallisuustoimintojen kehittämiseksi on yrityksellä oltava jokin järkevä **päämäärä eli toiminta-ajatus**. Tämä sisältää kuvauksen siitä, miksi yritys panostaa tietoturvallisuusasioidensa kehittämiseen ja miksi se on toiminnalle tärkeä asia. Sillä on oltava selkeä yhtymäkohta liiketoiminnan toiminta-ajatukseen sekä johdon kirjallinen vahvistus tai hyväksyntä.

Strategia ja politiikat kuvaavat kuinka yritys suhtautuu tietoturvallisuutensa kehittämiseen lähivuosina, millaisella panostuksella ja mitkä ovat tärkeimmät kehittämiskohteet. Ylimmän tason tieto- ja viestintäpolitiikan (ICT-politiikan) ja sen osa-alueen tietoturvapolitiikan lisäksi yrityksellä voi olla rajattuihin kohteisiin liittyviä yleisiä, kaikkia koskevia pelisääntöjä, sekä osalle henkilöstöä yksityiskohtaisia toimintaohjeita.

Hallinnollisesti tietoturvatyö etenee ylimmältä tasolta kohti koko henkilöstölle suunnattuja erilaisia tietoturvaohjeita. Ohjeisto muodostuu useista loogisesti eri tasolla olevista ohjetyypeistä, joilla on tietty tarkasti rajattu käyttötarkoituksensa sekä soveltamisalueensa.

Tietoturvapolitiikka (Information security policy) on yrityksen johdon kannanotto tai ohje (raamit ja linjaukset), miten yritys suhtautuu tietoturvallisuuteen ja millä tavalla sen tietoturvallisuustoimintoja johdetaan nyt ja tulevaisuudessa. Tietoturvapolitiikka on tärkein yrityksen tietoturvakäytäntöjä ja tietoturvallisuusprosessia ohjaava dokumentti. Se on luonteeltaan suhteellisen pysyvä, julkinen dokumentti ja siksi usein laadittu liiankin yleisluontoiseksi.

Hyvän tietoturvapolitiikka sisältää (Hakala & al.) seuraavat osa-alueet:

- Organisaation oman tietoturvallisuuden määritelmän, turvallisuuden keskeiset kohteet, laajuuden sekä ennen kaikkea turvallisuuden tärkeyden organisaation toiminnalle
- Johdon tahdonilmaus ja tuki tietoturvan tavoitteiden saavuttamiseksi ja siihen liittyvien periaatteiden noudattamiseksi osana organisaation liiketoimintastrategiaa
- Rakenteet, joiden avulla tietoturvallisuuteen pyritään, erityisesti ne rakenteet, joilla riskit tunnistetaan ja niitä hallitaan

- Yhteenveto tietoturvakäytännöistä, noudatettavista standardeista ja yleisperiaatteista

- Yhteenveto lainsäädännön, sopimusten ja kauppatapojen asettamista vaatimuksista
- Yhteenveto turvallisuusajattelun edistämistoimista ja turvallisuuskoulutuksen järjestämisestä
- Kuvaus liiketoiminnan jatkuvuuden hallinnasta ja sen liittymisestä tietoturvallisuuteen
- Määritelmät tietoturvallisuuteen liittyvistä vastuualueista ja turvallisuuteen vaikuttavien tapahtumien raportoinnista
- Käytännöt ja seuraukset turvallisuuspolitiikan rikkomuksista
- Luettelo politiikan tarkentavista tietoturvaohjeista ja standardeista

Tietoturvapolitiikka on kirjoitettu selkeään muotoon ja tarkoitettu henkilöstölle, asiakkaille ja kaikille sidosryhmille. Varsinainen politiikka on siis julkinen, mutta tietoturvapolitiikan liitteenä olevat tarkemmat käytänteet ja tekniset ratkaisut ovat luottamuksellisia tai salaisia.

Esimerkki tietoturvapolitiikasta:

"Yrityksen liiketoiminnan ja taloudellisten etujen turvaamiseksi, oikean ja luotettavan tiedon saamiseksi, tietojenkäsittelyn sekä tietojen eheyden, luottamuksellisuuden ja käytettävyyden turvaamiseksi noudatetaan Yhtiö X:ssä seuraavaa tietoturvallisuuspolitiikkaa:

- Yrityksen tietoasiakirjat, tietovälineet, tekniset tallenteet, niillä oleva tieto, sekä suullinen informaatio ovat yrityksen omaisuutta.
- Niiden antaminen yrityksen ulkopuolelle saa tapahtua vain yrityksen eduksi.
- Yrityksellä tulee olla erilliset kirjalliset ohjeet yrityssalaisen tiedon merkitsemistä, käsittelyä, säilyttämistä ja hävittämistä varten.
- Yritys toteuttaa standardin mukaista laatujärjestelmää ISO/IEC 17799 tietoturvallisuustoiminnan perustana.
- Yrityksessä tehdään riskikartoitukseen perustuva tietoturvallisuus-suunnitelma, joka toimii käytännön työn ja ohjeistuksen perustana. Suunnitelmaa päivitetään riittävän usein.
- Esimiehet huolehtivat siitä että työntekijät saavat tietoonsa heidän työtään koskevat tietoturvallisuusohjeet jo työsuhteen alussa.
- Jokainen työntekijä noudattaa tietoturvallisuudesta annettuja ohjeita ja vastaa omalta osaltaan tietoturvallisuuden toteutumisesta yrityksessä.
- Myös yritysjohto sitoutuu tähän tietoturvallisuuspolitiikkaan.

Tietoturvajohtamisen yhteenvetoa

- On huolehdittava yritysjohdon sitoutumisesta tietoturvallisuusasioihin ja -ratkaisuihin.
- On huolehdittava resursoinnin riittävyydestä (aika, koulutus, raha, tekniikka, henkilöstö)
- On suunniteltava lyhyen ja pitkän tähtäimen ohjelma
- On huolehdittava siitä, että kaikki organisaation tasot jakavat vastuun tietoturvallisuuden ylläpidosta ja kehittämisestä
- On peilattava tietoturvallisuustoimintaa organisaation muuhun toimintaan

2.3 Riskien hallinta

Tietoturvallisuusasiat joudutaan kohtaamaan viimeistään silloin, kun yritys on kohdannut ongelmia puutteellisten suojausten aiheuttamien vahinkojen vuoksi. Jotta tällainen voitaisiin välttää, on tietoturvallisuutta osattava tarkastella osana päivittäistä toimintaa.

Tietoturvallisuus asioiden hyvällä suunnittelulla ja hoidolla voidaan välttää monia uhkia ja riskejä sekä pienentää niistä aiheutuvien vahinkojen korjaamiseen liittyviä ylimääräisiä kustannuksia.

Uhat ja riskit

Tietoturvallisuuteen kohdistuu paljon erilaisia uhkia. Uusia uhkia syntyy ja osa vanhoista uhkista poistuu. Tietoturvatyössä uhkia on järkevämpää aluksi tarkastella loogisina kokonaisuuksina.

Yleistä uhkien luokittelua:

- Vahingossa syntyneet ja tarkoituksella aiheutetut uhat
    - ihmisen (taitamaton toiminta, huolimattomuus) tekemä virhe, esim. automaattisen varmuuskopioinnin epäonnistuminen
    - järjestelmään tunkeutuminen, tietojen varastaminen tai tuhoaminen
- Passiiviset ja aktiiviset uhat
    - passiivinen uhka ei aiheuta toiminnalle välitöntä vahinkoa, esim. yrityksen tietoliikenteen seuraaminen ja liikenteen nauhoittaminen ilman, että tahallisesti vaikutetaan lähiverkon toimintaan
    - aktiivinen uhka vaikuttaa suoraan yrityksen toimintaan
- Sisäiset ja ulkoiset uhat
    - sisäisen uhka on useiden tutkimusten mukaan kiistatta tietoturvallisuuden pahin uhka. Aiheuttaja esim. yrityksen työntekijä tai joku muu sisäiseen toimintaan vaikuttava henkilö
    - ulkoisia uhkia esim. amatöörien kiusanteko, ammattimainen tiedustelu ja vakoilu
- Ihmisen aiheuttamat ja luonnosta johtuvat uhkat
    - ihminen on kaikilla mittareilla mitattuna suurin yrityksen tietoturvallisuuteen kohdistuva uhka (tahallinen, tahaton toiminta), koska ihmisen toiminnan valvominen on huomattavan vaikeaa
    - luonnosta aiheutuvat uhat vaikeasti ennakoitavissa

Mihin tietoturvauhat sitten kohdistuvat?

- Tietojen tai tietojenkäsittelyresurssien tuhoutuminen.
- Tietojen sisällön luvaton muuttaminen alkuperäisestä poikkeavaksi.
- Tietoihin tai tietojenkäsittelyresursseihin kohdistuva varkaus, katoaminen tai muu menetys.
- Tietojen sisällön paljastuminen ulkopuolisille, tunkeutuminen tietojärjestelmiin.
- Tietojenkäsittelyresurssien toiminnan keskeytyminen, lamautuminen, käytettävyyden häirintä.
- Tietoturvatyön lähtökohtana pidetään tietoihin kohdistuvia uhkia.

Tietoturvatyön lähtökohdat organisaatiossa:

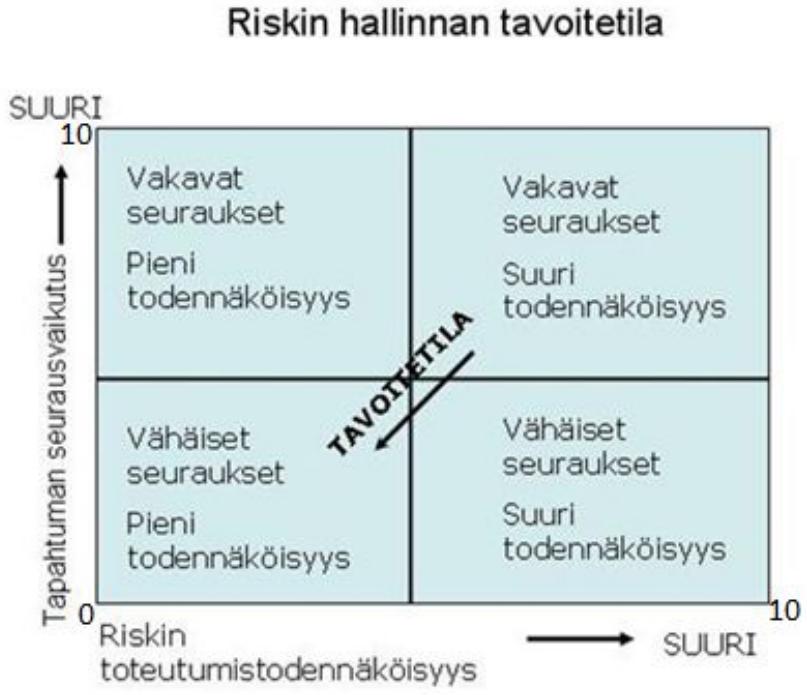
1. Haavoittuvuuksien kartoitus
2. Uhat
3. Riskit
4. Vahingot
5. Suojaukset

Esimerkki: Haavoittuvuuksien kartoituksessa voidaan löytää mm. ihmisen tahalliset toimet, ulkopuoliset onnettomuudet tai systeemin luotettavuus. Riskinä on että havoittuvuus ja uhka (esim. tietovarkaus, sähkökatko, järjestelmään kohdistuva sabotaasi tai työaseman rikkoontuminen) yhdistyvät. Sen seurauksena turvallisuus rikkoontuu ja se vaikuttaa organisaatioon erilaisina menetyksinä. Riskinhallinnan tehtävä on kartoittaa ja huolehtia suojauksista ja minimoida vahingot.

Riskiä tarkastelemalla pyritään tunnistamaan sen aiheuttamat uhat, jotta niitä vastaan voidaan suojautua. Epävarmuus liittyy riskiin olennaisesti. Etukäteen ei koskaan voi olla varma riskin toteutumisesta.

Riskien hallinnan tavoite

Riskien hallinnan tavoitteena on yrityksen toimintaan kohdistuvien ei-toivottujen tapahtumien eli riskien luonteen ja laajuuden ymmärtäminen, hyväksyttävän riskitason määrittely sekä olemassa olevan riskitason alentaminen hyväksyttävälle tasolle.



Riskien hallinnan vaiheet

- Riskien tunnistaminen
- Riskien arviointi ja priorisointi
- Riskien torjunnan suunnittelu

- Riskien torjunnan toteutus ja testaus
- Vahingoista toipuminen
- Seuranta, koulutus ja ylläpito

Riskien tunnistaminen

Lähestymistapoja tietoriskeihin

Tietoriski on vahingonvaara (uhka), joka kohdistuu organisaation hallussa olevaan tietoon, toimintaan, henkilöstöön tai omaisuuteen. Sen toteutuminen voi aiheuttaa suuren taloudellisen menetyksen, vahingonkorvauksia, ongelmia toiminnan jatkuvuudelle ja yrityskuvalle.

Ensimmäiseksi on tunnistettava haavoittuvuus ja uhkatekijä. Haavoittuvuus tarkoittaa tietojärjestelmän alttiutta uhkille, joita tietoturvatoimenpiteet eivät suojaa. Riskien arviointiin ja analysointiin on useita menetelmiä.

- Haavoittuvuus on suojattavan kohteen suunnittelusta, toteutuksesta tai toiminnallisista puutteista aiheutuva ominaisuus (heikkous), josta voi syntyä potentiaalinen uhka suojattavalle kohteelle tai toiminnalle.

- Järjestelmän, verkon, jne. haavoittuvuuksien kartoituksessa voidaan käyttää tarvittaessa luotettavaa konsulttia (Kuka on luotettava?).

- Haavoittuvuuksien etsinnässä apuna tarkastuslistoja, katselmointia.

Esimerkkejä lähestymistavoista:

1. **Tarkistuslistat**

   Kysymysluetteloita, joissa selvitetään tarkasteltavan kohteen tietoturvallisuuteen liittyviä asioita. Olemassa oleviin suojauksiin ja suojattavien kohteiden tunnistamiseen sekä puutteellisten tai kokonaan puuttuvien suojausten etsimiseen. Kysymyksiin vastataan usein ei/kyllä/en tiedä.

   Etuja: Helppo ja nopea tapa hahmottaa suojattavat kohteet ja suojausmenetelmät. Vaatii vain vähän perustietämystä.

   Haittoja: Ei sovellu hyvin uhkien tunnistamiseen, eikä anna kuvaa suojausten tehokkuudesta (ei sisällä mittareita) -> väärä kuva suojausten riittävyydestä. Tämän vuoksi on lisäksi käytettävä jotain muuta riskien arvioinnin ja analysoinnin menetelmää.

   Olemassa valmiita listoja (myös tietokoneohjelmia), mutta listoja voi tehdä myös itse. Kvalitatiivinen eli laadullinen menetelmä.

2. **Skenaarioanalyysi**

   Ryhmätyönä pyritään kuvaamaan pienten kertomusten eli skenaarioiden avulla erilaiset uhkatilanteet mahdollisimman tarkasti. Lisäksi kuvataan mahdolliset jälkiseuraamukset. Arvioidaan toteutumistodennäköisyydet ja tarvittavat muutokset. Seuraavaksi skenaariot asetetaan tärkeysjärjestykseen esiintymistodennäköisyyden ja taloudellisten seurausten (esim. riskitaulukko) mukaan ja lopuksi mietitään suojausmenetelmät.

   Käytetään apuna tarkastuslistoja ja/tai ohjelmallisia työkaluja (kalliita). Kvalitatiivinen menetelmä.

3. **Courtneyn menetelmä**

Courtneyn menetelmässä tarkastellaan tietoturvallisuuteen kohdistuvin uhkien sekä riskein esiintymien todennäköisyyksiä. Mm. vakuutusyhtiöiden suosiossa olleen menetelmän avulla lasketaan ei-toivottujen tapahtumien odotettujen frekvenssien ja vahinkojen aiheuttamien rahallisten vahinkojen suuruuden avulla odotusarvoja.

Laskentakaava:

E=P x A, jossa E (Expected loss) on vahingon odotusarvo, P (Probability loss) on vahingon todennäköisyys sekä A (Amount of possible loss) on odotetun vahingon suuruus rahayksikössä.

Haittana se, että laskennassa käytettävät arvo ovat vain suuntaa-antavia -> teoreettisia arvoja, joiden tulos voi olla harhaanjohtava. Hyvä menetelmä silloin kun laskennan arvot tarkkoja ja niitä on käytettävissä pitkältä ajalta.

Voidaan käyttää tietokoneavusteisesti ohjelmallisten työkalujen avulla. Kvantitatiivinen menetelmä.

4. **Baseline-menetelmä**

   Vaihtoehto edellisille menetelmille. Baseline-lähestymistapa on joukko menetelmiä, joilla yritys voi kehittää tietoturvallisuusasioita järjestelmällisesti. Saavuttanut de facto-standardin aseman ja osittain myös syrjäyttänyt perinteiset riskien tunnistamisen, arvioinnin ja analysoinnin menetelmät.

   Ei sisällä riskien arviointia eikä analysointia. Keskitytään ensisijaisesti suojattavien kohteiden tunnistamiseen sekä suojausten suunnitteluun ja toteuttamiseen.

   Perussuojausmenetelmien lisäksi voidaan käyttää omaan toimialaan kohdistuviin erityisuhkiin erityissuojausmenetelmiä. Apuna käytetään muiden vastaavien organisaatioiden vastaavissa olosuhteissa käytettäviä menetelmiä (=peruskontrolleja).

   Baseline-menetelmän taustalla on asianmukaisen huolellisuuden noudattaminen yrityksen kaikessa toiminnassa. Perusedellytys menetelmän tehokkaalle soveltamiselle on määriteltyjen peruskontrollien (Baseline Controls) tunteminen, jotta niitä on mahdollista soveltaa suojausta vaativiin kohteisiin.

5. **Katselmointi**

   Esimerkiksi organisaatiossa voidaan tehdä kattava tietoturvakatselmointi, jonka tavoitteena on löytää organisaation tietoturvan pahimmat puutteet ja haavoittuvuudet. Katselmointi on ISO-standardin mukaisen tietoturvatietoisuuden ohjelman mukaista.

   Tietoturvakatselmointi on ennalta suunniteltu formaali prosessi, jonka tavoitteena on lisätä tietämystä tietoturvaan sekä tarkastaa olemassa olevat suojaukset. Tietoturvakatselmointi muodostuu organisaation tietojenkäsittely-ympäristön, tietoresurssien, käytettyjen suojausten sekä järjestelmän haavoittuvuuksien ja uhkien arvioinnista. Katselmointiin sisältyy myös kerättyjen tietojen analysointi sekä tarvittavien suositusten tekeminen, tavoitteena tietojenkäsittely-ympäristön turvallisuuden parantaminen.

   Tietoturvakatselmoinnissa käydään läpi esim. verkon laitteet sekä ulkoa Internetin kautta että organisaation sisäverkossa, palomuurin sisäpuolella. Teknisen tarkastuksen lisäksi käydään läpi toimitilat ja haastatellaan henkilökuntaa. Haastatteluissa halutaan selvittää henkilöstön yleinen tietoturvataso ja -tietoisuus.

Riskien arviointi

Riskien arviointi on niiden järjestelmällisten toimenpiteiden muodostama kokonaisuus, joiden avulla yritys pyrkii arvioimaan löydettyjen tai havaittujen ei-toivotulla tavalla vaikuttavien tapahtumien seurauksia.

Arvioinnilla selvitetään löydettyjen riskien toteutumisen todennäköisyys ja niiden toteutuessaan aiheuttamat vahingot. Lisäksi selvitetään, onko uhkan poistaminen yleensä mahdollista. Tutkittaessa mahdollisia vahinkoja tulee huomioida myös välittömät ja ei-aineelliset sekä sidosryhmille aiheutuvat vahingot.

Riskien arviointiin sisältyy seurausvaikutusten arviointi, jos jokin ei-toivottu tapahtuma toteutuu ja myös siihen liittyvä raportointi yrityksen johdolle.

Riskianalyysi

Yksityiskohtainen tekninen tutkintaprosessi, jossa selvitetään tutkinnan kohteeseen kohdistuvat ei-toivotut tapahtumat. Se on teknisempi käsite kuin riskien arviointi ja siihen kuuluu yksityiskohtaisempia työvaiheita.

Esimerkki: tietokonevirusten torjunta

> **Riskien hallinta**
>
> Yrityksen lähiverkko muodostuu 100 työasemasta. Jokaisessa työasemassa on tietokonevirusten torjuntaohjelmisto, jolla estetään tietokonevirusten pääsy ja leviäminen yrityksen työasemiin.
>
> Riskien hallinnasta on päätetty, että tietokonevirusten torjunta on erittäin tärkeä osa toimintaa ja siksi kaikissa työasemissa on oltava automaattinen tietokonevirusten torjunta. Riski on otettu tietoisesti hallintaan automatisoidulla virustorjunnalla, koska yritys on ymmärtänyt tietokonevirusten luonteen ja laajuuden toiminnassaan (laaja virustartunta voi pahimmassa tapauksessa tuhota kaikki yrityksen työasemien sisältämät tiedot, mistä seuraa ongelmia liiketoiminnan jatkamiselle) sekä alentanut viruksista aiheutuvaa riskiä hyväksymälleen tasolle tietokonevirusten torjunta-ohjelmistolla.
>
> **Riskien arviointi**
>
> Riskien arvioinnilla pyritään arvioimaan kuvitteellisen tilanteen seurauksia liiketoiminnalle, mikäli vaarallinen tietokonevirus on levinnyt kaikkiin yrityksen työasemiin ja tuhonnut osan tai kaikki työasemiin tallennetut tiedot. Arvioinnin tuloksista kerrotaan yrityksen johdolle selkeän dokumentoinnin avulla.
>
> **Riskianalyysi**
>
> Tällä pyritään selvittämään kaikki ne yksittäiset tilanteet, joissa vaarallinen tietokonevirus voi levitä yrityksen työasemiin.
>
> Tällaisia tilanteita voivat aiheuttaa esim. sähköpostilla tai muistitikuilla yrityksen työasemiin siirrettyjen sanomien liitetiedostot tai muut viruksia sisältävät tiedostot ja www-sivuihin upotetut haittaohjelmat.

Riskilaskennan ongelmia

- Tilastojen puuttuminen: Yritykset harvoin huomaavat joutuneensa uhreiksi ja he myös harvoin raportoivat tietoturvaongelmistaan.

- Menetysten arvottamisen vaikeus: Esimerkiksi maineen tai markkinaosuuden menetyksen vaikutukset euroina?

Tietoriskien priorisointi

Tietoturvariskit priorisoidaan käyttäen esim. riskiluokitusta: korkeimman riskin haavoittuvuus, keskitason haavoittuvuus ja matalin haavoittuvuus:

- Korkeimman riskin haavoittuvuus tarkoittaa, että yksittäinen tietokone tai tietoverkko on haavoittuvainen niin, että kyseinen tietokone tai tietoverkko voidaan ottaa haltuun haavoittuvuutta hyväksikäyttäen. Tällaiset haavoittuvuudet tulisi korjata välittömästi.

- Keskitason haavoittuvuus mahdollistaa jossakin määrin luottamuksellisen tiedon keräämisen, joka saattaa mahdollistaa tietokoneen tai tietoverkon korkeamman riskiluokan haavoittuvuuden löytymisen. Nämä haavoittuvuudet eivät siis suoranaisesti vaaranna verkon tietoturvaa, mutta väärinkäytettynä voivat aiheuttaa esimerkiksi toimintahäiriöitä tai peittää tietomurron yritykset. Keskitason haavoittuvuus -tietoja ovat esimerkiksi käyttäjätunnukset tai laitteistojen käyttöjärjestelmäversiot.

- Matalimman tason haavoittuvuus mahdollistaa tiedon keräämisen tietokoneesta tai tietoverkosta, mutta se ei ole sellainen riski, joka voisi suoranaisesti johtaa tietomurtoon.

Esim. tietoturvakatselmoinnin tuloksina saadaan tietoa sekä siitä mikä on hyvin että mihin haavoittuvuuksiin tulisi kiinnittää huomiota. Katselmoinnin tuloksena syntynyt raportti on aina luottamuksellinen. Tietoturvakatselmoinnissa tulee käydä läpi kaikki haavoittuvuudet ja korjata ne vastaamaan yleistä haluttua tietoturvatasoa.

Haavoittuvuuksia tarkasteltaessa tulee kuitenkin myös pohtia esimerkiksi palvelimen käyttötarkoitus. Ovatko sen mahdolliset haavoittuvuudet tahattomia vai välttämättömiä asetuksia järjestelmän toiminnan kannalta?

Katselmoinnista saadussa raportissa annetaan korjausehdotuksia. Esimerkiksi kehotetaan tekemään korjauksia kuten loppukäyttäjien salasanat on järjestelmän toimesta pakotettava vanhenemaan 60 päivän välein tai uudet virustorjuntapäivitykset tulee päivittää automaattisesti.

Mittavat turvallisuusratkaisut ja niihin sijoitettu työpanos voivat olla hyödyttömiä, ellei ratkaisujen luotettavuutta ole tarkistettu.

Huomattava että jotkin tietoturvallisuuspalvelut ovat niin kriittisiä, että niiden käyttöön hyväksymisen perustana on oltava oma asiantuntemus.

Tietoturvasuunnittelu

Organisaation ns. tietoturvallisuussuunnitelmassa kerrotaan suojaamisen periaatteet. Koska se sisältää tarkkoja kuvauksia suojausten toteutuksesta, on suunnitelman valmistelu, ylläpito ja päivittäminen vastuutettu yleensä eri alojen teknisille asiantuntijoille. Se sisältää konkreettisessa muodossa ne käytänteet, joiden avulla haluttuun tietoturvallisuuden tasoon pyritään ja siksi se luokitellaan joko luottamukselliseksi tai salaiseksi. Käytänteet voivat olla luonteeltaan teknisiä tai ei-teknisiä. Suunnitelma pyritään tekemään keskipitkälle aikavälille (2-5 vuotta), mutta organisaatiossa tapahtuvat muutokset voivat edellyttää sen suhteellisen nopeaakin päivittämistä.

Keskeisin tietoturvasuunnittelun sisältöä ohjaava **yleisstandardi** on kansainvälisen standardoimisjärjestön ISO:n (International Organization of Standardization) yleinen tietoturvallisuuden menettelytapaohje (code of practice) 17799 eli ISO/IEC 17799:fi (engl. 27002:ksi) ja ISO/IEC 27001. Uudet standardit pohjautuvat vuonna 2005 päivitettyihin BS 7799 standardeihin.

- Standardin ensimmäisessä osassa on suuntaviivat ja yleisperiaatteet tietoturvanhallintaan, kuten riskianalyysi ja riskien evaluointi sekä riskien käsittely, turvallisuuspolitiikka, tietoturvallisuuden organisointi, tietoaineistojen luokitus ja valvonta, tietoturvallisuus henkilöstön kannalta, fyysinen turva ja turva ympäristöä vastaan, tietokoneiden ja tietoverkkojen hallinta ja järjestelmään pääsyn valvonta.
- Standardin toisessa osassa esitetään tietoturvallisuuden hallintajärjestelmiä koskevia vaatimuksia, kuten hallintakehyksen luominen, toteuttaminen, dokumentointi, dokumenttien valvonta ja tallenteet. Samoin esitetään valvontatoimet eriteltyinä.
- Kyseiset standardit ovat luonteeltaan ei-teknisiä. Niissä ei siis kuvata kuinka suojaukset teknisesti toteutetaan vaan ainoastaan vaatimukset tietoturvalle. Toteuttamalla standardissa vaaditut suojaukset ja täyttämällä siinä esitetyt vaatimukset voi yritys hankkia itselleen ko. tietoturvasertifikaatin.

ISO-turvastandardin lisäksi on lukuisia muitakin standardeja (www.iso.org tai www.sfs.fi).

Common Criteria (CC) eli ISO 15408: Evaluation Criteria for IT Security. Määrittelee laitteiden ja ohjelmistojen turvaominaisuuksia niin, että ne voidaan testata ja niille voidaan antaa turvaluokitus 1-7.

Lisäksi yleinen standardi on **COBIT** (Control Objectives for Information and related Techonology). Se linkittää tietoturvan ja muun IT-hallinnon. Standardi sisältää dokumentin COBIT Security Baseline.

Riskin hallitsemisen keinoja

- Riskin poistaminen
    - usein lähes mahdotonta; runsaasti ylimääräistä työtä ja kustannuksia vaativaa
    - lopetetaan riskialtis toiminta kokonaan tai siirretään toiminta alihankkijalle
    - riskin poistuminen on vaikea osoittaa, esim. riskihenkilön irtisanominen
- Riskin pienentäminen
    - yleisin tapa hallita tietoturvallisuusriskejä on pyrkiä pienentämään mahdollisia seurausvaikutuksia
    - yrityksen omat toimenpiteet, kuten suunnittelu, ohjeistus, koulutus, investoinnit
    - nykyiset suojausmenetelmät luonteeltaan sellaisia, että niillä ei voida poistaa riskejä kokonaan, voidaan ainoastaan pienentää niitä merkittävästi, esim. palomuuri ja virustorjunta
- Riskin siirto
    - toiselle osapuolelle kuten vakuutusyhtiölle
    - ei kata koko riskiä, esim. tulipalossa tuhoutunut tietoaineisto varmuuskopioineen
- Riskin hyväksyminen

- otetaan tietoinen riski esim. silloin kun riski tai sen toteutumistodennäköisyys on pieni tai sille ei yksinkertaisesti voida tehdä mitään, esim. ulkomailla olevien toimintojen muuttuminen poliittisen tilanteen vuoksi

Tavoitetaso

Riskienhallinnassa on hyvä pitää mielessä, että täydellisen turvallisuuden tavoittelu on lähes aina liian kallista suhteessa hyötyihin. *Suojaukset täytyy suhteuttaa mahdollisiin vahinkoihin.* Tällöin 10 euron arvoista tietoa ei kannata suojata 100 euron suojauksella. Lisäksi täydellinen tietoturva saattaa haitata ja hidastaa tietojärjestelmien käyttöä.

Alla olevasta kuvasta nähdään kuinka pyrittäessä 100 % turvallisuuteen, turvatoimien kustannukset nousevat helposti liian korkeiksi. Kustannusten on oltava tasapainossa hyötyjen kanssa.

Kuva: Optimaalitaso (Lähde: Olovsson T.: Structured Approach to Computer Security)

Käytännössä 100 % turvallisuus on mahdoton saavuttaa! Syy tähän on se, että tietoturvan lähestyessä 100 %:a, käytettävyys lähestyy nollaa ja kustannukset ääretöntä.

Tavoitetasoon vaikuttavat lainsäädännön vaatimukset, yrityksen toimiala, yrityksen toiminnan jatkumiseen tarvittava vähimmäistaso, asiakkaiden vaatimukset ja käytettävät resurssit (laitteet, henkilöstö, raha).

Riskien hallinnassa ongelmia aiheuttavat mm. tietojärjestelmien ja tietoliikennejärjestelmien monimutkaisuus, sekä teknologian että yhteiskunnalliset muutokset ja käsiteltävien asioiden abstraktisuus. Ongelmina nähdään myös tilastotietojen puute ja toisinaan arvottamisen vaikeus.

Kuvan optimitasoa on vaikea arvioida, koska muuttujia on niin monia: uhka, uhkan todennäköisyys, omat haavoittuvuudet, suojautumiskeinot ja niiden hinta, suojausten taso ja tehokkuus. Vaikka jäännösriskiä on vaikea arvioida onnistunut tietoriskien hallinta vähentää vahinkoja ja nopeuttaa yrityksen toipumista vahingoista.

Suojauskeinot

Suojauskeinoja voidaan ryhmitellä vaikkapa seuraavasti:

1. **Ennalta ehkäisevillä** suojauskeinoilla yritys pyrkii suojautumaan erilaisia riskejä vastaan ennen niiden toteutumista. Niillä keinoilla toteutetut suojaukset tarjoavat parhaan suojan erilaisia uhkia vastaan, koska niillä estetään uhkatilanteiden syntyminen.

2. **Havaitsevilla** suojauskeinoilla uhkia voidaan myös torjua tehokkaasti. Nämä suojauskeinot auttavat tunnistamaan syntyviä tai jo toteutuneita uhkatilanteita, tietoturvallisuusongelmia ja väärinkäytön mahdollisuuksia.
3. **Korjaavia** suojauskeinoja tarvitaan silloin, kun uhkatilanne on jo toteutunut ja siitä on aiheutunut vahinkoja. Korjaavilla suojauskeinoilla voidaan joko korjata jo syntyneitä vahinkoja tai rajoittaa syntyviä vahinkoja.

Eri suojauskeinot voivat kuulua useampaan ryhmään. Esimerkiksi viruksentorjunta on sekä ennaltaehkäisevä, havaitseva että korjaava suojauskeino.

Riskien torjunnan toteutus ja testaus

Tehdyt suunnitelmat täytyy tietenkin toteuttaa ja toteustus testata. Lisäksi on arvioitava tehdyt ja tulevat toimenpiteet, järjestelmien ja ympäristön muuttuminen. Tehty muutos saattaa aiheuttaa haavoittuvuuden johonkin toiseen kohtaan.

Toipumissuunnitelma

Riskien hallintaa kuuluu aina myös toipumissuunnitelma. Sen on oltava kirjallisessa muodossa ja ajantasainen. Toipumissuunnitelma ei estä vahinkoja, mutta se auttaa organisaatioita rajoittamaan vahinkoja ja toipumaan vahingoista nopeasti ja hallitusti sekä välttämään suunnittelemattomista ja hallitsemattomista toipumistoimenpiteistä aiheutuvat lisävahingot. Sen tulisi sisältää mm.:

- Kriittisten sovellusten ja tietojärjestelmien määrittely
- Pisin mahdollinen keskeytys kriittisille toiminnoille
- Hahmotellaan todennäköisimmät vahingot
- Toipumisorganisaatio ja vastuiden määrittely
- Sidosryhmien yhteyshenkilöt (laitteisto, ohjelmisto, huolto, asiakkaat, yms.)
- Sopimukset em. sidosryhmien kanssa
- Ohjeet tarvittavien toimenpiteiden tekemisestä
- Keskeytysvakuutukset
- Vahingon rajoittamismenettelyt
- Tiedottaminen ja asiakkaisiin liittyvät toimenpiteet
- Toimenpiteet toiminnan uudelleen käynnistystä varten
- Tarvittavat testaukset käynnistyksen jälkeen
- Suunnitelman testaus ja koulutussuunnitelma
- Suunnitelman päivitys- ja ylläpitovastuu

Koulutus, ohjeistus, ylläpito

Toimintaohjeet

Yrityksen tietoturvallisuuden **toimintaohjeet** tai **käytänteet** ovat yksityiskohtaisia, päivittäiseen toimintaan liittyviä käytännön soveltamisohjeita **käyttäjiä** varten. Tarkkoja toimintaohjeita, jotka voivat muuttua tarvittaessa nopeastikin.

Esim. **käyttäjätunnusten ja salasanojen ohjeistus**:

- Politiikka: Yrityksen kaikissa tietojärjestelmissä käytetään henkilökohtaisia käyttäjätunnuksia ja vahvoja salasanoja.

- Standardi: Tietojärjestelmän käyttäjätunnus muodostetaan kaikissa tapauksissa satunnaisgeneraattorin avulla ja sitä ei voi johtaa esimerkiksi henkilön nimestä. Tietojärjestelmän salasanassa on vähintään 8 merkkiä kaikissa järjestelmissä ja se vaihdetaan säännöllisesti.
- Toimintaohje: Samaa käyttäjätunnusta käytetään kaikissa niissä yrityksen tietojärjestelmissä, joita henkilöllä on oikeus käyttää. Salasanan tulee sisältää kirjaimia ja numeroita ja se vaihdetaan automaattisesti 2 kuukauden välein.

Ohjeistuksien suunnittelussa ja toteutuksessa on huomioitava mm.

- Yrityksen liiketoiminnan vaatimukset
- Ohjeistuksen on oltava käytännöllinen ja helposti ymmärrettävä
- Ohjeistuksen on keskityttävä liiketoiminnan keskeisiin asioihin
- Ohjeistuksen on katettava kaikki liiketoiminnan keskeiset osa-alueet
- Yksittäisten ohjeiden on oltava riippumattomia muista ohjeista.

Tietoturvatietoisuuden kohottaminen

Joskus sanotaan että tietoturvasta huolehtiminen on liian työlästä. Tämän ajattelun seurauksena se jätetään helpommin huomiotta. Kuinka sitten saadaan työntekijät panostamaan tietoturvallisuuteen. Menetelmiä:

- Ihmisten huomio kiinnitetään turva-asioihin (mm. uhkat; miksi tärkeää?)
- Hankitaan käyttäjähyväksyntä (mm. lainsäädäntö; perustelut, seuraukset; koulutus)
- Käyttäjät saadaan oppimaan ja sisäistämään tietoturvatoimenpiteiden välttämättömyys

Tietoturvatietoisuuden ohjelman tulisi sisältää ainakin seuraavat kohteet:

1. Yrityksen tietoturvapolitiikkaan liittyvät vaikuttimet samoin kuin politiikkaan, ohjeisiin, direktiiveihin ja riskien hallinnan strategiaan liittyvät laajennukset, joiden avulla riskeihin ja turvatoimenpiteisiin liittyvät asiat voidaan ymmärtää syvällisemmin.
2. Tietoturvaohjelman/suunnitelman toteuttaminen ja turvatoimenpiteiden tarkistukset.
3. Tietojen suojaamiseen liittyvät perustarpeet.
4. Luokitusjärjestelmän perustamisen, joka sisältää informaation suojaamisen.
5. Tarve raportoida tietoturvaloukkauksista ja niiden yrityksistä ja tutkia niitä.
6. Turvallisuuteen liittyvien parannusten merkitys hyväksikäyttäjille ja yritykselle.
7. Menettelytavat, vastuut ja työnkuvaukset.
8. Turvatarkastukset (auditointi) ja joustavat tarkastukset (chek).
9. Muutoksen- ja rakenteenhallinta.
10. Seuraukset toiminnasta, joka tapahtunut ilman valtuutusta.

Tietoturvatyön tuloksista

Ohjeistuksen toimivuutta ja tehokkuutta on voitava mitata jollakin järkevällä tavalla, jotta voidaan kehittää niistä mahdollisesti löytyviä puutteita tai heikkouksia. Toisaalta on syytä varoa, että työntekijöiden koko työskentelyprosessia ei sidota liiaksi kaikenlaisiin ohjeisiin ja rajoituksiin. Asioiden hoitaminen käskyttämällä aiheuttaa usein vastustusta. Osa tietoturvaohjeista ja säännöistä on kuitenkin sarjassa ns. pakko noudattaa. Näistä säännöistä ei sallita poikkeuksia ja niiden rikkomisista tulee

seurata sanktiot.

Loppukäyttäjiä varten teknisten tietoturvaratkaisujen tulisi olla mahdollisimman läpinäkyviä, eli loppukäyttäjän ei tarvitsisi erikseen miettiä ja ottaa kantaa suojausmenetelmien tarpeellisuuteen. Ratkaisujen tulisi olla mahdollisimman helppokäyttöisiä ja / tai huomaamattomia.

Vaikka organisaatiossa on oltava tietoturvapolitiikka ja -ohjeet, joita on kehitettävä (jatkuva prosessi), niin ensimmäinen askel organisaation toiminnassa tietoturvan suuntaan on se, että jokainen organisaation työntekijä tuntee perusteellisesti omat tietojenkäsittelylaitteensa ja osaa käyttää niitä asianmukaisesti. Lisäksi käyttäjiltä edellytetään, että he tuntevat käyttämänsä ohjelmistot ja/tai ohjelmointiympäristöt (ns. hyvän tietojenkäsittelytavan avulla voidaan ehkäistä tietojärjestelmien virhetilanteita). Samalla kun organisaatio nostaa työntekijöiden ammattitaitoa, se kehittää työntekijöiden tietoturvaosaamista.

Organisaatiossa tulee tavoitella positiivista ja avointa työilmapiiriä. Oikean ilmapiirin luominen ja työntekijöiden oikeiden asenteiden omaksuminen edesauttaa työntekijöiden sitoutumista ja tietoturvatietoisuutta sekä helpottaa tietoturvaratkaisujen kehittämistä.

2.4 Ulkoistaminen

Kun toimintoja ulkoistetaan, annetaan osa tai kaikki yritykselle kuuluvat toiminnot ulkopuolisen palvelun tarjoajan hoidettavaksi. Ulkoistamisella pyritään hankkimaan kustannussäästöjä, jotta pystytään keskittymään perusliiketoiminnan hoitamiseen, koska usein ajatellaan, ettei kaikkea voida itse hoitaa hyvin. Tyypillisiä ulkoistamistoimintoja ovat yrityksen tietojenkäsittely, tietoliikenne sekä talousasioiden hoitaminen tai tietoturvallisuus.

Tietoturvan ulkoistamisen syitä: Ajatellaan esimerkiksi, että tietoturva hoitaminen on kallista ja vaikeaa, eikä se tuota (rahaa) eikä tuo varsinaisesti lisäarvoa siihen toimintaan johon liiketoiminnassa on keskitytty.

Tietoturvallisuuden ulkoistamisen seurauksena

- Tietoturvan hallinta muuttuu aikaisempaa vaikeammaksi, koska tilanne ei ole enää välittömässä seurannassa
- Ulkoistamisen tuomien hyötyjen ja haittojen arviointi ja mittaaminen on vaikeampaa
- Vastuu tietovarastoista ja niiden suojaamisesta on siirretty ulkopuoliselle. Tästä seuraa että yrityksen luotettava vahvasti ulkopuolisen toimintaan
- Väärinkäytösten tutkiminen vaikeaa, koska yrityksellä ei yleensä ole valvontaa ulkopuolisen toimittajan turvajärjestelmiin
- Ei voida varmistua, että ulkopuolinen ei käytä hallussaan olevaa yrityksen tietämystä sitä vastaan.

Tietoturvallisuusasioiden hoidon ulkoistamiseen liittyy monia vaikeasti hallittavia asioita ja potentiaalisia riskejä ja siksi niitä ei ole syytä ulkoistaa ilman hyviä perusteluja. Ulkoistetut toiminnot ovat yrityksen suoran kontrollin tavoittamattomissa, vaikka yritys itse viime kädessä vastaa niiden virheistä.

Ulkoistamisen hyötynä nähdään kustannussäästöt. Säästöt löytyvät siitä, että palveluntarjoajan (toiminnan volyymi) useille yrityksille tekemä "samanlainen" työ tuo säästön (vrt. jos jokainen tekisi yksin ja erikseen koko työn). Toisaalta riski kasvaa kun palveluntarjoaja, joka on ulkopuolinen yritys, käsittelee myös kilpailijan tietoja!

Kun tietoturvatoimintoja ulkoistetaan, on palveluntarjoajan ja yrityksen tehtävä tietoturvallisuuden **palvelu- / varmistamissopimus**, jossa ulkopuolinen sitoutuu noudattamaan sovittuja suojauksia ja tietoturvarutiineja. Ulkopuolinen ei saa esim. käyttää toimintojen hoitamiseen alihankkijoita ilman ulkoistajan suostumusta ja ulkopuolinen yritys sitoutuu ilmoittamaan ulkoistajalle toimintoihin tai tietoihin kohdistuneista tietoturvarikkomuksista.

Itse palvelusopimuksen on oltava tarkka ja kattava myös lainsäädännöllisesti. Palvelusopimuksen sisällössä on määriteltävä kohde ja selkeät rajat: mitä kuuluu kummallekin osapuolelle, mitkä ovat rajapinnat (kuka kommunikoi kenenkin kanssa, kerättävät lokitiedot, vastuu riskeistä, palomuuri yms.). Siinä on määriteltävä palvelutaso eli esim. kuinka nopeasti uhkatilanteet on käsiteltävä, miten ja kuinka nopeasti tiedotettava jne.

Lisäksi yrityksen on pystyttävä erittäin lyhyellä varoitusajalla tarkistamaan (auditointi), että palveluntarjoaja on tehnyt toteutuksen sopimuksen edellyttämällä tavalla.

Ongelmina nähdään usein se, ettei yrityksessä tiedetä mitä vaatia. Mitä laitetaan palvelusopimukseen (sisältö, paljonko maksetaan ja kuinka tärkeä asiakas ollaan)? Kriisitilanteessa palveluntarjoaja joutuu

venymään moneen suuntaan!

Palvelusopimuksen tulee olla pitkäaikainen ja sitä on päivitettävä ajan kuluessa. Vaitiolosopimus tehdään useiksi vuosiksi eteenpäin.

Kontrollia ei voi ulkoistaa!

3 Tietosuoja

Tietojen suojauksen tarve voi johtua tarpeesta suojata yrityssalaisuudet. Toisaalta tiedon suojaus voi olla lainsäädännön velvoittamaa. Eräs tällainen laissa suojeltu oikeus on kansalaisten yksityisyys.

Huomatkaa käsitteiden ero: tietoturva suojaa tietoja (yleisesti), tietosuoja suojaa ihmisiä (lainsuoja ihmisten tiedoille).
On makuasia kumpaa pidämme yläkäsitteenä: yritysnäkökulmasta tietosuoja on tietoturvan alakäsite ja oikeustieteiden näkökulmasta tietosuoja on yläkäsite ja tietoturva alakäsite.

Yksityisyys

Yksityisyyden käsitteen oikeudellinen merkitys on suhteellisen uusi verrattuna alun perin perustavaa laatua olevaan jakoon yksityisyys - julkisuus (vrt. yksityiselämä). Oikeudellisesti se on alkanut kehittyä varhaisempien YK:n ihmisoikeusjulistusten (12 artikla) ja Euroopan ihmisoikeussopimuksen (8 artikla) myötä. Suomalaisessa lainsäädännössä käsitesekaannus yksityisyyden ja yksityiselämän suojan välillä näkyy siten, että perustuslaissa puhutaan yksityiselämän suojasta. Sitä vastoin yksityisyys on peruskäsitteenä henkilötietolaissa sekä rikoslaissa. Yksityiselämä on niitä sovellettaessa osa yksityisyyttä. Tietosuoja on yksityisten tietojen suojaamista.

Yksityisyys on siis perusoikeus. Teknologian kehittyessä sekä tietotekniikan käytön yleistyessä yksityisyyden loukkaamisen riskit lisääntyvät. Yhteiskunnan muuttuminen verkkoyhteiskunnaksi on edelleen lisännyt riskejä avoimissa tietoverkoissa erityisesti siellä, missä tietoturva on vaatimattomalla tasolla. Tietoyhteiskunnassa yksityisyyden turvaaminen ja ylläpito vaatii monien eri tahojen tietämystä ja huolellisuutta monissa eri vaiheissa. Uhkana on yksityisyyden katoaminen. Nämä seikat ovat johtaneet myös yksityisyyteen liittyvän oikeudellisen sääntelyn merkittävään kasvuun ja monimuotoistumiseen viime vuosina.

Yksittäisestä ihmisestä voi olla tietoja sadoissa eri rekistereissä eikä tuo yksilö todellakaan välttämättä tiedä, mihin kaikkiin rekistereihin hänen tietonsa (ja mitkä kaikki tiedot) ovat päätyneet. Rekisterit ovat tietokannoissa, jotka puolestaan ovat usein palvelimilla, joista on yhteys tietoverkkoihin. Ja kaikkihan me jo varmaan tiedämme kuinka nopeasti ja helposti tietoa voidaan siirtää tietoverkoissa. Tämä yhtälö luo helposti pelottavan mielikuvan Orwellimäisestä 'Isoveli valvoo' -yhteiskunnasta, jossa yksilön tiedot ovat kaupan eniten tarjoavalle ja sellainen käsite kuin yksityisyys on kadonnut.

Onneksi tietojen suojaaminen ei kuitenkaan ainakaan vielä ole päässyt täysin riistäytymään käsistä, sillä yksilön suojana ovat erilaiset normit ja käytänteet sekä tietoturvallisuus. Tietosuojan toteutumista valvovat tietosuojavaltuutettu ja tietosuojalautakunta.

Tietosuojan toteutumista pyritään suojaamaan juristien ja IT-tekniikoiden taholta; tosin tällöin tarkoitetaan tietosuojasta puhuttaessa usein eri asioita. Lakimiehet tarkoittavat henkilörekistereihin liittyviä asioita, IT-asiantuntijoille ja ”insinööreille” tietosuoja tarkoittaa kaikkien rekistereiden koskemattomuutta ulkopuolisilta tunkeutujilta. Näistä näkökulmaeroista johtuen tietosuojan järjestäminen on juristeille säädösten ja määräysten valmistelua ja IT-asiantuntijoille tietojärjestelmän teknisiä ratkaisuja ja viritelmiä, ja jatkuvaa kilpajuoksua rikollisten kanssa.

3.1 Tietosuojaan liittyvää lainsäädäntöä

Tietosuoja on yksilön, ihmisoikeuksien, perusoikeuksien suojaa, ja osa ihmisen oikeudellista kunnioittamista. Tämä merkitsee käytännössä rekisteri-, rekisteröinti- ja informaatiovapauden merkittäviä rajoituksia.

Historiallisesti tietosuoja liittyy perinteiseen kotirauhaan ja ihmisen 'oikeuteen olla yksin'. Vastaavia oikeuksia ovat esim. kirje- ja puhelinsalaisuus, salassapitosäännökset (mm. lääkäri, poliisi) ja kunnianloukkaussäännökset. Historia liitetään nykyään mm. tietokoneiden ja tietojärjestelmien kehitykseen. Kansallinen ja kansainvälinen lainsäädäntö asettaa sekä velvoitteita että rajoituksia tietokoneiden, ohjelmistojen ja verkkoyhteyksien käytölle. Huomatkaa, että harhaanjohtavasti englanniksi oikeudellisesti käsite tietosuoja on data protection ja Ruotsissa tietosuojaan liittyvä laki on datalagen.

Suomessa tietoturvallisuuden järjestämiseen ja tietosuojaan liittyvää lainsäädäntöä löytyy hajallaan mm. seuraavasti:

- Perustuslaki (10§ Yksityiselämän suoja, 12§ Sananvapaus ja julkisuus)
- Rikoslaki
- Henkilötietolaki ja EU:n tietosuojadirektiivi
- Sähköisen viestinnän tietosuojalaki
- Laki viranomaisten toiminnan julkisuudesta
- Arkistolaki
- Laki ja asetus yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta
- Laki oikeudenkäynnin julkisuudesta
- Laki yksityisyyden suojasta työelämässä
- Viestintämarkkinalaki
- Laki tietoyhteiskunnan palvelujen tarjoamisesta
- Laki sähköisestä asioinnista viranomaistoiminnassa
- Laki sähköisestä allekirjoituksesta

Yksityisyyden katsotaan olevan tällä hetkellä julkisuutta voimakkaampi periaate, vaikka ne hallitusmuodossa ilmenevätkin samantasoisina.

Yksityisyys on siis oikeutta olla yksin kotirauhan piirissä ja valvonnan ulottumattomissa. Se on oikeutta olla ihmissuhteissa, elämäntavoissa ja harrastuksissa yksin (ns. sosiaalinen yksityisyys) ja oikeutta pidättäytyä julkisuudesta. Se koskee myös yksityisyyttä työelämässä. Oikeus tietosuojaan on oikeutta päättää itseään koskevan informaation tarkastamisesta, tallentamisesta, käytöstä ja luovuttamisesta. Tiedollinen omitusoikeus on omaan nimeen, kuvaan ja hahmoon liittyvää. Lisäksi se on oikeutta tulla arvioiduksi oikeassa valossa.

Henkilötietolaki

Henkilötietolain (523/1999) 1 §:ssä on lain tarkoitus: "Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista".

Yksilöillä on siis lähtökohtaisesti päätösvalta siihen, miten häntä koskevia tietoja saa käyttää. Henkilötietolain tarkoituksena on siis suojata ihmisten oikeutta yksityisyyteen ja taata oikeusturva henkilötietoja kerättäessä, talletettaessa, järjestettäessä, käytettäessä, siirrettäessä, luovutettaessa, säilytettäessä, muutettaessa, yhdistettäessä, suojattaessa ja poistettaessa.

Henkilötietojenkäsittelyn on perustuttava rekisteröidyn suostumukseen. Henkilöllä on oikeus tietää ja päättää itseään koskevien tietojen käytöstä. Jokaisella on oikeus tulla arvostetuksi oikeiden ja oleellisten tietojen perusteella. Lakiin sisältyy siis huolellisuusvelvoite ja käyttötarkoitussidonnaisuus. Arkaluonteisia henkilötietoja koskee käsittelykielto joka liittyy mm. syrjintäkieltoon ja oikeuteen tulla yhdenvertaisesti kohdelluksi.

Laki koskee yritysten, viranomaisten, järjestöjen, muiden yhteisöjen ja yksityisten henkilöiden toimintaa. Se koskee jokaista työnantajaa koosta riippumatta ja sitä sovelletaan myös muualla kuin työpaikoilla. Lain ulkopuolelle suljetaan kuitenkin henkilötietojenkäsittely, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisiin ja tavanomaisiin yksityisiin tarpeisiin.

Henkilötietolaki elää 2010 –luvun alkupuolella murrosvaiheessa. Jo pitkään henkilötietoja on tallennettu yhä enenevässä määrin erilaisiin rekistereihin mm. julkishallinnossa. Henkilötiedoista on tullut myös usealle yritykselle osa ydinliiketoimintaa. Lisäksi ihmiset tuottavat itse valtavia määriä usein arkaluonteisiakin henkilötietoja esim. sosiaalisessa mediassa ja mobiiliapplikaatioiden avulla.

Tällä hetkellä henkilötietojen siirto EU:n ulkopuolelle on säädelty tapauskohtaisesti. Teknologisen kehityksen ja globalisaation vuoksi EU:n tietosuojadirektiiviin, monien maiden ja myös Suomen henkilötietotolakiin on lähivuosina odotettavissa muutoksia.

Tietojen tallennus vrt. palvelimen sijaintimaa ja ko. maan tietosuoja??

Tutustu tarkemmin henkilötietolakiin osoittessa http://www.finlex.fi/ tai http://www.edilex.fi/.

Tietosuojaviranomaiset

Henkilötietojen käsittelyn lainmukaisuutta valvoo **tietosuojavaltuutettu**. Hänellä on oikeus tarkistaa ja saada tietoja henkilörekisterien pidosta. Jos lakia on rikottu, voi valtuutettu antaa ohjeita ja suosituksia tai saattaa tapauksen tietosuojalautakunnan käsiteltäväksi. Asia voidaan myös ilmoittaa syytteeseenpanoa varten. Yksittäistapauksissa tietosuojavaltuutettu voi antaa määräyksiä henkilön tarkastusoikeuden toteuttamiseksi tai virheellisten tietojen korjaamiseksi.

Tietosuojalautakunta on tärkein päätöksentekovaltaa käyttävä elin tietosuoja- ja henkilörekisteriasioissa. Lautakuntaan kuuluu seitsemän jäsentä, joista osa on oikeusoppineita ja osa tietotekniikan asiantuntijoita.

Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä (759/2004) koskee työnantajan ja työntekijän suhdetta ja on olennainen erityslaki, joka asettaa työnantajalle velvoitteita. Työntekijöiden henkilötietoja koskee ns. minimiperiaate eli jos henkilötieto ei ole välittömästi tarpeellinen, se on jätettävä käsittelemättä ja kuuluu vain työntekijälle.

Henkilötiedot on kerättävä ensisijaisesti työntekijältä itseltään tai jos ne kerätään muualta, niin työntekijän suostumuksella. Lisäksi on erityistapauksista säännöksiä (henkilö- ja

soveltuvuusarviointitestit, terveydentilan testaaminen, huumetestit, kameravalvonta ja sähköpostin suoja).

3.2 Tietosuoja ja verkkoyhteiskunta

Tietosuojan oikeudelliset ongelmat verkkoyhteiskunnassa ja Internetissä koskevat erityisesti ATK-pohjaisia henkilörekistereitä. Näiden päätyypit ovat asiakasrekisterit ja markkinointirekisterit. Huomioitava mm. että kaikki rekisteröidyt eivät ole asiakkaita.

Internet-verkon ja sen palvelujen ylläpidosta kertyviä tunnistettavia käyttäjätietoja saa käyttää vain siihen tarkoitukseen, mihin niitä kerätään eli ennen kaikkea toiminnan ja sen turvallisuuden ylläpitämiseen ja kustannusten kohdentamiseen. Kertyneiden tietojen käyttö muihin tarkoituksiin edellyttää käyttäjän suostumusta.

Henkilötietoja talletetaan yhä enemmän tietotekniikan avulla erilaisiin henkilörekistereihin, jolloin tietojen siirto ja rekisterien yhdistely on entistä helpompaa. Tietoverkkojen sähköisestä kaupankäynnistä saadaan tietoja, joista on helppo laatia erilaisia rekistereitä mm. ostotottumuksista ja maksutavoista. Tietojen kerääjällä on aina ensisijainen vastuu tietojen käsittelyn asiallisuudesta ja turvallisuudesta.

Tietojärjestelmiin tallentuu tietoja myös automaattisesti mm. evästeitä (selainasetuksia muokkaamalla voit valita hyväksytkö evästeet vai et). Tietoverkon kautta tapahtuvan asioinnin pitäisi voida yksityisyyden suojaa toteuttaen tapahtua periaatteessa anonyymisti, ellei käyttäjän tietojen kerääminen ole tarpeellista esim. tavaran tai palveluksen toimittamiseksi.

Internetin ja sen palvelujen tarjoajan tulee ottaa käyttöön tietosuojaa ja tietoturvaa tukevia tekniikoita ja välineitä. Käyttäjää on informoitava ja ohjattava käyttämään niitä, silloin kun hän esim. rekisteröityy Internet-palveluihin tai ostaa ja maksaa verkossa ja kun hänestä kerätään tietoja.

Kiusalliset suoramarkkinointiviestit eli spammit sähköpostilaatikoissa perustuvat yleensä tehokkaisiin, halpoihin sähköpostiosoiterekistereihin. Vältä siis mm. rekisteröitymästä tai antamasta sähköpostiosoitettasi tarpeettomasti. Voi yrittää myös suojautua hakukoneen tiedonkeruulta antamalla osoitteesi esim. muodossa etunimi.sukunimi@firma.fi, tunnus(at)firma.fi tai tunnus@poistatämä.firma.fi.

3.3 Rekistereiden ongelmat

Yleisesti ottaen rekistereiden ongelmia ovat:

- Väärät, vanhat tai puutteelliset tiedot: esim. kiusanteko antamalla toisten vääriä henkilötietoja tai tiedot voivat olla sinänsä oikeita, mutta ne eivät enää anna oikeaa kuvaa kohteesta (esim. nuoruuden mielipiteet, luotto-tai maksuhäiriöt). Virheellinen tieto tietorekisterissa voi aiheuttaa rekiströidylle monenlaista haittaa: esim. häiriöt tiedonkulussa tai tavoitettavuudessa virheellisistä yhteystiedoista johtuen, aiheeton luottotieto- tai maksuhäiriötieto, virheelliset tulo- ja verotustiedot, virheet tai puutteet terveystiedoissa jne.
- Arkaluonteiset tiedot, salassa pidettävät tiedot, lakisääteisesti säilytettävät tiedot
- Vanhat tiedot pysyvät rekistereissä ellei niitä sieltä poisteta. Huomioitava että rekisteröidyllä on oikeus vaatio rekisterinpitäjältä omia henkilökohtaisia tietoja nähtäväksi ja tarkastettavaksi.

Mitkä tiedot ovat arkaluonteisia? Siihen vaikuttavat monet ulkoiset seikat kuten asiayhteys ja tarkoitus mihin tietoja käytetään. Tieteellistä tutkimusta varten luovutetaan tietoja, joita suoramarkkinointia varten ei anneta.

Arkaluonteisten tietojen tallentaminen on pääsääntöisesti kiellettyä. Tällaisia tietoja ovat rotu ja etninen alkuperä, yhteiskunnallinen, poliittinen ja uskonnollinen vakaumus, rikokset ja rangaistukset, terveydentila, sairaudet, vammaisuus, hoitotoimenpiteet, seksuaalinen käyttäytyminen, sosiaalihuollon palvelujen käyttö. Tietoja voidaan käsitellä tietyin poikkeuksin.

Ihminen luovuttaa itsestään mielellään positiivista tietoja, mutta kielteisen tiedon hän haluaa pitää salassa. Esimerkiksi terve ihminen luovuttaa helposti tiedon terveydentilastaan ja rikkeetön ihminen tiedot rikosrekisteristään.

Valvonta

Rekisteröidyllä on tiettyjä oikeuksia valvoa henkilötietojen käsittelyä. Näitä ovat

- Tiedonsaantioikeus
- Oikeus saada ilmoitus luottorekisteriin talletetusta ensimmäisestä merkinnästä
- Oikeus saada tieto mistä suoramarkkinoinnissa ja markkina- ja mielipidetutkimuksessa hankitut tiedot on saatu
- Rekisterin tarkastusoikeus tietyin rajoituksin
- Oikeus vaatia korjattavaksi tai poistettavaksi virheellinen tieto ilman viivytystä
- Oikeus kieltää tietojen käsittely tiettyihin tarkoitusiin

Esimerkki: Identiteettivarkaus

Identiteettivarkaus on yleistyvä teko, jossa rikollinen saa selville vieraan henkilön tiedot ja esiintyy tämän puolesta esimerkiksi tekemällä luottokorttiostoksia tai ottamalla pikalainoja. Luottokorttitietojen kaappaaminen ja kortin käyttäminen ovat vakava tietoturvaongelma yhä lisääntyvässä nettikaupankäynnissä.

Suomessa identiteetin varmistamiseen on esimerkiksi kaupoilla, pankeilla ja viranomaisilla hyvät valmiudet. Tietorekisterit ovat kattavia ja lähes jokaiselta löytyy ja vaaditaankin viranomaisen myöntämä kuvallinen henkilöllisyystodistus. Tämä vähentää identiteettivarkauksien määrää. Verkkopankkijärjestelmä maassamme on helppokäyttöinen ja turvallinen.

Suomessa identiteettivarkauksia tehdään esimerkiksi posti- tai roskalaatikoista löytyvien dokumenttien avulla. Henkilötietojen kaappauksen riskeiltä ei kuitenkaan voida sataprosenttisesti välttyä nettiä, sähköpostia tai sähköistä asiointia käytettäessä.

4 Palvelut; uhkista ja suojauksista

Tietoturvaan kohdistuvat uhkat voitiin jakaa mm. organisaation sisäisiin ja ulkoisiin uhkiin. Vaikka monia uhkia voidaan käsitellä molemmista näkökulmista, tuo Internet ja liittyminen yleisiin tietoverkkoihin ja erilaisiin palveluihin selkeästi oman alueensa tietoturvauhkien joukkoon.

Internetin tuomat uhkat kohdistuvat tiedon luottamuksellisuuteen, eheyteen, saatavuuteen,... ja voivat liittyä hyökkäyksiin, tunkeutumiseen lähiverkkoon ja sen palvelimille, tiedon paljastumiseen, sieppaamiseen, katoamiseen, väärentämiseen, varastamiseen,... joko tahattomasti tai tahallisesti.

Uhkia vastaan suojautumiseen tarvitaan monenlaisia ei-teknisiä ja teknisiä menetelmiä. Jokainen käyttäjä on omalta osaltaan viimekädessä vastuussa tekemisistään ja oman työpaikalla olevan työasemansa tai ehkä etäyhteydessä olevan kotikoneensa tietoturvallisuudesta.

Työpaikalla tai esim. oppilaitoksessa IT-osaston mikrotukihenkilöt huolehtivat työasemien perusturvallisuudesta: käyttäjätunnuksista, resurssien ja oikeuksien jakamisesta, virustorjunnasta, varmuuskopioinnista,...

Kannettavien tietokoneiden ja muiden mobiililaitteiden tietoturva tulee huomioida erikseen, koska niihin kohdistuu tavallisten työasemien uhkien lisäksi aivan omat uhkat. Tällaisia ovat mm. varastaminen julkisilta paikoilta, katoaminen, rikkoontuminen putoamisen seurauksena,...

Kannettavien laitteiden ja etäyhteydessä olevien kotikoneiden turvallisuus tulee huomioida erityisesti: ne ovat usein organisaation automaattisten suojaustoimenpiteiden ulottumattomissa. Internetin kautta kulkevat turvattomat tietoliikenneyhteydet vaativat myös omat suojausmenetelmänsä.

Usein etätyöntekijän tulee tavallisen kotikoneen käyttäjän lailla huolehtia koneensa turvallisuudesta monin osin itse.

4.1 Internet

Internet koostuu eri organisaatioiden itsenäisistä aliverkoista ja näitä yhdistävästä maailmanlaajuisesta runkoverkosta. Aliverkot kytketään toisiinsa reitittimien ja tietoliikenneyhteyksien avulla.

Reititin on laite, joka vastaanottaa tietoliikennepaketteja. Se tuntee oman aliverkkonsa koneet ja tietää, mihin suuntaan omasta verkosta ulos tarkoitetut tietoliikennepaketit on lähetettävä. Verkon luotettavuuden lisäämiseksi verkossa on useita vaihtoehtoisia reittejä, joita voidaan käyttää silloin, jos jokin yhteys on poikki.

Verkolla ei ole yhtä omistajaa, vaan se koostuu tietoliikenneoperaattoreiden ja muiden tietoliikennepalvelutarjoajien (ISP, Internet Service Provider) toisiinsa kytketyistä, itsenäisesti hallinnoimista verkoista. Sekä organisaatioiden lähiverkot että yksityisten kotikäyttäjien tietokoneet yhdistetään tietyn palveluntarjoajan kautta Internet-runkoverkkoon.

Tietoliikenneverkoissa liikennöintiin käytetään ns. tietoliikenneprotokollia, joista tärkeimmät IP-perusprotokollat ovat ICMP (Internet Control Message Protocol), UDP (User Datagram Protocol) ja TCP(Transmission Control Protocol)-protokolla. Näistä tärkein on TCP.

IP-protokolla

Tiedonsiirto Internetin koneiden välillä tapahtuu TCP/IP-protokollan eli -yhteyskäytännön avulla. Lähetettävä tieto jaetaan paketeiksi, joihin liitetään tieto vastaanottajasta. Tämän tiedon perusteella tietoliikennepaketit liikkuvat Internetissä jotakin reittiä pitkin päämääräänsä. TCP/IP sisältää laajan valikoiman protokollia, joihin mm. Internetin palvelut (www, sähköposti jne.) perustuvat. TCP/IP:hen kuuluvia yhteyskäytäntöjä ovat mm. seuraavat:

HTTP (Hypertext Transfer Protocol): käytetään hypertekstin siirrossa palvelimen ja käyttäjän selaimen välillä. **FTP** (File Transfer Protocol): kehitetty alunperin yksinomaan tiedostojen siirtoon. Voidaan siirtää tiedostoja esimerkiksi omalta tietokoneelta www-palvelimelle. **SMTP** (Simple Mail Transfer Protocol): nimensä mukaan yksinkertainen Internet-sähköpostin siirtoprotokolla. **Telnet**: käytetään etä- eli pääteyhteyksien muodostamisessa.

TCP huolehtii siitä, että datapaketit toimitetaan perille kohdeosoitteeseen ja ne ovat oikeassa järjestyksessä. Lisäksi jokainen datapaketti kuitataan vastaanotetuksi tai muussa tapauksessa paketti lähetetään uudelle. Tällä tavalla varmistetaan tiedon eheys. Muulla tavalla TCP/IP ei huolehdi tiedon tietoturvallisuudesta. Kaikki tarvittava turvallisuus tulee erikseen rakentaa TCP/IP- protokollan päälle. Loppukäyttäjä ottaa turvallisuuden huomioon esim. käyttämällä salattua yhteyttä (https://).

Internetin palvelut

Käytetyimpiä Internetin palveluja - erilaisia tapoja tietojen vaihtamiseen Internetissä - ovat sähköposti, keskusteluryhmät, WWW (World Wide Web) ja erilaiset sosiaalisen median palvelut.
Vähemmän tunnettuja Internet-palveluja ehkä ovat Telnet ja FTP (File Transfer Protocol) eikä näitä palveluita suositellakaan enää käytettäväksikään niiden turvattomuuden vuoksi.

World Wide Web

WWW on maailmanlaajuinen hypermediaverkosto, joka koostuu palvelimista ja niihin tallennetuista hypermediadokumenteista. Nämä HTML (HyperText Markup Language) -kielellä koodatut tiedostot voivat sisältää tekstiä, kuvia, ääntä, grafiikkaa ja videokuvaa. Lisäksi sivuilla voi olla eri ohjelmakoodeilla tehtyjä osuuksia. Dokumentit kytketään toisiinsa hyperlinkeillä, joiden kautta voidaan siirtyä viitattuun dokumenttiin, joka voi sijaita toisella palvelimella. Järjestelmä toimii usein myös edustapalveluna taustalla olevaan tietojärjestelmään. WWW onkin yleinen edusta erilaisille tietokannoille ja monille erilaisille palveluille.

Some, irc, chat, keskusteluryhmät, wikit, blogit,…

Internetissä on suuri joukko aihepiireittäin lajiteltuja keskusteluryhmiä, ryhmätyökaluja tai sosiaalisen median palveluita joihin Internetin käyttäjät voivat osallistua. Erilaiset palvelut voivat muodostua vapaalle keskustelulle eri aiheista, kun taas jotkin ovat suljetuille ryhmille ja käyttäjä voi itse määritellä, ketkä muut ovat mukana palvelussa. Varsinaisten keskustelukanavien lisäksi on muitakin kanavia kuten erilaiset wikit tai blogit ja muut some-palvelut joissa käyttäjät voivat jakaa ja/tai muokata omaa tai toisten tekstejä, kuvia, videoita, jne.

Eräs internetin alkuperäinen perusperiaate oli voida esiintyä anonyyminä. Nykyisin kuitenkin lähes joka palveluun on vähintään rekisteröidyttävä. Usein on luotava oma profiili tai ainakin erillinen tunnus ja samalla on kerrottava ainakin jonkin verran tietoja itsestämme. Siitä kuinka paljon suostumme kertomaan, on vastuu itsellämme. Kuinka turvassa nämä antamamme tiedot ovat? Joissakin palveluissa käyttäjän tiedot paljastuvat muille käyttäjille, jos niitä ei erikseen suojata. Suojaus voi olla loppukäyttäjän vastuulla.

Nämä asia herättävät monenlaisia kysymyksiä: Esimerkiski erilaisissa palveluissa voimme esiintyä työnantajamme edustajana tai / ja yksityishenkilönä.
Vaarana on, että nämä roolit sekoittuvat.
Toisaalta sosiaalinen media edellyttää, että esiinnymme aina omana itsenämme ja omien sanojemme takana.
Kuinka paljon meistä löytyy tietoja jotka olemme itse paljastaneet tai/ja hakukoneiden avulla?
Indentiteettivarkaudet lisääntyvät jatkuvasti. Tunnistammeko riskit?

"On the Internet, nobody knows you're a dog."

Huomioitava myös missäpäin maailmaa sijaitsee palvelin jonne tiedot talletetaan, minkä maan lakien mukaan tietojasi suojataan ja miten palvelin on ehkä suojattu (tätä emme voi tietää).

Esimerkiksi Facebook sijaitsee amerikkalaisella palvelimella. On kritisoitu että palvelunntarjoaja on muuttanut suojausasetuksia käyttäjiltä kysymättä. Lisäksi USA:n tietosuoja koskee vain USA:n kansalaisia, ei esimerkiski eurooppalaisia, joten palveluntarjoaja saa käyttää Facebookissa olevaa materiaali esim. valokuvia miten haluaa (vaikkapa myydä niitä).

Tietoturvanäkökohtia

Teknisesti Internettiin liittyvät tietoturvaongelmat ovat moninaiset, koska mm. TCP on ns. turvaton protokolla eikä sisällä itsessään minkäänlaista turvallisuutta, vaan kaikki turvallisuus on rakennettava TCP-protokollan päälle esim. salaamalla. Yleisiä salausmenetelmiä ovat SSL, ssh, VPN, PGP, jne.

Lisäksi TCP/IP:n turvallisuutta on parannettu seuraavilla protokollilla: HTTPS (salattu HTTP-protokolla, www-selaus), SSMTP (salattu SMTP-protokolla, sähköposti), NNTPS (salattu NNTP-protokolla, uutisryhmät) FTPS-protokolla (salattu FTP-protokolla, tiedostojen siirto) ja Telnets (salattu Telnet-protokolla, pääteyhteys). Toiset näistä ovat yleistyneet käyttöön enemmän kuin toiset.

Kahden solmun välinen salaus ei kuitenkaan estä esim. haittaohjelmien leviämistä. Erilaisten Internetin palvelujen kuten IRC- tai pikaviestiohjelman tms., avulla mm. madot kykenevät leviämään yhtä lailla kuin pelkän web-selaimen kautta. Haittaohjelmien kirjoittajat käyttävätkin usein juuri some-palveluja uusien haittaohjelmien levittämiseen.

Esimerkki 1:

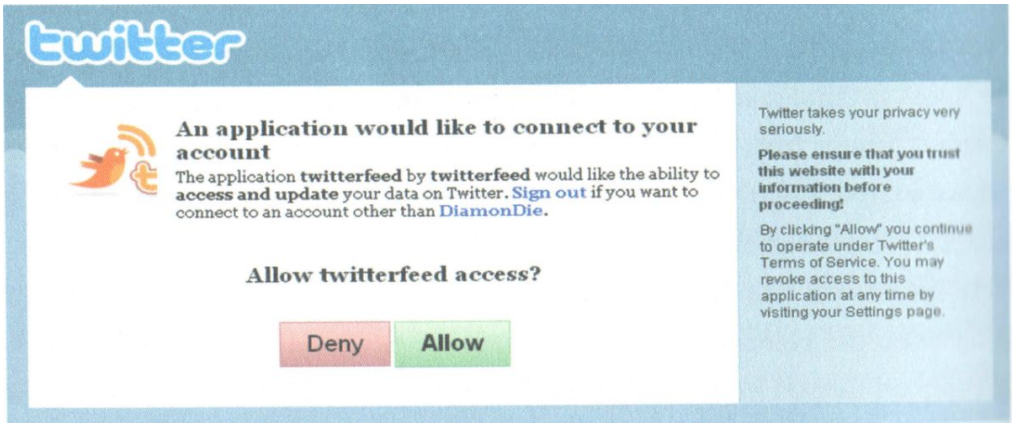
Skype (ilmainen nettipuhelin ja pikaviestipalvelu) on yleistynyt niin yksityis- kuin yrityskäytössä. Monet asiantuntijat eivät pidä Skypeä (kuten eivät muitakaan pikaviestiohjelmia) tarpeeksi turvallisena yrityskäyttöön, jossa yrityssalaisuudet puheluiden tai tietokoneella olevien tiedostojen kautta voivat joutua ulkopuolisille. Lisäksi, mitä kaikkia ominaisuuksia itse ohjelma sisältää, ei voida tietää, koska ohjelmakoodi on salainen. On mahdollista, että se kerää tietoja soittajista tai tarjoaa kuuntelumahdollisuuden kolmannelle osapuolelle.

Skype-tekniikka sisältää useita mahdollisia tietoturvaan liittyviä uhkia: liikenne kulkee esteettä palomuurin läpi, vertaisverkkopohjaisuus (jokainen Skype-kone toimii tämän virtuaalisen puhelinverkon solmuna ja välittää myös muiden puheluita silloin kun ohjelma on käynnissä), dokumentoimattomat salausmenetelmät, lokien puuttuminen sekä se etteivät virusskannerit pysty valvomaan Skypen käyttöä. Epäilyksiä on myös aiheuttanut se, että ohjelman koko on suuri ohjelman ominaisuuksiin nähden ja itse ohjelmakoodi on poikkeuksellisen huolellisesti salattu, eikä näin ollen voida tietää, mitä se pitää sisällään. Yksityiskäytössä on hyvä tietää mille riskeille koneensa altistaa.

Esimerkki 2:

Twitter (yhteisö- ja mikroblogipalvelu, jonka käyttäjät pystyvät lähettämään ja lukemaan toistensa päivityksiä Internetissä) on myös ollut mukana muutamissa ikävissä tietoturvaan liittyvissä uutisoinneissa mm. Twitter käyttäjien tunnuksia on hakkeroitu käyttämällä erään Twitter ylläpitäjän tunnusta. Suurin osa murroista kuitenkin tapahtuu käyttämällä hyväksi peruskäyttäjien huolimattomuutta.

Twitterissä on OAuth-järjestelmä jonka avulla voi kirjautua muihin palveluihin. Jos jokin tähän liittyvä palvelu väärinkäyttää tunnustasi, ei edes salasanan vaihto auta, sillä palvelulla on suora pääsy tunnukseesi. Ole siis tarkkana mihin järjestelmiin kirjaudut Twitterin OAuth-järjestelmällä.



Kuvan ruutu kertoo, että jokin palvelu haluaa käyttää tunnuksiasi. Harkitse ennen kuin painat Allow.

Huomaa että palvelun käyttöoikeudet voidaan kuitenkin poistaa asetusten Connections-välilehdeltä.

Esimerkkejä internetin palveluista ja niihin liittyvistä suojaustoimista löytyy jokapäiväisestä käytöstä. Esim. pankkipalvelut tai viranomaisasiointi, ekauppa jne.

Netiketti

Omalla käytöksellään verkkopalveluissa voi vaikuttaa tietoturvallisuuteen. Tällaisia verkon käyttäytymissääntöjä kutsutaan netiketiksi. Tämä Internet-etiketti tarkoittaa Internet-käyttäjien piirissä syntyneitä käytöstapoja, joiden mukaan käyttäjien edellytetään toimivan. Ne ovat Internet-käyttäjien eettisiä sääntöjä, eivätkä sido oikeudellisesti. Nämä säännöt perustuvat kollektiiviseen käsitykseen siitä, mikä Internet-käyttäjälle on hyväksyttyä ja mikä ei. Niiden tarkoituksena on tehdä verkon käytöstä mahdollisimman turvallista ja miellyttävää. Netiketin perusperiaatteisiin kuuluu toisten oikeuksien, yksityisyyden ja vakaumuksen sekä vapaan tiedonvälityksen kunnioittaminen.

Netiketille on tyypillistä, että Internet-etiketin noudattamista eivät valvo viranomaiset vaan muut käyttäjät. Kärjistyvimmillään netiketti on toiminut siten, että käyttäjät, jotka eivät hyväksy tietyn tahon toimintaa Internetissä, lähettävät tälle sähköpostiviestejä, joissa he ilmaisevat, että eivät hyväksy kyseisen käyttäjän menettelyä. Joissakin tapauksissa jonkun käyttäjän menettely saattaa saada liikkeelle tuhansien käyttäjien joukkoliikenteen, josta käytetään termiä flaming. Silloin tuhansien käyttäjien lähettämät viestit lamaannuttavat toiminnan kohteeksi joutuvan käyttäjän toiminnan Internetissä. Sähköpostiviestien tulva voi lamaannuttaa myös kyseisen käyttäjän Internet-operaattorin palvelimen toiminnan.

Netiketti on saanut tuhannet käyttäjät puuttumaan mm. sähköpostin välityksellä suoraan käyttäjille osoitettuihin mainoksiin ja joihinkin yhteiskunnallisiin arvostuksiin osoitettuun halveksuntaan.

Suomessa toimivat operaattorit Finnet-liitto ry, Jippii Group Oyj, Elisa Internet Oy ja Sonera Oyj ovat julkaisseet yhteisen netiketin.
Netiketti löytyy esim. osoitteesta: elisa.net/netiketti.shtml (HUOM. Netiketti kuuluu tenttialueeseen.)

WWW-tietoturva

Www-tietoturvalla tarkoitetaan koko www-ketjuun - www-palvelin, www-sivuja palveleva paikallisverkko ja www-selaimet standardeineen, protokollineen, ohjelmistoineen ja laitteistoineen - liittyviä tietoturvauhkia ja uhkien estämiseksi kehitettyjä menetelmiä. Web-tietoturva on siten laaja kysymys.

Tietoturva on tärkeä yrityksen www-palvelun ylläpitäjälle (web-master), koska avatessaan www-palvelun, avaa hän samalla koko Internet-maailmalle ikkunan yrityksen lähiverkkoon ja sitä kautta yrityksen muihin tietojärjestelmiin.

Nykyiset www-palvelimet ovat monipuolisia ja sisältävät turvallisuuteen liittyviä ominaisuuksia. Esimerkiksi intranet-verkossa www-palvelimen pitää pystyä tunnistamaan ja autentikoimaan erilaisia käyttäjiä. Käyttäjillä on erilaiset oikeudet resursseihin. Tietylle www-sivulle pääsyä voidaan rajoittaa pyytäjän IP-osoitteen mukaan tai vaatimalla käyttäjätunnus ja salasana.

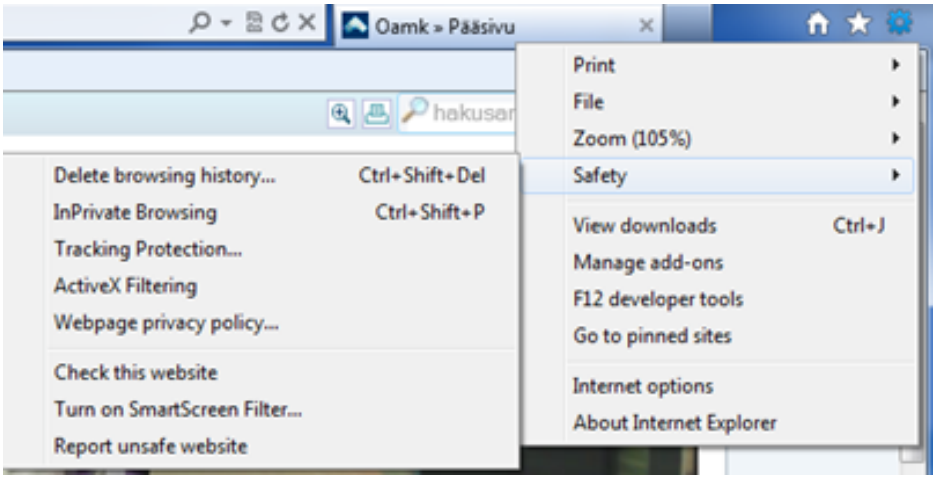
Www-palvelin voi sisältää myös palvelimessa suoritettavia ohjelmistokomponentteja, kuten **CGI-skriptejä** (Common Gateway Interface). Näiden ohjelmistojen kautta voidaan tarjota erilaisia dynaamisia tietopalveluita, (tavalliset www-sivut ovat staattisia). Käytännössä useimpia näitä ohjelmistoja käytetään lomakkeiden kautta: käyttäjä täyttää www-lomakkeen, jonka syötteen ohjelma käsittelee ja palauttaa selaimelle uuden www-sivun. Palvelimen ohjelmistolaajennusten kautta voidaan rakentaa varsin kehittyneitä sovelluskokonaisuuksia tietokantayhteyksineen. Kuitenkin www-palvelinten mukana tulevista erilaisista skripteistä on löydetty merkittäviä tietoturvaongelmia eivätkä ne ole olleet riittävän turvallisia.

Loppukäyttäjästä www-surffailu voi erheellisesti tuntua turvalliselta ja suojatulta. HTML-dokumentteihin sulautetut aktiiviset sisällöt, kuten **ActiveX-ohjelmat** ja **Java-sovelmat**, voivat tuoda haittaohjelmia käyttäjän sovelluksiin ja sitä kautta käyttäjän tietojärjestelmään. Varsinkin ActiveX-ohjelmilla on vapaa pääsy työaseman resursseihin; ne pystyvät esimerkiksi kirjoittamaan kiintolevylle. ActiveX-ohjelmien turvallisuutta onkin yritetty taata eräänlaisella elektronisella allekirjoituksella, jonka pitäisi taata esim. viruksen tapaan toimivan ohjelman ohjelmoijan joutumisen vastuuseen teostaan. Java-sovelmat ovat turvallisempia, koska ne suoritetaan käyttäjän selainohjelman sisällä ns. hiekkalaatikossa, jonka reunat estävät esimerkiksi tiedostojen kirjoittamisen työaseman kiintolevylle.

Aktiivisilla sisällöillä on merkitystä myös verkkoturvan kannalta, koska vahingolliset koodit voivat päästä web-selausten kautta palomuurin läpi käyttäjäyrityksen lähiverkkoon. Web-selailusta jää verkkoon historiatietoja, joista asiantunteva murtautuja voi käyttää hyväkseen.

Näiden tietoturvauhkien lisäksi sekä loppukäyttäjien että web-palvelun ylläpitäjän tulee pystyä vakuuttumaan siitä, että tiedot pysyvät luottamuksellisina ja autenttisina. TCP/IP-protokollia ei ole suunniteltu tietoturvamielessä, joten TCP/IP-protokollat ovat alttiita salakuuntelulle.

Viime vuosina selainten uusissa versioissa on otettu monenlaisia tekniikoita joilla parannetaan tietoturvaa: Kolmannen osapuolen evästeiden esto, PopUp ikkunoiden esto, haitallisten sivustojen tunnistaminen, InPrivate-selailu,...
ks. kuva IE-selaimen suojauksista



Web-tietoturvan riskit

Web-tietoturvan riskit voidaan jakaa kolmeen luokkaan:

- Web-palvelimen ohjelmavirheet (bugit) tai väärinkonfiguroinnit, jotka mahdollistavat etäkäyttäjän luvattomasti
    - anastaa luottamuksellisia dokumentteja
    - suorittaa palvelinkoneessa komentoja, jolla voidaan tehdä järjestelmään muutoksia
    - saada web-palvelimesta tietoja, jota voidaan käyttää järjestelmän murtamiseen
    - suorittaa palvelunestohyökkäyksiä (DoS, Denial-of-Service), jolla järjestelmä saatetaan hetkellisesti (tai pitemmäksi aikaa) käyttökelvottomaksi. Tarkoituksena on estää käyttäjiä pääsemästä www-sivustolle.

- Selainpään riskit, kuten
    - aktiiviset sisällöt, jotka kaatavat selaimen, vahingoittavat käyttäjän järjestelmää, murtavat yksilönsuojaa tai aiheuttavat muuta harmia
    - loppukäyttäjän antaman henkilökohtaisen informaation tahallinen tai tahaton väärinkäyttö

- Verkon salakuuntelulla toteutettu selaimelta palvelimelle tai päinvastoin lähetetyn datan sieppaaminen

Yksi esimerkki internetin peruspalveluista, joka alkaa olla jo jokaisen kaduntallaajan käytössä, on sähköposti. Sähköpostista seuraavaksi vähän takemmin omassa alaluvussa.

4.2 Sähköposti

Sähköposti on verkkoyhteiskuntamme peruspalvelu. Perusviesti kulkee verkossa salaamattomana ja salaamattoman sähköpostin tietoturvaa verrataan usein tavalliseen postikorttiin: kummassakin tieto on yhtä salassa. Sähköposteihin liittyvät tietoturvaongelmat liittyvätkin suojaamattomiin, salakuunneltaviin yhteyksiin ja käyttäjän puutteelliseen todentamiseen. Sähköpostin käytössä erityisen tärkeää on huomioida se, millaista tietoa sähköpostin välityksellä lähetetään! Onko tieto julkista, sisäistä, luottamuksellista vai salaista?

Vähimmäisvaatimuksena sähköpostin suojauksessa on käyttäjätunnus ja salasana. Myös yhteydenotot sähköpostipalvelimelle esim. mobiililaitteilla tulee varustaa salasanalla.

Lisäksi käyttäjän tulee ottaa huomioon muitakin seikkoja:

- Oikeustoimilain mukaan lähtökohtana on, että esimerkiksi sähköpostin lähettäjä kantaa vastuun tiedonsiirron onnistumisesta. Jos esim. sähköpostin välityksellä siirtyvän laskun eräpäivä tai jonkin tarjouksen tai hakemuksen määräaika umpeutuu, eikä lähetetty sähköpostiviesti ole mennyt perille tiedonsiirrossa tapahtuneen virheen tai katkeamien vuoksi, on vastuu lähettäjällä.

- Sähköpostisanomien automaattista edelleen lähettämistä tulee välttää. Vastaanottaja (=edelleen lähettäjä) ei voi tietää, minkä sisältöisiä viestejä hän tulee saamaan eikä lähettäjä voi tietää, että hänen viestinsä joutuvat aivan eri henkilöille. Samoin automaattista vastaustoimintoa (Out of Office AutoReplay), jota käytetään silloin kun viestin vastaanottaja on esim. lomalla, tulee välttää. Se mahdollistaa ns. sosiaalisen hakkeroinnin.

Kuva: Kevin Mitnick käyntikortti (yksi ehkä maailman tunnetuimmista entisistä hakkereista)

- Suojautuminen viruksia ja muita haittaohjelmia vastaan varovaisella toiminnalla (mm. HTML-muotoisten viestin estolla sekä virustorjuntaohjelmistolla!

Sähköpostin luottamuksellisuus

Yleensä yksityisen henkilön sähköpostilaatikkoa ylläpitää jokin yritys, joka vastaa sähköpostijärjestelmän teknisestä toimivuudesta ja toteutuksesta. Tällaisena organisaationa voi olla esimerkiksi työnantaja, oppilaitos tai yhteisö, joka tarjoaa palvelua. Kuitenkaan tällainen palveluntarjoaja ei omaa oikeuksia asemansa vuoksi puuttua yksityisen henkilön luottamukselliseen

sähköpostien viestintään. Viestintäsalaisuus on koskenut (niin sähköpostia kuin puheluja, tekstiviestejä tms.) sekä viestin sisältöä että tunnistetietoja ja mm. lokitietoja. Asian tiimoilta on viime vuosina käyty aika-ajoin keskustelua, työnantajien oikeuksia on laajennettu ja toistamiseen tiedotusvälineet ovat uutisoineet asian olevan esillä.

Milloin viestiliikennettä sitten valvotaan? Sähköpostipalvelua tarjoavan organisaation henkilöstössä on henkilöitä, jotka ylläpitävät tätä palvelua organisaation määräämin säännöin ja joutuvat tässä tehtävässään tarkkailemaan viestintää. Viestien välittämisen tarkkailuun voi olla syynä palvelussa ilmenevät tekniset ongelmat. Sähköpostiviesti voi ohjautua väärälle vastaanottajalle, tällaisessa tapauksessa organisaatiossa valvontatehtävissä oleva henkilö voi joutua selvittämään sähköpostiviestissä olevia tunnistamistietoja viestin ohjaamiseksi oikeaan osoitteeseen. Tai esimerkiksi oppilaitoksissa saatetaan valvoa sitä, että oppilaitoksen tarjoamaa sähköpostiosoitetta ei käytettäisi kaupallisiin tarkoituksiin. Samanlainen tilanne voisi syntyä työpaikoilla työnantajan ja työntekijän välisessä suhteessa. Yleensä työsopimukseen määritellään työntekijän oikeudet ja velvollisuudet, myös työnantajalla on sille kuuluvat velvollisuudet. Työnantajaa voi kiinnostaa, käyttääkö työntekijä omaa sähköpostiaan kaupallisiin tarkoituksiin tai luovuttaako työntekijä ulkopuolisille sellaisia tietoja, jotka voisivat vahingoittaa työnantajaa.

Yleensäkin yritysten ja yhteisöjen ongelmana on työntekijöiden yksityisten viestien kuormittaminen yrityksen tai yhteisön tietojärjestelmälle. Tähän kaikkeen liittyy olennaisesti myös tietoturvallisuuden valvonta. Tästä johtuen on yritysten ja yhteisöjen halu kontrolloida tietoverkoissaan tapahtuvaa sähköpostiviestintää pidetään hyvin ymmärrettävänä. Yritykset voivat olla huolissaan toimintaansa liittyvien salaisten tietojen vuotamisesta ulkopuolisille tahoille teollisuusvakoilun muodossa.

Laki luottamukselliseen viestiin puuttumisesta

Lain yksityisyyden suojasta työelämässä (2004) mukaan työnantajalla on oikeus puuttua työntekijän luottamukselliseen viestintään. Puuttuminen perustuu sopimukseen, jossa määritellään puuttumisperusteet.

Työelämän tietosuojalain mukaan työnantajan on käytävä yt-menettelyssä läpi organisaation sähköpostikäytäntö. Sopimus tehdään työnantajan ja työntekijän välillä ja siinä olisi pyrittävä löytämään ne tilanteet, joissa työnantajalla olisi oikeus puuttua työntekijän sähköpostiviestintään. Nämä sopimukset ovat kuitenkin luonteeltaan hyvin hankalia. Sopimustilanteessa tulee miettiä sitä, ovatko sopijaosapuolet tasavertaisessa asemassa. Joutuuko työntekijä pakon edessä suostumaan sellaiseen, mikä on hänen etujensa ja oikeuksiensa vastaista. Työntekijä voi työpaikan menettämisen pelossa sitoutua sopimukseen, jossa työnantaja voi asemansa vuoksi yksipuolisesti määritellä sopimuksen ehdot.

Mikäli työnantaja ja työntekijä tekevät sopimuksen sähköpostin käytöstä, tulee työnantajan määritellä, mitä nimenomaan tarkoitetaan luottamukselliseen viestintään puuttumisella. Voitaisiin esimerkiksi määritellä, saako työntekijä käyttää sähköpostiosoitettaan yksityiseen viestintään vai pelkästään työtehtävien hoitoon. Sähköpostin käyttäjälle tulee kertoa, miksi viestin salaisuuteen on tarve puuttua. Erityisesti ne tilanteet, joissa puututaan viestien sisältöön, on rajattava hyvin. Lain mukaan hyvin poikkeuksellisen tärkeän tiedon saaminen työntekijän sähköpostista, esimerkiksi työntekijän loman tai sairasloman aikana, yrityksen käyttöön voi olla tällainen erityisperuste, jos tietoa ei mitenkään muuten voi saada, työntekijälle on yritetty ilmoittaa asiasta eikä lupaa ole saatu kohtuuajassa. Huomattavaa on että tapauksessa jossa työntekijä on kieltänyt viestiensä aukaisun, eikä työnantaja saa tiettyjen ehtojen täyttyessä työntekijää kiinni, voi työnantaja silti aukaista viestin.

Lain mukaan viestejä voi etsiä järjestelmän pääkäyttäjä viestin otsikkotietojen perusteella. Viestiä avattaessa paikalla on työnantajan lisäksi oltava yksi todistaja. Heitä molempia sitoo salassapitovelvoite. Lisäksi työnantajalla on ns. huolehtimisvelvoite, jonka mukaan työntekijälle on tarjottava erilaisia mahdollisuuksia ohjata posti toiselle henkilölle. Lain mukaan sähköpostiviestejä saa hakea ainoastaan neuvottelujen loppuun saattamiseksi, asiakkaan palvelemiseksi ja työnantajan toimintojen turvaamiseksi. Lisäksi työntekijän tehtävien tai hänen vastuullaan olleiden asioiden perusteella on oltava ilmeistä, että hänellä voi ylipäätään olla työnantajalle kuuluvia viestejä. Henkilökohtaisiksi merkittyjä viestejä ei ole työnantajalla oikeus lukea.

Sähköpostin uhkat

Perinteisesti sähköpostiviestit ovat Suomessa siis saaneet kirjesalaisuuden kaltaista suojaa eikä niihin ole voitu puuttua muuten kun ylläpitohenkilöiden normaalin verkontarkkailun yhteydessä liittyvänä lähinnä otsikko- / lähettäjätietojen tarkkailuna.

Varsinaiset sähköpostin uhat voivat olla sisäisiä (esim. joku varastaa käyttäjätunnuksesi ja salasanasi näppäimistön alta) tai ulkoa verkkoa krakkeroivien hyökkääjien tekemiä. Sähköpostiin voidaan hyökätä joko palvelimelle tai tiedonsiirron yhteydessä.

Flaming

Tietoverkko on kaksisuuntainen media. Tästä johtuen verkon käyttäjiltä vaaditaan ja odotetaan yleisesti hyväksyttyjen käyttäytymissääntöjen noudattamista. Yritys tai käyttäjä voi joutua massapostituksen kohteeksi myös oman toimintansa seurauksena. Käyttäjä voi kotisivullaan tai esimerkiksi sosiaalisessa mediassa ilmaista itseään Internet-etiketin eli ns. netiketin vastaisesti. Tämä voi ärsyttää muita Internetin käyttäjiä ja he voivat lähettää viestejä netiketin vastaisesti toimivalle henkilölle. Tästä joukkoliikkeestä käytetään englanninkielistä termiä flaming, eikä sitä oikeudellisesti ole pidetty rikollisena tai edes vahingontekona.

Spam

Roskapostia eli spammia väitetään olevan kaikesta verkkoliikenteestä noin 95 % ja pahimpien ennusteiden mukaan Internetin on uskottu kaatuvan ylikuormitetun verkkoliikenteen vuoksi. DNS-pohjaisten mustien listojen avulla saadaan kuitenkin suodatettua suurin osa (noin 99,8 %) sähköposteista ennen niiden pääsyä käyttäjän postilaatikkoon.

Suodatus voidaan asentaa erillisen ohjelman avulla suoraan sähköpostipalvelimelle. Esimerkiksi sähköpostipalvelimelle tehdään sääntö, jossa kaikki tietyt sanat (ohjelma tutkii viestin otsikosta ja sisällöstä useita sanoja, joilla omat ns. painoarvot) omaaviin sanomiin lisätään tietty merkkijono sanoman otsikko-osaan. Merkkijonon sisältävät sähköpostit siirretään suoraan roskaposti-kansioon. Sähköposti on mahdollista suodattaa myös käyttäjän client-ohjelmassa (ks. asiakas- / palvelin-järjestelmä), mutta yrityskäytössä parempi on suodattaa postit jo palvelimella. Spammin suodatus on erittäin haasteellista, koska spammiviestin tekstit on voitu esim. upottaa kuviin.

Mikäli roskapostit pääsevät suodatuksen läpi, ovat ne yleensä vain kiusallista käyttäjien kuormittavaa mainontaa ja ne tulee tuhota aina heti. Mukana kulkevassa liitetiedostossa voi olla haittaohjelma tai viestit voivat olla erilaisia huijauksia (mm. Nigerialaishuijaukset, phishing). Roskapostittajien pyyntöön vastata viestiin ei koskaan (ei silloinkaan kun siinä tarjotaan mahdollisuutta päästä pois ko. postituslistalta) kannata vastata. Vastausta ei todennäköisesti huomioida mitenkään tai parhaimmillaan sen avulla vain kerrotaan roskapostittajalle, että sähköpostiosoitteesi on aktiivisesti käytössä. Näin

saat lisää roskapostia.

Spammiksi luetaan myös erilaiset kiertokirjeet. Niidenkin edelleen lähettämiseen tulisi suhtautua varauksella. Esimerkiksi jos laitat nimesi kiertokirjeen nimenkeräyslistaan, kuinka voit varmistua kuka postin alkuperäinen lähettäjä oli, mikä todellinen tarkoitus listan kierrätyksellä on ja mihin käyttöön se lopulta päätyy? Kaikki verkkoon itsestäsi laittama tieto pysyy siellä "ikuisesti".

Toiseksi roskamainosten tavoin kiertokirjeet täyttävät suunnattomasti levytilaa. Ne ovat aina luonteeltaan pyramidiskeemoja:

Päiviä kulunut	Viestin on lukenut yhteensä
0	1
1	6
2	31
3	156
4	781
5	3.906
6	19.531
7	97.656
8	488.281
9	2.441.406
10	12.207.031
11	61.035.156
12	305.175.781
13	1.525.878.906
14	7.629.394.531

Jos jokainen vastaanottaja lähettää viestin seuraavana päivänä viidelle henkilölle, niin noin kahdessa viikossa viestin on lukenut koko maailman väestö. Käytännössä samat ihmiset saavat ketjukirjeen luettavakseen useampia kertoja. Erilaisia ketjukirjeitä liikkuu kuitenkin useita. Emme varmaan voi edes kuvitella verkossa liikkuvien viestien määrää, silloin kun useammat kiertokirjeet (tärkeytensä) vuoksi saavat laajan levikin.

Spammista ei varmaan koskaan päästä kokonaan eroon. Vaikka Suomessa mainospostinlähetys, ilman kuluttajan etukäteistä suostumusta on kielletty, suurin osa roskaposteista tulee USA:sta, jossa eri osavaltiossa mainosposteihin suhtaudutaan eri tavoin. USA:n lakien mukaan vastaanottajan on ilmoitettava ettei halua "roskaposti"mainoksia. Käytännössä roskapostituskielto on tehoton, koska vastuu on siirretty vastaanottajalle. Osa USA:sta tulevista roskaposteista on siis USA:n lakien mukaan täysin sallittuja, eivätkä ne näin ollen varmaankaan tule ainakaan vähentymään. Niitä vastaan voidaan kuitenkin yrittää suojautua esimerkiksi suodattamalla tulevaa postiliikennettä.

Suomessa tilaamatta lähetetty sähköpostimainos saatetaan katsoa erityistapauksissa jopa Rikoslain 38 luvussa tarkoitetuksi tietoliikenteen häirinnäksi. Vaikka säännös ei estä sähköpostien automaattista lähettämistä yrityksille, on yrityksilläkin mahdollisuus kieltäytyä viestien vastaanotosta.

DNS-kaappaus

Yksi esimerkiksi sähköpostiin kohdistuvasta hyökkäysmenetelmästä on **DNS-kaappaus**. Sähköpostit löytävät perille nimipalvelun avulla. Jos krakkeri onnistuisi siirtämään nimipalvelun osoittamaan omaan postipalvelimeensa, hän saisi kaiken yritykselle X osoitetun postin tulemaan omaan koneeseensa. Lukemisen jälkeen krakkeri voisi edelleen lähettää postin pelkän IP-osoitteen varassa yritykseen X, eikä tämä edes huomaisi minkään olevan vialla. DNS -kaappausten ehkäisemiseksi operaattorien ja

Viestintäviraston, joka vastaa fi-loppuisten verkkotunnusten hallinnoinnista, pitää varmistaa kaikkien domain -nimien siirtoon liittyvät pyynnöt huolellisesti ja todentaa, että pyynnön lähettäjä on siihen oikeutettu henkilö.

Palvelunestohyökkäys

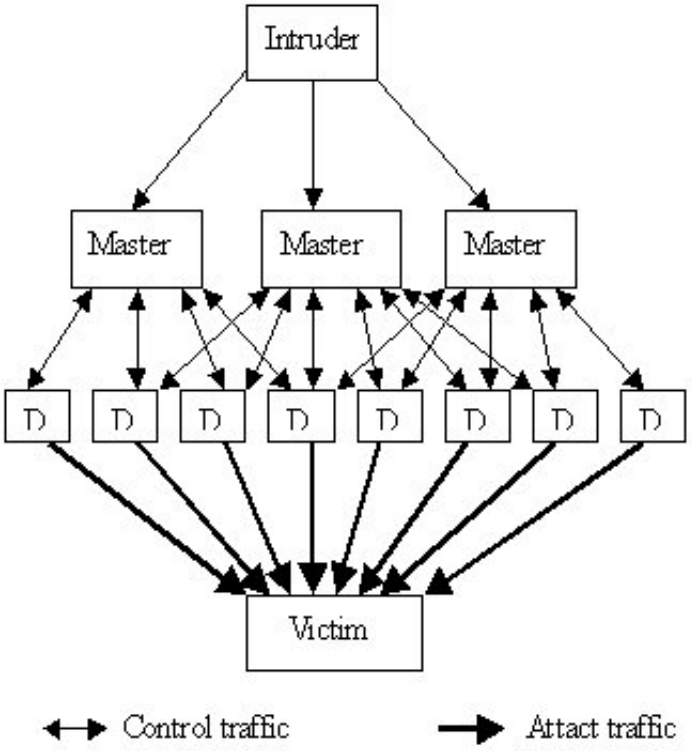
Sähköpostipalvelimeen kohdistuvat massapostitukset aiheuttavat vahinkoa yrityksen sähköpostiliikenteelle. Saapuvien sähköpostien suuri määrä pysäyttää koko sähköpostiliikenteen, koska sähköpostipalvelin ei kykene välittämään tulleita viestejä. Palvelimen on otettava kaikki viestit vastaan ja yritettävä välittää ne oikeisiin osoitteisiin. Koska viestejä voi tulla yhtä aikaa todella paljon, ei tehokaskaan palvelin pysty hoitamaan viestin välitystä. Tämä voi aiheuttaa sähköpostipalvelun kokonaisvaltainen hidastumisen tai kaatumisen.

Edellä kuvatun kaltaista sähköpostihyökkäystä eli **palvelunestohyökkäystä (ns. DoS-iskua)** on hyvin vaikea torjua ennakolta, koska postipalvelin ei voi tietää, milloin viestien tarkoituksena on pysäyttää yrityksen koko sähköpostiliikenne, milloin taas on kyse normaalista sähköpostiliikenteestä. Jos esim. osoitteet on generoitu erilaisiksi, niiden automaattinen erottaminen oikeasta postista on vaikeaa.

Massahyökkäyksiin on kehitetty tehokkaita tapoja (verkkohyökkäystyökaluja), jotka käyttävät ns. hajautettua järjestelmää jota kutsutaan **hajautetuksi palvelunestohyökkäykseksi (DDoS)**. Verkkohyökkäystyökaluilla voi saada aikaan vakavia tuhoja. Työkalut kuten snifferit, scannerit ja massahyökkäystyökalut on ohjelmoitu valmiiksi, käyttäjäystävälliseksi ja ne laitetaan vapaasti kenen tahansa saataville Internetiin.Näitä työkaluja käytetään hajautettuihin sähköpostihyökkäyksiin, jolloin hyökkääjä voi helposti lähettää kymmeniä tuhansia yhtäaikaisia viestejä yhteen tai muutamaan suojaamattomaan Internet solmuun.

Hyökkääjä käyttää hyväkseen Internet-verkossa olevia suojaamattomia palvelimia tai pahaa-aavistamattomia suojaamattomia kotikoneita, asentaa niihin ns. daemon -prosesseja, joiden avulla hajautettu hyökkäys tapahtuu. Sekä nämä järjestelmät että varsinaiset hyökkäyksen kohteeksi joutuneet solmut ovat uhreja.

Hajautettu hyökkäysjärjestelmä pohjautuu yleiseen asiakas-/palvelin-malliin, josta tyypillinen esimerkki (ks. kuva) on, että hyökkääjä kontrolloi joitakin isäntäpalvelimia (master) käynnistettävien prosessien (daemons) kautta. Näitä prosesseja voidaan käyttää laukaisemaan viestitulva kohti uhria.



Hyökkäyksen kohteeksi joutuneelle seurauksista toipuminen voi kestää kauan. Tuhojen korjaamiseen voi mennä useita päiviä ja vaikka lähettävältä palvelimelta tuhottaisiin kyseiset daemon-prosessit, voi järjestelmään olla uusia prosesseja odottamassa ajastettuna käynnistymistä.

Tämä kaikki on laajalti automatisoitu niin, että hyökkääjän omat prosessit (scannerit ja snifferit) saavat selville Internet verkon palvelimien ja suojaamattomien kotikoneiden haavoittuvuuksia, saastuttavat (takaovet, rootkit, yms.) ja keräävät näistä listoja, vaarantavat nämä saastuttamansa koneet asentamalla ns. daemon-prosesseja ja lopulta kätkevät hyökkäyksen jäljet. Myöhemmin hyökkääjä voi helposti yhdellä näppäimen painalluksella käynnistää nämä prosessit, jotka lähettävät valtavan määrän viestejä kohti lopullista uhria.

Palomuuri voi tunnistaa palvelunestohyökkäyksen (DoS) siitä, että kaikki postilähetykset tai sivunhakupyynnöt tulevat samasta osoitteesta ja sulkea osoitteen tilapäisesti pois käytöstä. Mutta jos kyse on hajautetusta palvelunestohyökkäyksestä (DDos), häiriöliikenteen tunnistaminen on jo paljon vaikeampaa, koska palvelua pommitetaan yhtä aikaa useista eri osoitteista.

Massapostituksiin ja hyökkäyksiin, joita on erittäin vaikea jäljittää tai joita vastaan on erittäin vaikea suojautua, tulisi kuitenkin yrittää varautua etukäteen mm. suojaamalla, tarkkailemalla ja valmistautumalla siihen, että yrityksessä osataan toimia oikein hyökkäyksen sattuessa. Yrityksen tulisi etukäteen huolehtia paremmin teknisistä ratkaisuista ja vastuuhenkilöiden kouluttamisesta. Sen tulisi luoda ympärilleen yhteistyöverkosto, jossa tietoa voidaan jakaa yhteistyökumppaneiden kanssa. Lisäksi yrityksen tulisi suojautua hyökkääjien nopeasti kehittyviä työkaluja vastaan pysymällä ajan tasalla uuden teknologia välineissä. Ennen kaikkea jos yritys joutuu hyökkäyksen kohteeksi, tulisi yrityksessä olla henkilöitä, jotka ymmärtävät asian laajuuden ja osaavat toimia oikealla tavalla.

Kotikoneita hyväksikäytetään kaappaamalla ne osaksi ns. **bot- tai orjaverkkoa** haittaohjelmien avulla.

1. Tavallisen loppukäyttäjän tietokone kaapataan viruksen tai muun haittaohjelman avulla. Koneen hidastuminen, modeemin omia aikojaan vilkkuvat valot tai erikoiset virheilmoitukset voivat olla merkki siitä, että tietokone on kaapattu. Hyvin usein asia kuitenkin jää koneen käyttäjältä

huomaamatta.

2. Kun saastuneita koneita on tarpeeksi paljon, muodostuu ns. bottiverkko (orjakoneverkko), jota voidaan käyttää esimerkiksi roskapostin lähetykseen tai palvelunestohyökkäyksiin.
3. Bottiverkon luonut voi myydä verkon eteenpäin esim. roskapostittajille.
4. Bottiverkkoa hallitseva roskapostittaja pakottaa orjakoneet lähettämään roskapostia muille internetin käyttäjille.

Key escrow

Poikkeustapaus puuttua luottamukselliseen viestintään on ns. key escrow, jossa viranomainen (poliisi) voi määrätyissä tilanteissa saada haltuunsa salatun viestin purkuavaimet päästäkseen käsiksi salatun viestin sisältöön. Yleensä tämä tapahtuu erillisenä oikeuden päätöksenä. Key escrow -konseptin avulla voidaan auttaa lain toimeenpanoa käytännössä samalla periaatteella kuin telekuuntelussakin. Poliisi voi siten epäillessään terrorismia, huumausainekauppaa, rahanpesua tai muita vakavia rikoksia kuunnella määrättyjä teleyhteyksiä. Salattujen viestien avaaminen käsitetään tässä yhteydessä telekuunteluksi. Key escrow -toiminto ei ole yksiselitteisesti hyväksyttävä, koska on vaikea erottaa yleistä etua esimerkiksi kansallista turvallisuutta.

Yhdysvalloissa ja Englannissa työnantaja saa valvoa työntekijän puhelinta, nettiä ja sähköpostia lähes mielensä mukaan, koska maksaa niiden käytöstä aiheutuvat kustannukset. Pohjoismaissa työntekijän asema on vahva eikä työnantajalla ole tällaista oikeutta. Asian ympärillä käydään kuitenkin jatkuvasti keskustelua.

Viestin salaus

Sähköpostisanomien tiedonsiirto tapahtuu yleisissä tietoverkoissa pääsääntöisesti selväkielisenä. Tärkeät (käyttäjän mietittävä mikä on tärkeää) sähköpostit tulisi salata, koska niiden turvallisuudesta tai viestintäsalaisuuden säilymisestä ei voida olla täysin varmoja. Salauksen avulla estetään ulkopuolisia lukemasta viestejä ja sen avulla voidaan myös torjua mahdolliset sähköpostien salakuunteluyritykset. Esim. Internet-sähköpostin siirtoprotokolla **SMTP** (Simple Mail Transport Protocol) ja sanomarakenne eivät sisällä minkäänlaista tietoturvaa, joten Internetin perussähköpostissa on varsin helppoa muuttaa sanomien sisältöä tai väärentää lähettäjän osoitetietoja.

Viestien turvallisuuden parantamiseksi yritykset ovatkin ottaneet käyttöön erilaisia salaustekniikoita. Toimittaessa julkisessa televerkossa verkon viestiliikenne voidaan suojata ainoastaan kyllin tehokkaalla salauksella. Koska koko verkkoa on mahdoton suojata, on suojattava viestiliikenne. Salaustekniikoita on monenlaisia ja ne todettu teknisesti käyttökelpoisiksi.

Arkaluonteisten tai luottamuksellisten tietojen lähettämistä sähköpostin välityksellä tulee aina välttää ja jos sähköpostijärjestelmästä puuttuu mahdollisuus salata viesti, tulee sanoma lähettää muulla tavoin. Salaisiksi luokiteltuja tietoja ei saa lähettää ollenkaan, ei edes salattuna.

Salauksen (kryptografian) avulla on löydettävissä työkaluja myös viestin eheyden ja alkuperän varmistamiseen: Viestin autenttisuuden toteaminen tulee tärkeäksi eli se, onko lähetetty viesti tullut väitetyltä henkilöltä vai onko joku mahdollisesti päässyt muuttamaan viestin tunnistetietoja viestien liikkuessa verkossa.

Yrityksen kannalta salausohjelmien hankinta on aina kustannuskysymys. Vaikka erilaisia salausmenetelmiä on vapaasti saatavissa Internetistä, ei yritys voi rakentaa omaa suojauspolitiikkaa

näiden ilmaistuotteiden varaan. Luotettavien menetelmien käyttö on yritykselle imagokysymys ja tietoturva osa organisaation laatua.

Salaustuotteiden käyttö koetaan hyvin tärkeäksi tietoturvan alueeksi myös kansainvälisesti.

Salausohjelmistoja

PGP (Pretty Good Privacy) on eräs yleinen salausohjelmisto sähköpostiviestien salaukseen. PGP perustuu epäsymmetriseen salaukseen (salainen ja julkinen avain sekä digitaalinen allekirjoitus) jossa avainten aitous varmistetaan ns. luottamusverkon avulla. PGP:stä on versiot mm. PC-, UNIX- ja Mac-ympäristöihin. PGP:stä on uusi standardi **OpenPGP**.

PGP:n kilpailija **Secure MIME (S/MIME)** on toiminnaltaan hyvin samankaltainen kuin PGP. S/MIME käyttää X.509 mallisia varmenteita ja luottamusmallia (CA).

GPG4Win on ilmainen sähköpostinsalausohjelma.

”Karvalakkimalli”

Jos käytettävissäsi ei ole varsinaista salausohjelmaa, voit lisätä viestin luottamuksellisuutta esim. kirjoittamalla viestin erilliseksi tekstitiedostoksi ja pakkaamalla sen Winzip-ohjelmalla salasanalla suojattuna. Tiedosto voidaan kirjoittaa myös esim. Word:llä ja suojata se tallennuksen yhteydessä salasanalla.

Nämä eivät kuitenkaan ole turvallisia tapoja lähettää luottamuksellisia tietoja sisältäviä viestejä. Esim. Internetistä on saatavilla ohjelmia joilla voidaan Word-salasanalla suojattu tiedosto avata ja muuttaa tietoja, sulkea uudelleen samalla salasanalla ilman, että kukaan huomaa, että asiakirjaa on muutettu.

Huomatkaa käsitteiden salaus ja suojaus ero!

4.3 Haittaohjelmat

Haittaohjelmilla tarkoitetaan kaikkia niitä ohjelmia tai merkkijonoja, jotka aiheuttavat tietojärjestelmissä ei toivottuja ilmiöitä. Puhekielessä käytämme usein yleisnimitystä virus, silloin kun puhumme haittaohjelmista. Tämä virus -käsite sisältää kuitenkin laajan joukon erilaisia haittaohjelmia, jotka toimivat monin eri tavoin.

'Virus' ei välttämättä ole jonkun ilkeän ohjelmoijan luomus, vaan se voi aivan yhtä hyvin olla virheellinen ohjelma, joka käyttäytyy tavalla, jolla sen alkujaan ei ollut tarkoitus käyttäytyä. Kaikkia haittaohjelmia, jotka on ohjelmoitu tarkoituksella tuottamaan vahinkoa käyttäjille, kutsutaan **Malware** -ohjelmiksi.

Haittaohjelmien hyvin tunnettu leviämismekanismi on jo pitkään ollut sähköpostin liitetiedostot (vrt. tehokas sähköpostisuodatus). Tällä hetkellä yleinen leviämistapa on suoraan web-selailun tai esim. sosiaalisen median, vertaisverkon tai pikaviestipalveluiden yhteydessä. Haittaohjelmat leviävät myös CD-ROMn tai muistitikkujen avulla.

Tietokoneviruksien ominaisuuksiin kuuluu, että ne tarvitsevat isännän, siis tietokoneen tai ohjelman, jossa ne voivat levitä. Lisäksi viruksen pitää voida replikoitua eli luoda kopioita itsestään ja aktivoituakseen niiden pitää saada jokin signaali itsensä ulkopuolelta. Virukset leviävät piraattikopioitujen tietokonepelien, Internetistä imuroitujen pakattujen tiedostojen, muititikun tai esim. sähköpostin mukana. Viruksen kantoalustana voi olla jokin muukin kuin ohjelma, esim. tekstinkäsittelyn ohjelmalla tehty tiedosto, kuva tai video.

Perinteinen neljän päätyyppin luokittelu viruksille:

1) Järjestelmävirus (käynnistyssektorivirus) kopioidaan levykkeeltä tai CD-ROM:lta kiintolevyn niihin sektoreihin, joissa järjestelmätiedostot ovat. Kun käynnistyssektorivirus tartuttaa tietokoneen, se siirtää tai poistaa järjestelmän tietoja, minkä jälkeen tiedot korvataan viruksen omalla informaatiolla. Tämä aiheuttaa sen, että ne ladataan usein ennen itse käyttöjärjestelmää ja näin ne pystyvät ohjaamaan useimpia tapahtuvia asioita.
2) Tiedostovirukset ovat ohjelmiin upotettuja viruksia. Kun ohjelma ajetaan, suoritetaan viruksen oma ohjelmakoodi. Osa tiedostoviruksista yrittää tartuttaa kaikki suoritettavat tiedostot, kun osa suuntautuu vain järjestelmätiedostoihin.
3) Polymorfinen virus on salakirjoitettu niin, että virus muuttuu joka kerta, kun se tartuttaa jotakin. Osa viruksista muuttaa jopa itse salakirjoitusalgoritmia, mikä saattaa aiheuttaa joidenkin virusten kohdalla useita miljoonia ulkoasultaan erilaisia muotoja. Näiden virusten havaitseminen on vaikeinta, koska etsittävänä on useita erilaisia allekirjoituksia eli jälkiä, joita virukset jättävät levylle.
4) Makrovirus on virustyyppi, jota aiemmin oli valtaosa kaikkien havaittujen virusten kokonaismäärästä. Ne ovat riippuvaisia skriptikielistä, joita on sisäänrakennettuina monissa ohjelmissa, muun muassa Microsoft Office -paketissa. Nykyisin MS-Officen paketin ohjelmissa on oletuksen estetty makrojen automaattinen ajo.

Virukset kehittyvät koko ajan eivätkä nykyiset haittaohjelmat ole useinkaan puhtaina virustyyppeinä, mutta nykyisin niissä saattaa olla ominaisuuksia useista eri tyypeistä yhdisteltynä.

Mato muistuttaa virusta, mutta eroaa siitä siten, että se ei vaadi ohjelman muodossa olevaa isäntää. Madot leviävät tyypillisesti automaattisesti suoraan koneelta toiselle. Esim. **sähköpostimato** ilman sähköpostien liitetiedostojen avaamista. **Verkkomadot** leviävät ilman sähköpostin käyttöäkin, esim.

Sasser ja Blaster, jotka etsivät verkkoon kytkettyjä koneita, joihin ei ole asennettu viimeisimpiä korjauspäivityksiä.

Bot tulee sanasta robot, joka kuvastaa hyvin tämän haittaohjelman leviämistapaa. Se on muistuttaa leviämistavaltaan verkkomatoa. Botissa voi olla mukana myös monia muita ominaisuuksia, kuten takaportteja ja vakoiluohjelmia. Botit ovat haittaohjelmia, joiden avulla tietokonetta voidaan hallita käyttäjän huomaamatta verkon välityksellä. Botilla varustettua konetta voidaan tyypillisesti käyttää laittomiin tiedosto- tai verkkopalveluihin ja roskapostin välitykseen. Automaattisesti leviävät botit muodostavat ns. botverkkoja, joita voidaan ohjata tekemään edellä mainitun kaltaisia toimenpiteitä. Erilaisia boteja on olemassa kymmeniätuhansia ja yhdessä botissa voi olla satojatuhansia koneita. (Boteista lisää luvussa Sähköposti.)

Tartunnan saanutta tietokoneohjelmaa sanotaan **Troijan hevoseksi**. Troijan hevonen haittaohjelma, joka näennäisesti suorittaa jotakin hyödyllistä tai välttämätöntä, mutta joka samanaikaisesti suorittaa haittakoodin. Troijalainen yrittää tartuttaa muita ohjelmatiedostoja tehdäkseen myös niistä Troijan hevosia. Se voi etsiä käyttäjän koneelta tiedostoja ja lähettää niitä verkon toisessa päässä odottavalle krakkerille tai se voi avata tietokoneessa olevan mikrofonin ja välittää mikron lähellä käydyn keskustelun verkon yli salakuuntelijan korviin (takaportti).

Takaportiksi kutsutaan ohjelmaa, joka avaa ulkoisen tietoliikenneyhteyden suojaamattomaan tietokoneeseen. Takaportin kautta voidaan mm. varastaa käyttäjän henkilökohtaisia tietoja koneesta.

Spywaret eli vakoiluohjelmat ovat viruksen tapaisia ohjelmia, jotka vaativat tavallisimmin käyttäjä apua asentuakseen. Vakoiluohjelmia latautuu ja asentuu esim. epämääräisiltä web-palvelimilta. Automaattinen asentuminen käyttää hyväkseen selaimen haavoittuvuuksia. Vakoiluohjelma voi avata pääsyn tietokoneeseen verkon kautta asentamalla koneeseen takaportin (kerää erilaista tietoa käyttäjästä ja lähettää sitä eteenpäin esim. näppäimistön kuuntelu, näytön kaappaus, luottokortti tai pankkitietojen varastaminen). Vakoiluohjelmat saattavat lisäksi aiheuttaa ongelmia muiden ohjelmien toiminnalle.

Rootkit on ohjelma, joka osaa piilottaa oman toimintansa täysin näkymättömiin niin käyttäjältä kuin tavalliselta virustentorjuntaohjelmalta. Rootkittejä on käytetty myös bot-ohjelmien piilottamiseen virustentorjuntaohjelmilta. On myös tapauksia, jossa rootkit-ohjelmaa on käytetty sinänsä ihan laillisen kopiosuojauksen toteuttamiseen cd-levyllä.

Mainosohjelmat luokitellaan joissain tapauksissa haittaohjelmiksi, joskin ne ovat monesti osana ns. ilmaisjakeluohjelmia. Mainosohjelman tavoitteena on saada käyttäjä menemään halutulle internet-sivustolle.

Haittaohjelmat aiheuttavat monenlaisia harmeja tietokoneen käytölle. Koneen levytila täyttyy, käyttö saattaa hidastua sekä verkkosurffailu ja sähköpostin käyttö voivat hankaloitua merkittävästi. Ohjelmistojen toiminnassa saattaa esiintyä häiriöitä ja kone saattaa käynnistyä itsestään ilman käyttäjän toimenpiteitä. Muita ongelmia ovat tietojen häviäminen tai muuttuminen, selaimen kotisivun muuttuminen sekä muut käyttöhäiriöt. Hankalimmissa tapauksissa operaattori saattaa sulkea liittymän, jos tietokone käyttäjän tietämättä lähettää häiriöliikennettä verkkoon tai toimii roskapostin välitystoimistona. Vaikka kaikki haittaohjelmat eivät ole kovin vahingollisia, niin todella vaarallisiakin löytyy (*esim. Duqu- ja Stuxnet-mato, ks. Wikipedia).*

Vuonna 2004 löydettiin ensimmäiset **matkapuhelin haittaohjelmat**: Cabir-virus levisi kalleimmissa puhelinmalleissa käyttäen hyväkseen puhelimen bluetooth-yhteyttä. Älypuhelinten myötä ja erilaisten

palveluiden käytön levitessä kännyköissä haittaohjelmien leviäminen ja leviämismuodot lisääntyvät.

Puhelimien haittaohjelmat voivat ohjata puhelimen soittamaan kalliisiin numeroihin tai lähettämään viestejä kalliisiin kohteisiin. Jotkin haittaohjelmat viestittelevät itsestään yhteystiedoissasi oleville ihmisille ja näin pyrkivät leviämään. Ne voivat poistaa tärkeitä tietoja tai tehdä koko puhelimen käyttökelvottomaksi tai estävät uhrin puhelinta toimimasta ellei uhri maksa ns. lunnaita rikollisille. Mitä ilmeisimmin laajempi leviäminen alkaa sitten kun haittaohjelmien tekijät keksivät kuinka voivat laajemmin ansaita rahaa näiden haittaohjelmien avulla.

Melkein kaikki haittaohjelmat on suunnattu Microsoft Windows-ympäristöihin, Linuxiin ja Maciin niitä on merkittävästi vähemmän. Applen suosion kasvu tulee varmaankin lisäämään haittaohjelmia myös ko. laitteisiin. Suomessa on kaikkiaan tehty muutamia satoja haittaohjelmia (virusohjelmat), joista suurin osa on levinnyt maailmalle. Käytännössä kaikki Suomessa nähdyt tapaukset aiheutuvat ulkomailla tehdyistä haittaohjelmia.

Haittaohjelmien valtakaudet

- Käynnistyslohkovirukset 1986-1995
- Makrovirukset 1995-1999
- Sähköpostimadot 1999-2003 ->
- Verkkomadot 2003 - >
- Yhdistelmävirukset ->

Tällä hetkellä troijalaiset ovat yleisimpiä. Käyttäjien varomattomuus ohjelmien käytössä ja tietämättömyys haittaohjelmien leviämistavoista ovat osasyynä virusten maailmanlaajuiseen leviämiseen. Myös haittaohjelmien huomaaminen on paljon vaikeampaa kuin aikaisemmin. Tämän hetkisen maailmantilanteen ja top-10 listan voit tarkistaa esim. osoitteesta: http://www.f-secure.com/en/web/home_global/worldmap

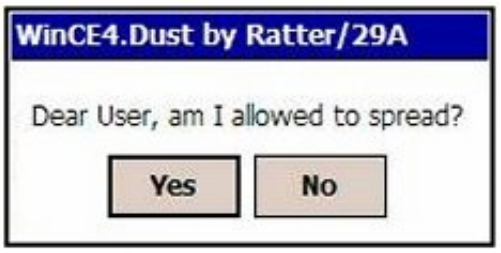
Useissa sähköpostiohjelmissa oleva esikatselutoiminto kannattaa asettaa pois käytöstä. Tietokone ei voi myöskään tavallisesti saada tartuntaa tavallisista tiedostoista - kuvat, äänet, teksti, tms - ellei niiden avaamiseen käytetty ohjelma ole saanut tartuntaa. Jotkut tiedostot käyttäytyvät kuitenkin ohjelmina, esim. komentotiedostot (.bat) ja erityyppiset makrot esim. Wordissa tai Excelissä. Lisäksi kuvatiedostoihin voidaan piilottaa näkymättömiä käskyjä, jotka kuvaa näyttävä ohjelma saadaan suorittamaan eräissä tilanteissa tai html-muotoisen sähköpostiviestin avaaminen voi aiheuttaa tartunnan, vaikka viestissä ei olisi liitettä.

Ammattimaista toimintaa

Tehokkaat haittaohjelmat ovat nykyään ns. ammattilaisten tekemiä (= haittaohjelmientekijöille maksetaan siis palkkaa) ja yhä useammat niistä ovat tehty varastamaan tietoja koneilta ja/tai ottamaan saastunut laite hallintaansa. Järjestäytynyt rikollisuus on yhä yleisemmin nettiuhkien taustalla. Rikolliset harjoittavat tuottavaa liiketoimintaa käyttäen luottokorttipetoksia, nettihyökkäyksillä kiristämistä tai roskapostia käyttäviä huijauksia. Tietoturvayhtiö Verisign:in mukaan rikolliset käyttävät hyväkseen nopeisiin laajakaistoihin liitettyjä suojaamattomia tietokoneita, jotka on virusten avulla saastutettu ja apuohjelmilla liitetty suuremmaksi hyökkäysverkoksi omistajien tietämättä (ns. bottiverkot). Lisää voit lukea esim.: Muistio tietoja varastelevista haittaohjelmista osoitteessa http://www.cert.fi/ohjeet/2010_14.html

Suojautuminen

Tietokonetta voidaan turvata kohtuullisen helpoilla menetelmillä: ajanmukaisilla palomuuri- ja virustorjuntaohjelmistoilla sekä ajantasalla olevalla käyttöjärjestelmällä, selain- ja muilla ohjelmilla. Automaattisesti päivittyvän virustorjuntaohjelmiston ns. sormenjälkitiedosto voi päivittyä jopa kerran tunnissa.



Vaivaako sinua ns. OK-syndrooma? Haluatko päästä eroon häiritsevistä kyselyistä painamalla aina Yes tai Enter.

Käyttäjän omalla varovaisella käyttäytymisellään on iso merkitys, esim. jätä avaamatta epäilyttävät liitetiedostot ja tarkista lataamasi ohjelmat ja komponentit ja vastaa kysymykseen Sallitko... : EI, jos et ymmärrä mitä todella olet sallimassa.

Jos selaimesi sallii esim. ponnahdusikkunat, on ne turvallisinta sulkea ikkunan oikeassa laidassa olevasta X-merkistä, koska vastaamalla ”Kyllä tai Ei” voidaan koneellesi ladata joka tapauksessa jokin haittaohjelma. Vielä parempi tapa on sulkea ikkuna käyttäen Alt+F4 -näppäinyhdistelmää.

Tutustu ja opiskele suojaamiseen liittyvi asioita esim. f-securen www-sivuilla.

Sähköpostin liitetiedostojen suhteen mieti, onko tiedosto peräisin tunnetusta lähteestä, onko sinulla jokin perusteltu käsitys sisällöstä, onko sinulla avaamiseen jokin perusteltu syy vai avaatko sen pelkästä uteliaisuudesta. Turvallisempaa on aina tallettaa tiedosto ensin levylle ja avata vasta sen jälkeen tiedosto, koska virustorjunta yleensä tarkistaa kovalevyltä avattavat tietyn tyyppiset tiedostot. Varmista että virustorjuntasi tarkistaa ainakin tavallisimmantyyppiset tiedostot (.bat, .bin, .cmd, .com, .exe, .pif, .scr, .sys ja .vbs., jne.)

Koska tietokoneohjelmat ja järjestelmät ovat ja tulevat olemaan haavoittuvia, on tärkein yksittäinen suojauskeino päivittää käyttöjärjestelmä ja kaikki muutkin ohjelmat. On vain ajan kysymys milloin jokin ohjelma todetaan turvattomaksi. Esim. vielä joitakin aikoja sitten Acrobat Reader -ohjelmaa ja .pdf -dokumentteja pidettiin turvallisina, mutta tänä päivänä ei enää niin ole. Tavallinen käyttäjä suojautuu parhaiten käyttämällä uusia ohjelmistoversioita ja olemalla varovainen.

Todellisuudessa ei ole mitään keinoa suojautua 100 %:sti. Lähes kaikki jo tietävät, että tuntemattomilta sähköpostin tulleita liitetiedostoja ei saa avata, mutta myös tutuilta tulleet liitetiedostot voivat siis sisältää haittaohjelmia. Internetissä surffailu vain luotetuilla sivustoilla ei sekään estä haittaohjelmia; se vain on turvallisempaa kuin ns. missä vain surffailu. Toisaalta haittaohjelmat (verkkomadot) voivat luikerrella koneeseen ilman, että käyttäjä tekee yhtään mitään - ei esimerkiksi tarvitse edes istua koneen ääressä. Muun muassa siksi konetta ei kannata pitää aina auki, jos sitä ei käytetä.

Saastuneen tietokoneen puhdistamiseen ainoa *varma* keino voi olla kiintolevyn formatointi ja uudelleenasennus. Vaikka siis käytettäisiin viruksenpoistotyökalua, niin aina ei voida olla varmoja etteikö jokin rootkit tms. jää järjestelmän uumeniin. Uudelleenasennuksen yhteydessä puhtaat ja toimivat varmuuskopiot ovat usein korvaamattoman arvokkaat.

Varautuminen: 1) Järjestelmien eristäminen julkisista verkoista ja toisistaan. 2) Ylimääräisten palvelujen poisto ja esto (SQL, levyjaot, chatit, p2p; sähköpostin liitetyypit). 3) Lukitut vakiokokoonpanot työasemilla ja palvelimilla. 4) Käyttöoikeuksien hallinta (hidastaa haittaohjelmien leviämistä, haittaohjelmilla samat oikeudet kuin käyttäjillä). 5) Testattu varmuuskopiointijärjestelmä. 6) Vastuuhenkilöt ja kriisisuunnitelma. 7) Päivystys

Reagointi: 1)Hälytyksen saaminen. 2) Avainhenkilöille tiedottaminen. 3) Toimintaohjeiden testaus ja jakelu.

Virustorjuntaohjelmia

Virustorjuntaohjelmia löytyy sekä maksullisia ja ilmaisia.
Maksulliset: F-Secure anti-virus,Symantec Norton anti-virus, McAfee virusscan, Etrust antivirus, Norman virus control, Panda antivirus, Sophos anti-virus,...
Seuraavassa muutamia laajasti käytettyjä maksuttomia: Antivirus Personal Edition, Avast! Home Edition,AVG Free Edition,...

Vakoiluohjelmien poisto

Virustorjuntaohjelmat eivät pysty poistamaan ns. mainosohjelmia ja eivätkä aina vakoiluohjelmiakaan, siksi virustorjuntaohjelman lisäksi koneella tulisi olla muutama poisto-ohjelma niitä varten. Saatavana on monia erilaisia kaupallisia ja ilmaisia poisto-ohjelmia. Näistä esimerkkeinä löydät ilmaiset Ad-Aware ja Spybot Search & Destroy. Vakoiluohjelmienpoisto on nykyisin usein myös osana kaupallisia tietoturvapaketteja.

KISS

Koska kaikissa ohjelmissa on ns. bugeja ja monimutkaisissa järjestelmissä on aina paljon bugeja, niin minimoi ja yksinkertaista: ei turhia palveluita, ei turhia softia, ei turhia ominaisuuksia asennettuna tai käyttöönotettuina. Aja ohjelmat minimioikeuksilla: älä käytä konetta admin-oikeuksilla, jolloin haittaohjelmilla on vain käyttäjän oikeudet! Joskus tietoturvaohjeissa käytetäänkin lyhennystä **KISS** eli **K**eep **I**t **S**imple **S**tupid.

Tietoturvaoppaan itsepuolustuskurssi-video ja CERT-FI tietoturva nyt:
http://www.tietoturvaopas.fi/perusohjeet/tietoturvaiskut/internetin_itsepuolustuskurssi.html

http://www.cert.fi/tietoturvanyt/2012.html

Vaaran aiheuttaminen tietojenkäsittelylle

Virusohjelmat voivat aiheuttaa laajaa oikeudellista epävarmuutta ja estää mm. sähköisen asioinnin tuhoamalla sähköisten asiakirjojen luotettavuusperustan. Suomen rikoslain lukuun 34 on 1999 lisätty Vaaran aiheuttaminen tietojenkäsittelylle -niminen rikos, jonka mukaan rangaistavaa on tietojenkäsittelylle tai tieto- tai telejärjestelmän toiminnalle haittaa aiheuttamaan suunnitellun viruksen valmistaminen, saataville asettaminen ja levittäminen ja josta voidaan tuomita sakkoa tai vankeutta enintään kaksi vuotta.

4.4 Salasana

Autentikoinnissa perinteinen tapa on käyttää salasanoja. Vaikka joissakin tapauksissa salasanat voivat tallentua järjestelmään selväkielisinä, on salasana yleensä salakirjoitettu ottamalla siitä tiiviste yksisuuntaisen funktion avulla. (Joissakin tapauksissa salattu salasana voidaan myöhemmin muuttaa takaisin selväkieliseksi tekstiksi.) Helppo, lyhyt ja/tai sanakirjan sanaan perustuva salasana voidaan kuitenkin sopivan ohjelman avulla aukaista muutamassa minuutissa. Jos järjestelmään tunkeutuja pääsee työaseman luokse ja salasana on kirjoitettu lapulle työaseman viereen tai piilotettu näppäimistön alle, ei mitään ohjelmia edes tarvita.

Käyttäjän todennuksen ja pääsynhallinnan pohjana tulisi olla ns. user lifecycle management, jolloin käytössä on yhteinen tietokanta kaikkien järjestelmien kaikista käyttäjistä ja heidän oikeuksistaan ja kaikissa erillisjärjestelmissä on kryptografiset todennusmenetelmät ja omat salausmenetelmänsä. Lisäksi voidaan käyttää kertakäyttöisiä salasanoja tai todentamislaitteita ja toimikortteja.

Käytännössä loppukäyttäjien itse keksimien salasanojen joukossa jonkun käyttäjän (todennäköisesti useiden) salasana on aivan liian suurella todennäköisyydellä huono. Tällöin ne voidaan erilaisilla menetelmillä ja tarkastusohjelmilla saada selvitettyä muutamassa minuutissa.

Murtotekniikoita

Sanakirjahyökkäys

Sanakirjahyökkäys käyttää pohjanaan laajaa, jopa satoja tuhansia sanoja sisältävää listaa. Jokainen listassa oleva sana kokeillaan erikseen. Usein ohjelmat osaavat tehdä yksinkertaisia sanamuunnoksia kokeilemalla sanat takaperin sekä isolla ja pienellä alkukirjaimella, tai yhdistelemällä niihin erilaisia numeroita. Periaatteessa salasana ei saa olla minkään valtakielen perusmuodossa oleva sana. Sanakirjalistoja on saatavissa myös suomeksi. Huonoja ovat myös kaikenlaiset mytologiaan ("phoenix", "merlin", "venus"...), fantasiakirjallisuuteen tai -elokuviin ("gandalf", "spock"...) ja tietokoneslangiin ("virtual", "reality", "byte" …) liittyvät sanat, sillä ne kuuluvat jokaisen krakkerin sanavarastoon.

Brute-force -menetelmä

Brute-force eli ns. raa'an voiman murto perustuu nimensä mukaisesti pelkkään laskentavoimaan. Tietokone yksinkertaisesti kokeilee kaikki mahdolliset kirjanyhdistelmät yksi kerrallaan, kunnes löytää oikean salasanan. Kyse on siis vain ajasta ja kärsivällisyydestä. Nykyisten tehokkaiden tietokoneiden aikana brute-force on tehokas työkalu.

Petteri Järvisen kirjassa Tietoturva ja yksityisyys (2002) on esimerkki siitä, minkä verran Pentium III käyttää salasanan etsintään aikaa:

Salasana	Aika	Kokeiluja
mu	0 s	360
mui	0,1 s	9 344
muik	1,0 s	159 612
muikk	38 s	6 316 166
muikku	16 min 40 s	164 220 312
muikkuj	13 h 30 min 7 s	4 269 728 096

Jokainen kirjain lisää murtoon kuluvaa aikaa 26-kertaiseksi. Pitkät salasanat ovat aika turvallisia, koska niiden murto kestää niin kauan, ettei siitä ole hyötyä krakkerille.

Tilanne muuttuu kuitenkin jatkuvasti. Kuinkahan nopeasti nykyisillä nopeilla koneilla voitaisiin avata vastaavat salasanat?

Katso: http://www.lockdown.co.uk/?pg=combi

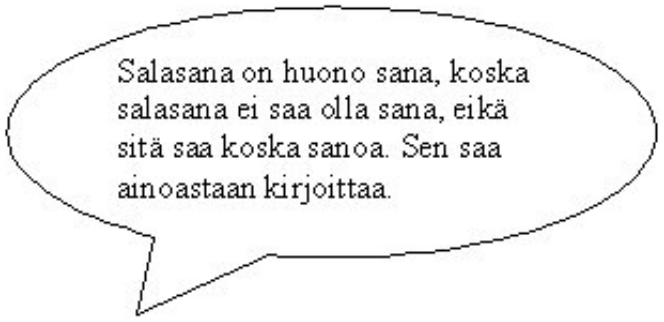
Se millaisia tietoja järjestelmä sisältää on suorassa suhteessa siihen, kuinka paljon krakkeri on valmis käyttämään murtautumiseen aikaa! Nykyisin peruskäytössä suositellaan / vaaditaan salasanan pituudeksi 8 merkkiä. Onko pituus riittävä siinäkään tapauksessa, että itse järjestelmässä ei olisi haavoittuvuuksia?

Kaappaaminen verkosta

Krakkeri voi myös yrittää kaapata salasanan verkosta. Tällöin krakkeri salakuuntelee verkkoliikennettä toivoen löytävänsä viestin, jossa salasana siirretään verkossa. Erityistä huomiota tulee kiinnittää yrityksiin ja koteihinkin rakennettujen langattomien verkkojen suojaamiseen (WLAN). Suojaamisessa tulee käyttää kotonakin mm. salausta ja yrityskäytössä kodin ja työpaikan välisessä liikenteessä VPN:ää.

Hyvä salasana

Ei johdettavissa: käyttäjätunnuksesta johdetut salasanat ovat niitä joita on helpoin arvata ja murtautujat kokeilevat ensimmäiseksi. Jos käyttäjätunnuksesi on vvirta, ei salasana saa olla esimerkiksi virtav, virtavirta, atrivv eikä varsinkaan vvirta. Tosin usein itse järjestelmäkään ei hyväksy tällaisia salasanoja. Erittäin huonoja ovat myös tietyt salasanaan yleisesti liittyvät sanat kuten "salasana", "salasala" "salainen", "password", "secret" jne.



Ei mitään henkilökohtaista: käytännössä käyttäjät valitsevat usein helposti muistettavia salasanoja jotka liittyvät jollakin tapaa heihin itseensä. Tällaisia ovat esimerkiksi puolison, lapsen tai lemmikin nimi, toinen etunimi, syntymäpäivä, auton rekisterinumero, jne. Näitä salasanoja murtautujat kokeilevat toiseksi.

Riittävä pituus: usein järjestelmä vaatii tietyn mittaisen salasanan. Brute force- tekniikan murto-ohjelmat käyvät jokaisen kirjaimen läpi erikseen. Siksi esimerkiksi aaaaaaaa on parempi salasana kuin Kas8n0.

Eri sana eri paikkoihin: meillä on muisteltavana useita käyttäjätunnuksia, salasanoja ja PIN-koodeja ja lisäksi salasanat eri paikkoihin tulee vaihtaa säännöllisesti. Verkkopalvelut, työasemat, sähköpostit, puhelin, pankkikortit, jne. Älä kuitenkaan käytä samoja salasanoja tai pidä ainakin työpaikan, koulun, henkilökohtaiset ja verkkopalveluiden rekisteröinnin yhteydessä annettavat salasanat erikseen.

Isot ja pienet kirjaimet ja erikoismerkit: käyttö moninkertaistaa brute-force -hakuun vaadittavan ajan. Esimerkiksi:

Salasana	**Mitä kokeiltava**	**Aikaa kului**
muikku	pienet	16 min 40 s
MuikKu	pienet, isot	8 h 58 min
Mui789	pienet, isot, numerot	1 vrk 13 h 43 min
Mui-89	pienet, isot, numerot, erikoismerkit	19 vrk 13 h 27 min

Luo muistisääntöjä, joiden avulla vain sinä tiedät salasanan kirjainnumeroyhdistelmän. Esim. jotta paremmin muistaisit salasanan, valitse lause joka perustuu pitkäaikaiseen muistiisi ja käytä esimerkiksi koosteita alku- tai lopputavuista tai ensimmäisistä tai toisista kirjaimista. Sekoittamalla näihin erikoismerkkejä ja numeroita saat hyviä salasanoja:

- Jospa minulla olisi rahaa kuin itsellään Roope Ankalla! -> Jmo$kiRA!
- Myös (too -> two -> 2) minä synnyin Kirkkokatu 20 A 20 osoitteeseen -> 2msK20A20o
- Tietoturva opintojakso 3 op -> Tta-ojo+3op
- Helppo sala -> sapo_Hela

Kirjaimen tai sanan osan korvaaminen sitä muistuttavalla numerolla tai erikoismerkillä taikka numeron lisääminen perusmuotoisen sanan alkuun tai loppuun on huono keino. Älä valitse salasanaksi esimerkiksi merkkijonoa "n011aus", "5uur15uu", "$atanen" tai "1salattu2". Muissa tapauksissa numeron/kirjaimen/erikoismerkkien sekoittaminen vaikeuttaa salasanan selvittämistä. Esim. sapo_Hela --> $ap0_He1a

Salasanaideoiden loppuessa ja vaihtamisen kiireessä tulee keksittyä huonoja salasanoja. Tutustu ohjeeseen vahvoista salasanoista.

Erityisesti verkon etäkäytössä kertakäyttöiset salasanat ovat hyviä. Silloin käyttäjä luo salasanan (tai numeron) tavallisesti erityisellä todentamislaskimella (mm. token), johon hänellä on henkilökohtainen PIN-luku. Menetelmiä miten todentamisessa (synkroninen / asynkroninen) käytetty salasana luodaan ja varmistetaan on useita (esimerkki RSA SecurID Token -kortti).

Salasanojen riskit

Pitkät ja monimutkaiset (=turvalliset) salasanat voivat unohtua helposti. Lisäksi niiden kirjoittamisessa tulee virheitä ja jos joudut kirjoittamaan salasanan hitaasti tai kahdella sormella on vaarana, että lähettyvillä olevat henkilöt näkevät mitä näppäilet.

Koneelle on voitu ujuttaa takaovi- tai vakoiluohjelma, joka tallentaa kaikki näppäinpainallukset ja paljastaa salasanan, olipa se kuinka pitkä tai mutkikas tahansa.
Varmistu siis, että kone on puhdas!

Salasana liikkuu usein selväkielisenä (kuten POP3-sähköpostiprotokollassa) kun se lähetetään palvelimelle tai Internet-palveluun. Ratkaisuna voidaan käyttää haaste/vaste-menetelmää, jolloin palvelu lähettää joka kirjautumiskerralla satunnaisen haasteen, jonka käyttäjä koodaa omalla salasanallaan ja lähettää takasin. Palvelu laskee saman koodauksen tiedossaan olevalle käyttäjän salasanalle ja vertaa tuloksia. Jos ne ovat samat, todennus onnistuu.

Helpon tapa siepata salasana on saada käyttäjä kertomaan se itse. Tätä kutsutaan **sosiaaliseksi hakkeroinniksi**. Jos esimerkiksi "mikrotukihenkilö" soittaa sinulle ja kertoo tarvitsevansa salasanaasi vaikkapa jonkin huoltotyön yhteydessä, älä kerro sitä. Jos jostain kumman syystä kirjautumistietosi olisi välttämätöntä kertoa, katkaise puhelu ja soita itse takaisin mikrotukihenkilölle. Näin varmistut, että kyseessä on oikea mikrotuki.

Kertakäyttösalasanat/-koodit ovat usein käytössä esimerkiksi pankki- ja osakevälityspalveluissa. Ne vanhenevat heti ensimmäisen käyttökerran jälkeen ja salasanalistan jokin toinen salasana on aina seuraava voimassaoleva salasana. Oleellista on että salasanalista ja käyttäjätunnus pidetään erilleen talletettuina ja piilossa. Käyttäjätunnus tulee mieluiten painaa muistiin, eikä sitä tule kirjoittaa mihinkään ylös.

Useissa järjestelmissä on mahdollista tallentaa salasana järjestelmän muistettavaksi, niin että uudella kirjautumiskerralla salasanaa ei enää kysytä. Tätä mahdollisuutta ei pipäisi käyttää missään järjestelmässä (ks. luku Sosiaalinen media; twitter)!

Käyttäjätunnuksen ja salasanan tulisi olla aina henkilökohtainen. Joissakin tapauksissa voidaan käyttää useille henkilöille yhteisiä ryhmäkäyttäjätunnuksia. Näiden käyttöä tulisi välttää, koska yhteistunnusten käytön valvonta on vaikeaa. Ongelmatilanteissa ei voida osoittaa riittävän tarkasti kuka, mitä ja milloin teki.

Huomattavaa on myös se, että joissakin järjestelmissä on takaporttina ns. vakiosalasana. Tämä sijaitsee BIOS:ssa siltä varalta, että käyttäjä unohtaa salasanansa.

Eri järjestelmissä on käytettävä erilaisia salasanoja. Esimerkiksi OAMK:n järjestelmissä käytettäviä salasanoja ei tule käyttää missään muussa järjestelmässä. Jos käyttäjällä on esimerkiksi gmail- tai hotmail-osoite, ei sen salasana saa olla sama kuin OAMK:n salasanat. Krakkeri tarkistaa usein, kelpaako yksi kaapattu salasana muihin saman ihmisen käyttämiin palveluihin.

Säilytä salasana varmassa paikassa; älä kuljeta sitä kännykän muistissa, lompakossa tai paikassa, josta se voi joutua vääriin käsiin.

Työtiedostojen salasanat

Uusimmissa Office työvälineohjelmissa työtiedostojen salasanasuojauksessa on mahdollista hyödyntää käyttöjärjestelmän tarjoamaa salauspalvelua. Tämän tarkoitus on esim. suojata Word-asiakirja muutoksilta. Kovin luotettava tämä ei ole, koska Internetistä on mahdollista saada krakkerointiohjelma, jolla salaus voidaan purkaa, asiakirjan sisältöä muuttaa ja lopuksi laittaa alkuperäinen salasana takaisin.

Jos asiakirjoja, esim. sopimuksia tai tarjouksia, lähetetään verkossa, kannattaa ne **suojata muutoksilta** ennemmin käyttäen digitaalista allekirjoitusta tai vaikkapa PDF-formaattia.

Varmin tapa **salata** työtiedostot on käyttää jotakin salausohjelmaa.

Varmista, että ymmärrät tiedon suojauksen ja salauksen eron! Mitä tiedon ulottuvuutta eli peruselementtiä niissä suojataan?

Yhteenvetoa

Lähiverkossa työasemat, palvelimet ja verkon käyttö tulee aina suojata vähintään käyttäjätunnuksen ja salasanan avulla. Myös puhelimet, tablet-tietokoneet jne tulee suojata salasanalla tai koodilla.

Kirjautuminen ja resurssien jakaminen tulee tapahtua ennalta määrättyjen pääsynvalvontakontrollien mukaan.

Tavallista käyttäjätunnus-salasana-menetelmää vahvempia suojausmenetelmiä ovat käyttäjän todentaminen kertakäyttösalasanoilla, toimikortilla (sisältää salasana/PIN-koodi) sekä biometrisillä todentamismenetelmillä. Useamman menetelmän yhtäaikainen käyttö lisää suojaa entisestään.

Useissa järjestelmissä on mahdollisuus ottaa käyttöön turvallisuutta parantavia ominaisuuksia. Esim. useita kertoja väärän salasanan syötetty käyttäjätunnus lukitaan joko määräajaksi tai kokonaan (kunnes tukipalvelut vapauttavat käyttäjätunnuksen) tai pankkikortin PIN-tunnus, jolloin automaatti ns. syö kortin.

4.5 Biometriset tunnistusmenetelmät

Luotettava tunnistaminen on tietoturvallisuuden yksi tärkeimmistä vaatimuksista. Henkilöllisyyden tunnistusmenetelmät voidaan jakaa kolmeen ryhmään:

1. Tietoon perustuvat (esim. salasanat, PIN-koodit) eli jotain, mitä tiedät
2. Aineelliset, omistettavat asiat (toimikortit, passi) eli jotain, mitä omistat
3. Henkilön fyysiset tuntomerkit (fysiologiset ja behavioristiset) eli biometriset tuntomerkit eli jotain, mitä olet

Kaksi ensimmäistä menetelmää ovat haavoittuvia, koska ne ovat varastettavissa. Kolmas eli biometriikka on tulossa kahden ensimmäisen menetelmän rinnalle. Siinä käyttäjä tunnistetaan henkilökohtaisen ominaisuuden perusteella eli käyttäjä itse on oma ns. salasanansa. Tällaisia henkilön ominaisuuksia ovat esim. sormenjälki, kasvonpiirteet, silmä, ääni.

Biometriikka perustuu joukkoon tekniikoita, joilla henkilö tunnistetaan mittaamalla jotain hänen yksilöllistä piirrettä. Tämä on tehokas tapa, koska yksilöllisiä fysiologisia yksityiskohtia tai toimintatapoja on lähes mahdoton varastaa tai täydellisesti imitoida. Lisäksi biometrisen salasanan hukkaaminen tai unohtaminen on epätodennäköistä. Käytännössä biometristen tunnistusmenetelmien helppouteen ja turvallisuuteen vaikuttavat monet eri tekijät.

Biometriset tekniikat voidaan jakaa kahteen luokkaan:

- Fysiologiset mittaavat fyysisiä ominaisuuksia
- Behavioristiset, käyttäytymiseen perustuvat menetelmät

Biometriset menetelmät perustuvat biometrisen informaation muuntamiseen numerotiedoksi, jonka perusteella tuotetaan matemaattinen malli. Mallia voidaan verrata henkilön aiemmin antamiin näytteisiin. Vertailtaessa alkuperäistä ja annettua näytettä saadaan arvo kuinka hyvin annettu näyte vastaa alkuperäistä. Jos ko. arvo hyväksytään, käyttäjälle annetaan pääsy haluttuun tietoon tai toimitilaan. Kyseinen arvo annetaan yleensä välillä 0..100, joka kuvastaa kuinka hyvin prosentuaalisesti näyte on vastannut alkuperäistä. Itse tarkistuksessa usein tapahtuu jotain mittausvirheitä ja tästä johtuen jokaiseen järjestelmään määritellään erikseen oma mittaustaso prosentteina mikä pitää ylittyä, jotta biometrinen salasana on hyväksyttävä. Lisäksi käyttäytymiseen liittyvissä malleissa alkuperäinen näyte tulee uusia aika-ajoin, jotta näyte on ajan tasalla ja vastaa henkilön sen hetkistä toimintamallia.

Biometrisen tunnistusmenetelmien toimintaan vaikuttaa myös se mihin niitä käytetään: varmistamiseen (verify) jolloin varmistetaan, että käyttäjä on kuka hän väittää olevansa vai tunnistamiseen (identify) jolloin käyttäjä on joku järjestelmän tunnetuista henkilöistä. Ensimmäisessä vaihtoehdossa käyttäjän täytyy ensin esittää väite omasta henkilöllisyydestään esim. PIN-koodilla, älykortilla tai käyttäjänimellä ja sen jälkeen todistaa henkilöllisyys biometrisella näytteellä. Toisessa vaihtoehdossa käyttäjästä otettua näytettä verrataan kaikkiin tallennettuihin näytteisiin ja hyväksytään tunnistus, jos näyte on riittävän lähellä jotain tallennetuista näytteistä.

1) Fysiologiset mittausmenetelmät

Fysiologiset menetelmät mittaavat fyysisiä ominaisuuksia, kuten kasvoja, silmää (iiris), sormia (sormenpää, peukalo, sormen pituus tai muoto), kämmentä (muoto tai kosketuspinnat), käden mittasuhteita, kämmenselän suonistoa tai käden lämpökuvaa.

Sormenjälki

Tunnistus sormenjäljestä on kaikkein käytetyin fysiologinen tunnistusmenetelmä. Ihmisen sormenjälki on erittäin luotettava. Luotettavuus perustuu kahteen perusasiaan. Ihmisen kaikki kymmenen sormenjälkeä ovat yksilöllisiä. Jopa identtisillä kaksosilla on erilaiset sormenjäljet. Toiseksi, sormenjälki ei muutu iän myötä toisin kuin jotkut muut fyysiset ominaisuudet kuten kasvot. Sormenjäljen käyttäminen on yleisesti hyväksyttyä ja sitä onkin käytetty jo lähes vuosisata täysin luotettavana todisteena rikostutkinnassa.

Luotettavuuden lisäksi sormenjäljen käyttöä puoltavat muutkin seikat. Ihmisellä on esimerkiksi 10 sormea joilla on kaikilla identtinen sormenjälki ja kaikkien sormien menettäminen on erittäin harvinaista kun verrataan esimerkiksi

ihmisen yhteen ääneen tai kahteen silmään.

Menetelmä on halpa ja helppo toteuttaa. Tunnistukseen vaikuttaa kuitenkin sormen pinnalla olevat haavat, rypyt, lika, rasva ja kova pakkanen. Lisäksi ikäihmisten ja raskasta työtä tehneiden sormet asettavat omat haasteensa tunnistukselle. Sormenjäljestä tunnistaminen tapahtuu siis 100 % tarkkuudella. Ongelmana on kuitenkin ollut huijaaminen ns. sormenjäljen kopiokuvalla.

Sormenjälkitunnistusta käytetään mm. kulunvalvonnassa, kannettavissa tietokoneissa, matkapuhelimissa ja tietokoneen hiirissä tai näppäimistöissä.

Sormenjälkitunnistin USB-muistissa

Yhden sormen tunnistuksen sijaan voidaan käyttää myös esim. kahta sormea. Erilaisiin skannereihin voit tutustua esim. sivuilla http://www.crossmatch.com/

Kasvojen tunnistus

Kasvojen tunnistamismenetelmien historia ulottuu 1950-luvulle, jolloin julkaistussa artikkelissa esiteltiin tunnistamismenetelmä, joka perustui tallennettuun referenssikasvokuvaan merkittyjen tunnistuspisteiden vertaamiseen testikuvan vastaavien pisteiden kanssa. Kuitenkin ensimmäiset toimivat sovellukset olivat testausvaiheessa vasta 80-luvun vaihteessa.

Kasvojen tunnistusmenetelmät voidaan jakaa mm. käytettävän syötedatan perusteella kasvokuvien vertailua käyttäviin menetelmiin ja kasvojen sivuprofiilia syötteenä käyttäviin menetelmiin. Yksinkertaisesti sanottuna **kasvokuvan tunnistaminen** tapahtuu erilaisten kiinnepisteiden, kuten silmien, sieraimien, suun jne. sijainnin ja muodon vertaamista kasvojen geometriseen malliin, jonka avulla voidaan varmistaa onnistuiko piirteiden kartoitus.

Käytännössä kuitenkin lopputulokseen pääsemiseksi tarvitaan lukuisa määrä erilaisia korjaus- ja varmistusoperaatioita, kuten kasvojen joustavuudesta johtuvan vinoutuman korjaus ja kuvan valoisuuden, skaalan ja rajauksen normalisointi. Itse korjatun näytteen vertaaminen alkuperäisnäytteeseen vaatiikin sitten monimutkaisten matemaattisten mallien hyödyntämistä, jotta saadaan lopullinen mittaustulos.

Samoin kuin kasvokuvan tunnistuskin, **kasvoprofiilien** tunnistusprosessi lähtee liikkeelle kuvien esikäsittelystä. Voimakas kontrastin lisäys, kulmien etsintä ja lopulta kuvan muuttaminen binääriseksi ovat yleisimmin suoritettavia esikäsittelyoperaatioita, joiden tuloksena saadaan musta sivuprofiilisilhuetti valkoista taustaa vasten. Tämän jälkeen kasvojen ääriviiva mallinnetaan murtoviivalla niin, että jokainen viiva yhdistyy toiseen muodostaen katkeamattoman ketjun. Tästä kuvasta prosessoitua matemaattista mallia sitten verrataan samoin käsiteltyyn alkuperäisnäytteeseen.

Kasvojen tunnistusta pidetään yleensä kohtalaisen vakaana ja halpana tunnistusmenetelmänä. Kasvojen perusteella tapahtuvassa tunnistamisessa on kuitenkin jonkin verran ongelmia luotettavuuden osalta jonka takia sitä ei pitäisi käyttää ainoana tunnistamismuotona tärkeissä yhteyksissä. Ongelmia on aiheuttanut juuri se, että tunnistus ei ole ollut ikinä täydellinen eli täyttä 100 %:a. Mahdollisena käyttösovelluksena mainittakoon esimerkiksi yksittäisen ihmisen tunnistaminen suurista ihmisjoukoista.

Tunnistus silmästä

Biometriseen tunnistukseen silmien avulla on kaksi pääasiallista tekniikkaa: verkkokalvon tunnistus ja iiriksen tunnistus.

Verkkokalvon (silmän takaosassa oleva osa, jossa valoa aistivat solut sijaitsevat) perusteella tehtävässä tunnistuksessa käyttäjä tunnistetaan verkkokalvon takana olevan verisuoniverkoston perusteella. Käyttäjän on oltava lähellä tunnistuslaitetta.

Iiriksen (silmän pupillin ympärillä oleva värillinen alue) avulla voidaan tunnistaa henkilö jopa muutaman metrin päästä. Nykyisillä menetelmillä tunnistuksen tekemiseen menee vain sekunnin murto-osa eli se on erittäin nopea tapa.

Verkkokalvon pohjalta toimiva tunnistus on teknisesti vaikeampi. Verkkokalvon kuvaaminen on tarvittavan laitteiston kannalta vaikeampaa kuin iiriksen kuvaaminen. Siitä huolimatta verkkokalvotunnistus on julkisuudessa tunnetumpi tekniikka. Verkkokalvon tunnistamiseen vaadittava laitteisto on mm. huomattavasti kalliimpi kuin iiriksen tunnistukseen käytetyt välineet. Ihmisen silmä on jokaisella yksilöllinen ja se pysyy muuttumattomana koko eliniän aivan kuten sormenjälkikin. Sen avulla voidaan tunnistus suorittaa erittäin luotettavasti.

Vaikeutena silmän tunnistamisessa mainitaan ainakin seuraavat seikat. Tarvittavat tiedot sijaitsevat erittäin pienellä alueella, jolloin käytännössä tunnistus on tapahduttava lähietäisyydeltä. Iiriksen liikkuvuus saattaa aiheuttaa myös omat ongelmansa, koska kohde voi olla vaikeasti paikannettavissa. Valaistus voi myös tuottaa ongelmia johtuen silmän kaarevuudesta, joten silmän heijastama kuva voi häiritä tunnistusta. Lisäksi silmäntunnistusmenetelmät ovat poikkeuksetta kalliita.

B) Behavioristiset mittausmenetelmät

Behavioristiset eli käyttäytymiseen perustuvat menetelmät puolestaan tutkivat ääninäytteitä, allekirjoitusta ja näppäimistön painalluksien kiihtyvyyksiä.

Käsiala ja allekirjoitus

Varmaan kaikkein tutuin ja käytetyin käyttäytymiseen perustuva tunnistusmenetelmä on käsialan tai allekirjoituksen tutkiminen. Kaikilla meillä on oma henkilökohtainen käsiala ja varsinkin allekirjoituksemme on 100 % yksilöllinen. Nämä seikat mahdollistavat varsin tarkan ja varman lopputuloksen yksilön tunnistamiseen. On mm. sanottu, että jos törmää kahteen identtiseen allekirjoitukseen voi olla varma toisen olevan väärennös.

Käsialan tutkimiseen on olemassa ainakin kaksi tunnustettua menetelmää. Ensinnäkin käsin kirjoitettua tekstiä voidaan vertailla saman ihmisen aiemmin kirjoittamaan tuotokseen. Tällainen vertailu voidaan suorittaa joko tietokoneella tai käsiala-asiantuntijan toimesta. Kuitenkin pitää muistaa, että digitaalisessa muodossa olevaa käsinkirjoitettua tekstiä ei voida pitää kovinkaan luotettavana sillä sen kopioiminen on helppoa. Toinen keino on nimikirjoituksen kirjoittaminen, jolloin itse kirjoitusprosessi tutkitaan. Tätä menetelmää pidetään varmempana kuin edellä mainittua. Kirjoitusprosessia tutkitaan sarjana liikkeitä. Näin saadaan kerättyä yksilöllistä, uniikkia tietoa. Liikkeistä tutkitaan esimerkiksi rytmiä, nopeutta, kiihtyvyyttä ja painetta. Vaikka nimikirjoitus on jokaisella ihmisellä aina erilainen, näin se voidaan yhdistää tiettyyn henkilöön.

Käsiala-analyysiä pidetään kohtuullisen luotettavana menetelmänä. Ongelmia kuitenkin aiheuttaa jo aiemmin mainittu digitaalisen analyysin huijattavuus ja menetelmän kohtuullisen kallis hinta.

Ääninäyte tunnisteena

Ääninäytteen tunnistaminenkin pohjautuu aiemmin annettuun alkuperäisnäytteeseen. Tunnistusmittausta varten tulee siis nauhoittaa henkilön alkuperäinen ääninäyte, joka talletetaan tietokantaan, josta sitä voidaan käyttää sitten vertailukohtana itse tunnistustilanteessa.

Äänitunnistuksen huonona puolena on helppo huijattavuus. Menetelmä on sinänsä halpa ja helppo toteuttaa, mutta edellä mainitun ongelman takia varsin harvoin käytetty.

Näppäilydynamiikka tunnisteena

Näppäilydynamiikka tunnistusmenetelmänä on prosessi, jossa analysoidaan käyttäjän näppäilytapaa mittaamalla näppäimistöltä tulevaa syötettä tuhansia kertoja sekunnissa, ja tämän perusteella yritetään identifioida käyttäjä

vertaamalla syötteenä saatua näppäilyrytmin hahmoa tietokannassa oleviin yksilöityihin näppäilyrytmin hahmoihin. Tämä muistuttaa menetelmää jota käytetään käsiala-analyysissä, kun kartoitetaan henkilön käden liikkeitä ja kirjoitusrytmiä.

Näppäilydynamiikkaan perustuva tunnistus luokitellaan staattiseen ja jatkuvaan tunnistamiseen. Staattinen tunnistus tarkoittaa, että näppäilyrytmiä analysoidaan esimerkiksi silloin kun kirjoittaudutaan sisään johonkin järjestelmään. Staattinen tunnistus ei täten pysty esimerkiksi huomaamaan, jos käyttäjä vaihtuu kesken istunnon. Jatkuvassa tunnistuksessa seurataan taukoamatta käyttäjän syötetulvaa. Tämä mahdollistaa mm. käyttäjän vireystilan tarkkailun. Jatkuvaa tunnistusta käytetään ainakin lennonvalvojien vireystilan seuraamiseen.

Näppäilydynamiikkaan perustuvat sovellukset ovat vasta viime vuosina saavuttaneet riittävän tason, jotta niillä olisi käytännön merkitystä. Ennusteiden perusteella todennäköisesti tätä teknologiaa tullaan hyödyntämään lähinnä käyttäjien tunnistamiseen erilaisessa tietoverkkojen sovelluksissa. Biometristen tunnistusmenetelmien ominaisuuksien vertailutaulukko löytyy esim. Heurekan sivuilta.

Biometria ja tietosuoja

Seuraava on suora lainaus sisäministeriön sivuilta:

> Biometriset tunnisteet ovat henkilötietoja samalla tavalla kuin nimi, henkilötunnus ja kotiosoitekin. Biometriset ominaisuudet ovat pysyviä, peruuttamattomia ja yksilöiviä. Tunnistamiseen soveltuvat biometriset tunnisteet asettavat erityisiä vaatimuksia tietosuojalle sekä tietoturvalle, jotta sen jonka biometrisiä ominaisuuksia tallennetaan tai käsitellään, yksityisyyden suojan toteutuminen voitaisiin varmistaa.
>
> Biometristen tunnisteiden tietosuojaan liittyy lisäksi joitakin erityisiä piirteitä, jotka on huomioitava biometristen järjestelmien ja alan lainsäädännön suunnittelussa.
>
> - Monia biometria tunnisteita on vaikeata pitää salassa. Esimerkiksi lähes kenestä tahansa on mahdollista hankkia kasvokuva ja sormenjäljet.
> - Biometrisia tunnisteita voidaan yrittää väärentää. Tekosormilla voi yrittää huijata sormenjälkitunnistusta, piilolinsseillä iiristunnistusta ja naamareilla kasvontunnistusta.
> - Biometrisia tunnisteita ei voi vaihtaa kuten vääriin käsiin joutuneita salasanoja tai puhelinnumeroa.
> - Biometrian avulla on ehkä tulevaisuudessa mahdollista valvoa ihmisen liikkumista hänen tietämättään. Erityisesti valvontakameroihin yhdistetty kasvontunnistus saattaa joskus kehittyä tasolle, joka riittää ihmisen tunnistamiseen etäältä ja liikkeestä.
>
> Esimerkiksi alan kehitystyössä panostetaan voimakkaasti aitojen biometristen tunnisteiden ja väärennösten erottamiseen. Lisäksi alan juridisesta säätelystä käydään aktiivista keskustelua monissa maissa.
>
> Perustuslain mukaan oikeus yksityisyyteen on perusoikeus. Biometrinen ominaisuus on henkilötietolain mukainen henkilötieto ja henkilöiden tunnistamisessa tarvittava vertailurekisteri on henkilötietolain mukainen henkilörekisteri. Henkilötietojen keräämisestä ja muusta käytöstä tulee perustuslain 10 §:n mukaisesti säätää lailla.

4.6 Palomuuri

Palomuuriksi (engl. **firewall**) kutsutaan ohjelmaa (sovelluspalomuuri) tai laitetta (rautapalomuuri), joka valvoo ja rajoittaa tietokoneen ja muun maailman välistä verkkoliikennettä. Erityisesti sillä pyritään estämään, että joku voi näkymättömästi käyttää konettasi verkon kautta. Se saattaa myös estää koneeseen päässeitä haittaohjelmia ottamasta yhteyttä ulospäin.

Palomuurilla on osittain samanlainen tehtävä kuin virustentorjunnalla, mutta kumpikaan ei korvaa toista, vaan ne täydentävät toisiaan. Palomuuri toimii verkkoliikenteen tasolla, ja siksi se hoitaa asioita, joihin virustentorjunta ei tehoa. Virustentorjunta käsittelee ohjelmia ja tiedostoja, jotka ovat päässeet koneeseesi. Palomuuri taas estää ulkopuolisia ns. komentamasta koneessasi olevia sinänsä asiallisia ohjelmia asiattomalla tavalla.

Laajakaistayhteyksiä käyttävät koneet ovat usein aina päällä ja ne näkyvät verkkoon pitkiä aikoja samalla IP-osoitteella. Samana pysyvä IP-osoite auttaa krakkeria löytämään koneen uudestaan. Siksi kaikissa koneissa tulisi olla vähintäänkin sovellus- eli ohjelmallinen palomuuri. Sitä suositellaan myös yritysten työasemiin, vaikka ne olisivat jo yhdellä rautapalomuurilla eristetty julkisesta verkosta.

Palomuurin tehtävät

Palomuurit on suunniteltu valvontapisteiksi tietokoneen ja verkon väliin ja sen perustehtävät ovat pääsynvalvonnan suorittaminen (access control) ja tapahtumanseuranta (activity logging). Pääsynvalvontaa tulee suorittaa sekä ulospäin (out-bound access) että sisäänpäin (in-bound access).

Palomuurit arvioivat yhteyspyyntöjä ja päättävät ennalta määritellyn sääntöjoukon perusteella, pitääkö verkkoliikenne sallia vai hylätä. Verkkoliikenteen suodatuksen palomuurit toteuttavat lähde- ja kohdeosoitteiden / porttinumeroiden / sovellusten /palvelun / protokollan / liikenteen sisällön / käyttäjän seulonnalla. Mitä kehittyneempi palomuuriohjelmisto sitä tarkemmin sitä voidaan konfiguroida.

Työaseman sovelluspalomuurit ovat laitteistopalomuureja yksinkertaisempia. Yritysten palomuurijärjestelmät vaihtelevat verkkotopologialtaan ja voivat olla monimutkaisia.

Palomuuri toiminnot voi jakaa karkeasti kahteen ryhmään: TCP/IP-protokollien yleinen pakettisuodatus ja yhdyskäytäväohjelmat eli sovellusprotokollakohtaiset proxyt.

Esimerkki: Kotikoneen hyväksikäyttö

Vaikka kotikoneessa on harvoin mitään tietomurtajaa kiinnostavaa, niin tunkeutuja voi hyödyntää suojaamatonta kotikonetta monin tavoin:

- Koneeseen voidaan piilottaa palvelunestohyökkäyksessä tarvittava kuormitusohjelma, joka aktivoituu hyökkääjän antamasta merkistä.
- Koneen laskentakapasiteettia voidaan käyttää salausavainten murtamiseen. Vaarallisia usein ovat netistä haettavat ohjelmat, joissa saattaa olla takaovia.
- Murtautuja voi kierrättää yhteyksiään usean sivullisen koneen kautta, jotta hänen jäljittämisensä vaikeutuisi. Kohteena olevan verkon tai suojamuurin lokiin tallentuu vain viimeisen koneen IP-osoite, joka saattaa kuulua kotikäyttäjälle.
- Jos koneessa on paljon levytilaa, voidaan sitä käyttää piraattitiedostojen väliaikaisena

varastona.
- Joku saattaa pelkästä uteliaisuudesta ujuttaa koneeseen takaovia tai muita vakoiluohjelmia (mm. identiteettivarkaudet).

Kotikäytössä riittää yleensä ohjelmistolla toteutettu palomuuri. Näitä on sekä maksullisia ja maksuttomia. Esim. Komodo, AVG, Zonealarm, Symantec, F-Secure ja Windows'n oma palomuuri (parempi kuin ei mitään).

Maksuttoman, yleensä suppeamman, palomuuriversion tunnistat sanasta ”Personal”. Maksulliset Pro-versiot ovat monipuolisempia ja ne sallivat mm. tarkemmat liikennöintirajoitukset.

Esim. ZoneAlarm (Pro) tarkkailee Internetiin menevää liikennettä ja antaa ilmoituksen aina, kun koneeseen yritetään ottaa yhteyttä ulkoapäin. Ilmoitus näkyy Windowsin työpöydällä pienessä ikkunassa ja tallentuu myös tekstimuotoiseen lokitiedostoon. ZoneAlarm hälyttää myös, kun jokin koneen ohjelmista yrittää itse ottaa yhteyttä ulospäin. Tämä onkin ohjelmallisen palomuurin paras puoli: se kertoo, mitkä ohjelmat liikennöivät koneesta ulos ja saattaa siten paljastaa erilaisia vakoilu- ja mainostietojen keruuohjelmia.

Toisena esimerkkinä on F-Securen kaupallinen vaivaton tietoturvapaketti kotikoneille, joka sisältää ohjelmistopalomuurin lisäksi muitakin turvallisuuteen liittyviä ohjelmia samassa paketissa, mm. virustorjunnan ja vakoiluohjelmientorjunta. Palomuuri saattaa olla myös mukana WLAN-tukiasemassa. Vaihtoehtoja on lukuisia.

WindowsXP:tä uudempien versioiden käyttöjärjestelmien myötä Windows on saanut paremman palomuurin käyttöjärjestelmän ohessa. Siinä missä Windows XP:n palomuuri tarkkaili täysin riittämättömänä vain koneeseen sisäänpäin tulevaa liikennettä, tarkkailee uudempien versioiden palomuuri myös ulospäin menevää liikennettä.

Jos käytössäsi on jo jokin palomuuriohjelma ja haluat vaihtaa sen, poista ensin aiempi palomuuri (palomuurin kokonaan poistossa voi olla ongelmia!). Samoin poista Windowsin oma palomuuri käytöstä, jos asennat jonkin muun palomuurin. Tämä sääntö koskee myös virustorjuntaohjelmia. Vain yksi ohjelma / kone!

Mikäli etätietokoneella ollaan yhteydessä yrityksen verkkoon, on se suojattava yhtä hyvin kuin verkkokin (anti-virusohjelma, palomuuri, päivitykset). Lisäksi yhteydet on suojattava (esim. VPN:llä).

4.7 Salaus

Salaustekniikat ovat keskeinen osa tietoturvaa. Salausta on yleisesti pidetty vaikeana ja monimutkaisen asiana ja sitä se onkin. Mutta vaikka itse salaus (salausalgoritmi) ja salaukseen liittyvä matematiikka onkin hyvin vaativaa, eivät itse salauksen perusteet ole vaikeita. Erinäisten salausalgoritmien yksityiskohtia ei yleensä tarvitsekaan tietää, kunhan tietää mikä algoritmi sopii mihinkin tarkoitukseen ja miten niitä käytetään eri tuotteissa.

Salakirjoitus ei käsitteenä ole mitään uutta, sillä salakirjoitusta on käytetty tärkeiden viestien lähetyksessä antiikin ajoista lähtien. Tässä ns. Caesarin salauksessa viestin kirjainta siirrettiin kolme pykälää eteenpäin. Näin A:sta tuli D, B:stä E jne. Caesarin salaus on hyvä esimerkki heikosta algoritmista, joka nykyisin voidaan purkaa helposti vaikka käsin. Aikoinaan Caesarin salausalgoritmi oli kuitenkin riittävä harvinaisen lukutaidon vuoksi.

Caesarin salauksessa ovat mukana kaikki elementit jotka ovat ns. oikeiden salaustekniikoissakin. Alkuperäistä viestiä kutustaan selvätekstiksi (plaintext) ja kun se salataan (encrypt) jollakin ennalta sovitulla menetelmällä eli salaimella (chiper), saadaan salateksti (cipertext). Jotta kuka tahansa, joka tuntee menetelmän, ei pystyisi purkamaan (decrypt) salausta, tarvitaan vielä avain (key). Nykyisin Caesarin salaus on aivan riittämätön salausalgoritmi ja siksi uudemmat salausalgoritmit ovat Caesarin salausta huomattavasti tehokkaampia.

Voit kokeilla ns. samantapaista siirtosalausta kuin Caesarin salaus osoitteessa: http://www.rot13.com/index.php . ROT-13 -koodauksessa 13 aakkosmerkkiä siirretään eteenpäin / taaksepäin. Välimerkkejä ja skandinaavisia merkkejä ei muunneta. Mikä on selväteksti salatekstistä: Ghyva, aäva wn ibvgva!

Modernit salaustekniikat

Modernit salaustekniikat pohjautuvat joko tietokoneella tapahtuvaan bittien sekoittamiseen tai matemaattiseen laskentaan. Salakirjoitusmenetelmien turvallisuus perustuu aina niiden monimutkaisuuteen ja niissä käytettyihin suuriin avaimiin (salauksen turvallisuus on suorassa suhteessa avaimen pituuteen). Tietokoneet nopeuttavat salausta ja salauksen purkua oleellisesti. Yleisesti ottaen klassiset salausmenetelmät ovat menettäneet tehonsa nykyaikaisten tietokoneiden myötä. Tämä on pakottanut kehittämään uusia vahvoja salausmenetelmiä. Se, mitä salausalgoritmia tulisi käyttää, riippuu kuitenkin yleensä tiedon laadusta ja siitä kuinka kauan tiedon on tarkoitus pysyä salassa.

Salauksen perustarkoituksena on siis muuttaa alkuperäinen, selväkielinen kirjoitettu viesti koodattuun muotoon, jonka viestin vastaanottaja voi purkaa takaisin selväkieliseksi. Salauksessa alkuperäinen viestin sisältö käsitellään algoritmin avulla. Tämä algoritmi on jokin tunnettu menetelmä, jolla muunnetaan viestin sisältö.

Salaaminen on jaettavissa kahteen perustekniikkaan: salaisen ja julkisen avaimen salaukseen.

Salaisen avaimen salauksessa käytetään yhtä avainta. Viesti salataan ja puretaan samalla avaimella. Sen hyvä puoli on sen nopeus ja haittana avainten hallinta: salatun viestin välittämistä varten meidän täytyy ensin sopia jaetusta salaisesta avaimesta esimerkiksi tapaamalla kasvokkain. (Ks. symmetrinen salaus)

Julkisen avaimen salauksessa on kaksi avainta. Se perustuu erilaisiin matemaattisiin ongelmiin kuin

salaisen avaimen salaus ja täydentää salaisen avaimen salausta. Julkisen avaimen salauksessa avaintenhallinta helpottuu, mutta haittana on hitaus. (Ks. epäsymmetrinen salaus)
Julkisen avaimen menetelmällä voidaan toteuttaa myös ns. digitaalinen allekirjoitus.

Useat käytännön toteutukset (ns. korkeamman tason protokollat, esim. SSL, IPSec) hyödyntävät molempia menetelmiä eli ovat ns. **hybridejä**. Tällöin epäsymmetrisen salauksen avulla vaihdetaan yhteinen salainen avain jota sitten voidaan käyttää jatkossa.

Kolmas tärkeä elementti kryptografiassa on **eheysfunktio**: kyseessä on ns. yksisuuntainen muunnos, jota voidaan käyttää eheyden varmistamiseen - eli voimme tarkastaa, ettei kukaan ole muuttanut viestiä matkalla. Sitä käytetään myös salasanojen suojaamisessa ja tallentamisessa. Oleellista yksisuuntaisessa salakirjoituksessa on, ettei salattua viestiä tarvitse missään vaiheessa purkaa.

Kryptologia

Kyrptologia voidaan jakaa symmetriseen (salainen jaettu avain; esim. DES, 3DES, IDEA, Blowfish, CAST, AES, RC4) epäsymmetriseen (yhteinen julkinen ja yksityinen salainen avain; RSA, DH (Diffie-Hellman) ja avaimettomiin (tiivisteet, hash; esim. UNIX crypt, MD4, MD5, SHA-1) menetelmiin.

1. Symmetrinen salaus

Perinteisesti salausmenetelmät ovat olleet symmetrisiä, mikä tarkoittaa sitä, että samaa avainta käytetään viestin salaamiseen ja salauksen purkamiseen. Tässä tapauksessa siis vain vastaanottaja, joka tietää salausavaimen pystyy purkamaan viestin salauksen.

Jos samaa avainta käytetään liian pitkään, on mahdollista, että avain joutuu ulkopuolisten tietoon. Tämän vuoksi avain tulisi vaihtaa tarvittavan usein. Symmetrisen salauksen etu on sen nopeus, joten se sopii hyvin suurten datamäärien salaamiseen. Menetelmän haittana on avaintenhallinta.

Symmetrinen salaus on jaettavissa kahteen ryhmään: **jonosalaukseen** ja **lohkosalaukseen**. Jonosalaimissa taas dataa salataan bitti kerrallaan. Lohkosalaimien perusperiaate on salattavan datan jakaminen lohkon mittaisiin palasiin, jotka salataan yksi kerrallaan. Lähes poikkeuksetta kaupallisessa käytössä ja erilaisissa protokollissa olevat algoritmit ovat lohkosalaimia. Avaimen pituus on tyypillisesti esim. 128 bittiä (esim. www-käytössä).

2. Epäsymmetrinen salaus

Järjestelmän kehittäjiä ovat Ronald **R**ivest, Adi **S**hamir ja Leonard **A**dleman. He käyttivät hyväkseen vuonna 1976 Martin Hellmanin ja Whitfield Diffien huomiota, että on mahdollista rakentaa kahteen eri avaimeen perustuva salausmenetelmä. Tätä menetelmää alettiin kutsua RSA -menetelmäksi. Järjestelmä pohjautuu kahteen avaimeen, jotka luodaan yhdessä, mutta niitä käytetään erikseen. Toista avainta käytetään salaukseen ja toista salauksen purkamiseen. RSA -menetelmässä avaimet sidotaan toisiinsa matemaattisesti. RSA-algoritmi löytyy lähes kaikista epäsymmetristä salausta käyttävistä tuotteista.

RSA- menetelmän toinen avain on siis julkinen ja toinen salainen. Julkinen avain voidaan ilmoittaa kenelle tahansa (julkinen avain voi olla saatavissa esim. www-sivuilla), salainen pidetään nimensä mukaan salaisena. Avaimet on sidottu toisiinsa, mutta julkisesta avaimesta ei voida päätellä salaisen avaimen sisältöä. Avainten sisällöt ovat suuria lukuja, jotka muunnetaan käytössä heksadesimaaliluvuiksi tai kirjaimiksi. Epäsymmetrisen salauksen turvallisuus on suorassa suhteessa

avaimen pituuteen.

Salakirjoituksessa käytetään siis salausavaimia eli salausavainpareja, joiden avulla tietojen salaus ja purku voidaan suorittaa. Toimintaperiaate on seuraava:

1. Viestin lähettäjällä on hallussaan vastaanottajan julkinen avain (public key), jonka lähettäjä on saanut joko vastaanottajalta itseltään tai jollakin muulla tavalla.
2. Viestin lähettäjä salakirjoittaa lähetettävän tiedon tällä vastaanottajan julkisella avaimella, jolloin salattua viestiä ei voi kukaan muu kuin julkista avainta vastaavan yksityisen avaimen haltija purkaa.
3. Viestin vastaanottaja purkaa saapuneen tiedon omalla yksityisellä eli salaisella avaimellaan (private key).

Epäsymmetrisen salauksen käyttökohteita mm. salaisten avainten vaihto symmetrisen salauksen alustamiseksi (esim. SSL, SSH) autentikointiin (SSL-sertifikaatit, SSh hostkey) ja digitaalinen allekirjoitus (mm. PGP).

Tosin digitaalinen allekirjoitus toimii päinvastoin: lähettäjä allekirjoittaa viestinsä omalla salaisella avaimella ja vastaanottaja voi julkisen avaimen avulla varmistaa, että viesti on tullut salaisen avaimen käyttäjältä eikä viestin sisältöä ole muutettu.

Symmetrinen vs. epäsymmetrinen salaus:

Symmetrisen avaimen pituus	**Epäsymmetrisen avaimen pituus (RSA)**
64 bit	768 bit
128 bit	1024 bit
168 bit	2048 bit

Symmetrisen ja epäsymmetrisen salauksen avaimenpituuksiin tulee suhtautua varauksella, sillä niitä **ei** juuri voida vertailla, koska algoritmit perustuvat aivan eri asioihin. Mainittakoon että epäsymmetrinen avain on pitempi, koska osa siitä saa paljastua.

Salauksen turvallisuus on suorassa suhteessa avaimen pituuteen (esim. 56 bit salaus on murrettu jo aikoja sitten, mutta 128 bit salauksen murtaminen vie vielä useita kymmeniä vuosia).

3. Tiivisteet

Tiivisteet ovat yksisuuntaisia funktioita, jotka laskevat syötteestä tiivisteitä, joista ei pysty selvittämään alkuperäistä syötettä. Alkuperäisestä syötteestä tulee kuitenkin aina tuloksena sama tiiviste.

Tiivisteitä käytetään tyypillisesti tarkastussummana eheyden tarkistamiseen ja salasanojen tallentamiseen (MD5 passwords).

Digitaalinen allekirjoitus

Julkisen avaimen tärkeä sovellus on sähköinen allekirjoitus, jota käytetään todentamaan tiedon eheys tai lähettäjän aitous. Digitaalisen allekirjoituksen tapauksessa yksityistä, salaista avainta käytetään viestin allekirjoitukseen ja vastaavaa julkista avainta käytetään allekirjoitetun viestin todentamiseen.

Tällä tekniikalla saadaan aikaan luottamuksellisen viestinnän ja sähköisen allekirjoituksen hyödyt avoimessa verkkoympäristössä, jossa viestinnän osapuolet eivät ennestään tunne toisiaan.

Julkisen avaimen teknologia mahdollistaa digitaalisen allekirjoituksen avulla seuraavia asioita:

1) Osapuolten luotettavan tunnistuksen (trusted authentication), jossa käyttäjät voivat tunnistaa luotettavasti itsensä muille verkon käyttäjille ja palvelimille.
2) Tiedon eheyden (data integrity), jossa digitaalisen allekirjoituksen varmentaja voi havaita, onko ko. tietoa muutettu allekirjoituksen jälkeen.
3) Kiistämättömyyden tuen (non-repudiation), joka tarkoittaa sitä, että tiedon allekirjoittajalla ei ole mahdollisuutta myöhemmin enää kiistää jo olemassa olevan tiedon oikeellisuutta ja allekirjoitusta.

Digitaalista allekirjoitusta voidaan pitää tietoturvan keskeisenä palveluna. Sitä tarvitaan kaikkialla tietoyhteiskunnassa käytettäessä verkkojen tietoturvapalveluita henkilöiden tunnistamiseen mm. sähköisessä kaupankäynnissä tai viestinnässä. On kuitenkin huomattava ero omakätisen ja digitaalisen allekirjoituksen välillä, koska omakätinen allekirjoitus todentaa ko. henkilön, digitaalinen allekirjoitus todentaa puolestaan dokumentin oikeellisuuden. Jos lisäksi käytetään henkilösertifikaattia, allekirjoitus varmentaa myös allekirjoituksen tehneen henkilön. Sertifikaatti (varmenne) on varmentajan (CA) myöntämä elektroninen asiakirja jossa todistetaan, että henkilön julkinen avain, sertifikaatin sisältämä muu informaatio ja käyttäjän nimi, vastaavat toisiaan.

Digitaalinen allekirjoitus, kun se on toteutettu modernilla kryptografialla ja se pohjautuu kansainvälisiin hyväksyttyihin standardeihin yhdessä luotettavan kolmannen osapuolen kanssa, on teknisessä mielessä yhtä lainvoimainen kuin omakätinen allekirjoitus. Se soveltuvatko digitaaliseen allekirjoitukseen jo olemassa olevat lait, ei ole yhtä selvää.

PKI (Public Key Infrastructure)

Julkisen avaimen kryptografian käyttö edellyttää sitä, että käyttäjien tulee vakuuttua kommunikoivansa luotettavien osapuolten kanssa. (Julkinen avainhan voi olla esim. www-sivulla). Tämän vuoksi kaikilla PKI:n käyttäjillä tulisi olla oma rekisteröity varmenne. Nämä varmenteet tallennetaan ns. digitaalisena julkisen avaimen sertifikaattina.

Varmenneviranomaiset tai varmentajat (CA, Certificate Authority) ovat henkilöitä, prosesseja ja työkaluja, joiden avulla tehdään digitaalisia sertifikaatteja. Sertifikaateilla tarkoitetaan digitaalisia dokumentteja, joissa yhdistetään käyttäjien (henkilö, sovelluskoodi tai muu yksikäsitteisesti määritelty olio) tunnisteet (nimet) tai muu yksikäsitteinen ominaisuus luotettavasti niiden julkisiin avaimiin.

Luotettavan varmenteen ehdot:

- Varmenteen myöntäjään luotetaan
- Varmenteen myöntäjän yksityisen avaimen on pysyttävä salassa
- Varmenteen myöntäjän julkinen avain on saatu turvallista kanavaa pitkin
- Varmenteessa käytetty salaustekniikka on riittävän turvallista

PKI tarkoittaa siis ns. julkisen avaimen infrastruktuuria. Valmis PKI -standardi on avoimiin X.500 -hakemistostandardeihin kuuluva X.509, joka määrittelee sertifikaatit ja näiden todentamismenettelyt.

Julkisten avainten teknologioiden avulla saavutetaan luottamuksellisuus (confidentiality) ja pääsyn

valvonta (access control). Näin ollen käytettäessä salausta ja siirrettäessä salaisia avaimia turvattomien tietoliikenneyhteyksien välityksellä pyritään riittävään tietoturvan tasoon. Tarkasteltaessa epäsymmetrisen algoritmin avaimen pituuksia, turvallisena pituutena voidaan pitää yli 1024-bitin avaimia. Riittävä avaimenpituus riippuu kuitenkin algoritmista.

PKI - järjestelmää käytetään hyväksi julkiseen avaimeen perustuvaan salaukseen, digitaaliseen allekirjoitukseen ja avainten hallintaan. Myös ns. looginen yritysverkko VPN (=Virtual Private Network) käyttää hyväkseen PKI - järjestelmää. PKI -palvelussa jakelu, hallinnointi ja ylläpito, joka sisältää avainten hallinnan, on koko toiminnan perusta. PKI:n tärkein ominaisuus onkin transparenttisuus eli läpinäkyvyys, jolloin käyttäjän ei tarvitse ymmärtää, miten PKI käyttää avaimia ja sertifikaatteja.

PKI - palvelujen merkitys tulee kasvamaan siirryttäessä yhä enemmän elektroniseen kaupankäyntiin ja muihin verkoissa tapahtuviin tietoyhteiskunnan sovelluksiin. Edellytyksenä on, että palveluihin tulee pystyä luottamaan ja niiden käytön pitää olla mahdollisimman vaivatonta.

Sertifiointi liittyy keskeisesti organisaation tietoturvaan. Suomessa tietoturvan varmennetoiminta on ollut sidoksissa eri viranomaisiin. Sertifioinnin tarkoituksena on herättää yhteistyökumppaneissa luottamusta.

PGP (Pretty Goog Privacy)

PGP (Pretty Good Privacy) on yleisin Internetissä käytetty ohjelmisto, jolla pyritään turvaamaan mm. sähköpostiliikennettä. PGP käyttää hyväkseen julkisen avaimen ja symmetrisen avaimen menetelmiin perustuvaa tekniikkaa sisältäen datan luotettavuuden ja digitaalisen allekirjoituksen. Sen kehittäjänä on tunnettu Philip Zimmermann.

PGP:llä on *oma ns. sertifikaattikonsepti*, missä otetaan ensiksi PGP:n julkinen avain, jolle lasketaan allekirjoitus käyttämällä toista salaista avainta, jonka jälkeen allekirjoitus liitetään alkuperäiseen julkiseen avaimeen.

PGP ei käytä erillistä varmennepalvelua (vrt. PKI) ja sen sertifikaattimallia kutsutaan suoraksi luottamukseksi tai *luottamusverkostoksi* (web of trusts) (vrt. varmentajan myöntämä sertifikaatti, jolloin luotettava kolmas osapuoli (CA) varmentaa erillisellä sertifikaatilla henkilön ja hänen julkisen avaimen välisen yhteyden).

PGP:ssä hallitaan sertifikaatteja manuaalisesti, joten jokaisen PGP -käyttäjän tulee pitää itse huolta muiden käyttäjien julkisista avaimista tallentamalla ne ns. avainrenkaaseen (key ring). PGP:ssä käytettävien avainten hallinta perustuu näihin avainrenkaisiin, joihin käyttäjä voi halutessaan tallentaa ne julkiset avaimet, joihin hän luottaa. PGP ei siis käytä hyväkseen keskitettyä sertifiointiosapuolta.

PGP:n perustana ovat seuraavat tietoturvapalvelut: autentikointi, jossa hyödynnetään digitaalista allekirjoitusta ja yksityisyyden suoja, jossa käytetään kryptausta.

Julkisen avaimen salaus ei pysty poistamaan avaintenhallintaan liittyviä ongelmia. Vaarana on niin sanottu välimieshyökkäys (Man-in-the-middle). Sillä tarkoitetaan hyökkäystä, jossa verkossa julkisia avaimia vaihtamalla kolmas osapuoli pääsee seuraamaan keskustelua. Avainten vaihdossa hyökkääjä korvaa pyydetyn julkisen avaimen omalla avaimellaan.

Vaikka PGP on saavuttanut eräänlaisen defacto -standardin mukaisen statuksen, sen käytettävissä

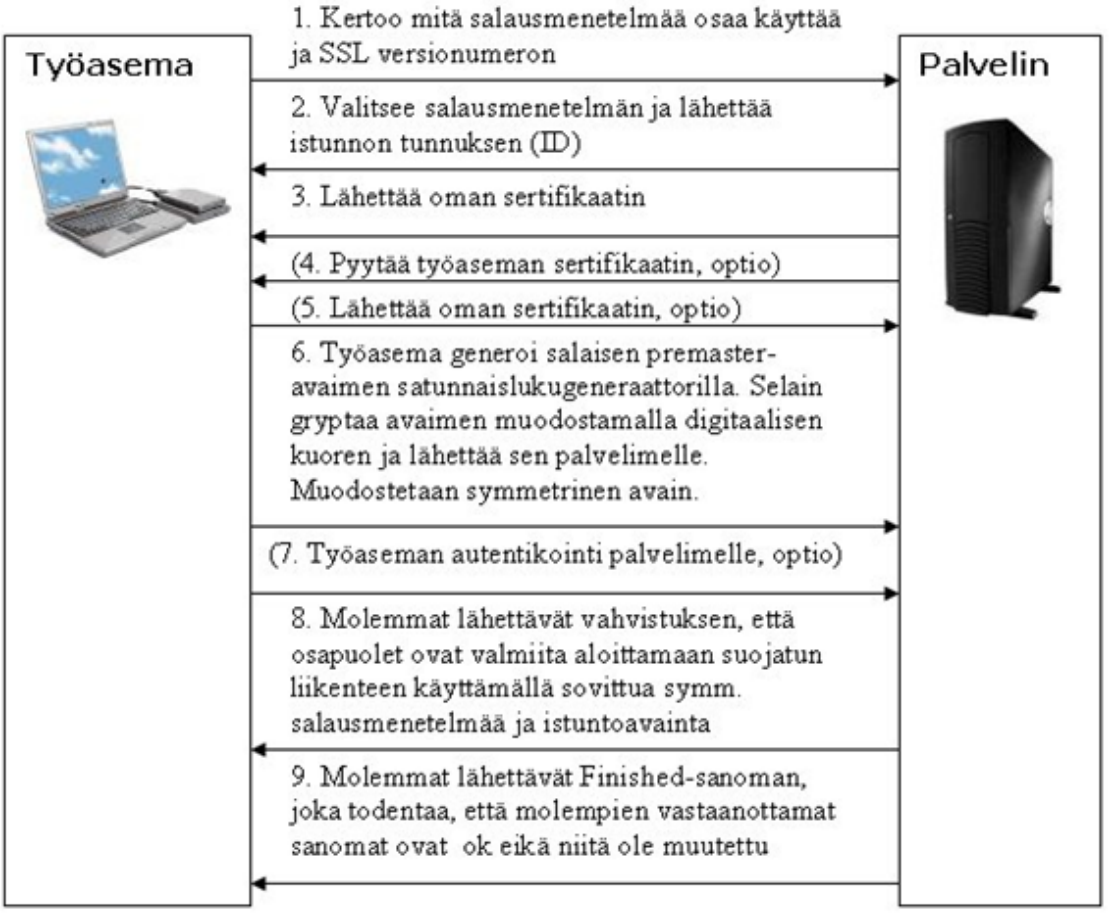
oleva luotettavien käyttäjien verkosto ei ole riittävä esimerkiksi ammattimaisen sähköpostin tarpeisiin. PGP:n avulla organisaatiot eivät voi luoda kattavaa luotettavien käyttäjien verkostoa, koska sen toiminta perustuu yksittäisten henkilöiden luottamuspäätöksiin, jolloin väärinkäytösten riskit ovat suuria. PGP-malliin ei voi sisällyttää vastuuta tai toteuttaa sellaisia järjestelmiä, joilla voitaisiin ratkaista kiistatilanteita.

Verkkotason tietoturva

SSL (Secure Sockets Layer)

SSL on Netscapen kehittämä Internetin TCP- eli kuljetustason protokollan päälle tehty symmetrinen salausprotokolla, jonka tarkoitus on salata tunnistus käyttäjän ja palvelimen välillä, tunnistaa palvelin sekä neuvotella liikenteessä käytettävä salaus. SSL- käyttää varmenteita eli sertifikaatteja.

SSL-yhteyden avaaminen eli kättely:



Tämän jälkeen sekä työasema ja palvelin luovat premaster-avaimesta istuntoavaimen (master-avain) salatakseen tulevan liikenteen symmetrisesti molempiin suuntiin.

SSL-protokollaa voidaan käyttää esim. seuraavilla protokollilla: HTTPS (salattu HTTP-protokolla, www-selaus), SSMTP (salattu SMTP-protokolla, sähköposti), NNTPS (salattu NNTP-protokolla, uutisryhmät) FTPS-protogolla (salattu FTP-protokolla, tiedostojen siirto) ja Telnets (salattu Telnet-protokolla, pääteyhteys).

SSL tarjoaa luottamuksellisuuden (salaisen avaimen määrittämiseksi tarvittavan kättelyn jälkeen kaikki siirrettävät tiedot salakirjoitetaan), autentisoinnin eli todentamisen (palvelin tunnistetaan aina, käyttäjän tunnistaminen niin haluttaessa) ja eheyden (viestiä ei ole muutettu).

SSL on nykyisin yleisin esim. pankkipääteyhteyksien suojausmenetelmänä. Käytännössä salaus on hyvin turvallinen. Sen murtamiseen kokeilemalla kuluu useita vuorokausia, vaikka käytössä olisi kymmeniä huipputehokkaita koneita. Eikä murron tuloksena saatavasta avaimesta ole krakkereille mitään iloa, sillä avain on istuntokohtainen ja voimassa vain niin kauan kuin pankkiyhteys on käytössä.

Käyttäjä ei koskaan edes näe omaa istuntokohtaista avaintaan. Lisäksi pankkipalveluissa käytetään kertakäyttöisiä tunnuslukuja, mikä entisestään vaikeuttaa murtautujan työtä.

SSH (Secure Shell)

Suomalaista alkuperää oleva SSH on pääte-yhteyksille tarkoitettu salausprotokolla, mutta sen kautta voidaan tunneloida myös mikä tahansa muukin yhteys. SSH:lla voidaan siirtää esim. tiedostoja työasemasta palvelimeen ja päinvastoin. SSH toimii omana ohjelmanaan sekä työasemassa että palvelimessa. SSH-protokolla toimii sovelluskerroksessa TCP-protokolla päällä.

SSH-protokollan tarkoituksena on korvata mm. turvattomat FTP ja Telnet. SSH:ssa käyttäjätunnistus voidaan tehdä kolmella tavalla: ensinnäkin käyttäjätunnuksen ja salasanan avulla, toiseksi käyttäjätunnuksen ja julkisen avaimen avulla ja kolmanneksi käyttäjätunnuksen ja työaseman perusteella.

IPSec (IP Security)

IPSec on salausprotokolla, joka on myös rakennettu suoraan IP:n päälle ja tarjoaa lähtöpisteestä määränpäähän ulottuvaan salaukseen pohjautuvan suojauksen sekä IPv4:lle että IPv6:lle. Koska IPsec on toteutettu IP-kerrokseen, se pystyy suojaamaan kaikkia IP-protokollia mukaan lukien TCP:n ja UDP:n.

Sen tarjoamat palvelut ovat:

- Viestien eheyden varmistamisen
- Viestien lähettäjän varmistamisen
- Viestien toistamisen estämisen
- Viestien salakirjoittamisen

IPSec:iä käytettäessä voidaan valita kaksi toimintatapaa: kuljetusmoodi tai tunnelimoodi. IPSec-suojaus on transparenttia eikä näy sovelluksille.

Murtautumiset salausalgoritmeja vastaan

Hyvän salausalgoritmin ominaisuuksiin kuuluu, että salattua tekstiä ei voida tulkita muulla kuin oikealla avaimella tai kokeilemalla kaikkia mahdollisia avaimia (brute force -menetelmä). Avainta ei pidä saada selville vaikka hallussa olisi salattuja viestejä ja niitä vastaavia selväkielisiä viestejä. Salausmenetelmän tulee aina olla julkinen ja avaimen salainen. Salaus perustuu avaimen pituuteen eli lyhyttä avainta käyttävät salausmenetelmä on aina turvaton. Pitkää avainta käyttävä menetelmä saattaa olla turvallinen.

Vanha salausmenetelmä, jonka heikkoudet ovat tiedossa, on turvallisempi kuin uusi menetelmä, jota ei ole vielä analysoitu tarpeeksi. Ajan kuluessa nähdään kuinka turvalliseksi uusi menetelmä osoittautuu.

Murtautumistyyppejä on useita. Periaatteessa siis mitä enemmän murtautuja tuntee salasanomaa ja mahdollisesti sitä vastaavaa selväkielistä tekstiä ja tuntee käytetyn algoritmin ja mahdollisesti löytää käytetyn avaimen sitä helpompi hänen on murtaa salatekstit.

Kuinka sitten voidaan löytää vertailukelpoisia selväkielisiä ja salakielisiä tekstejä? Esim. yleiset tiedostoformaatit, kuten Word ja Excel, alkavat aina samantyyppisellä johdannolla. Ellei hyökkääjällä ole käytössään juuri salatun tiedoston alkuperäistä versiota, hän voi luoda itse vastaavan tyyppisen tiedoston ja vertailla sen alkua salattuun versioon.

Lisäksi monia muita murtautumistekniikoita ja mm. ns. raa'an voiman käyttö, jolloin murtautuja käyttää uhkailua, kiristystä ja lahjontaa salausavaimen selvittämiseen. Se on käytännössä lähinnä vitsi, mutta kaikista halvin, nopein ja yksinkertaisin tapa päästä selville hyvän algoritmin suojaamista salaisuuksista.

Algoritmin tulee olla varma kaikkia murtautumistekniikoita vastaan. Salausavaimen pituudella voidaan vaikuttaa siihen, ettei esim. brute force -menetelmän käyttö ole järkevää (vie liian kauan aikaa). Kaikki salaukset ovat kuitenkin murrettavissa. Kyse on vain siitä paljonko on käytettävissä aikaa ja tietokonetehoa.

OECD:n suositukset kryptografiajärjestelmille

OECD-järjestö on toiminut jo pitkään aktiivisesti yksityisyyden, tietosuojan ja tietoturvanedistämisen alueilla. Järjestön kiinnostuksen kohteena on viime aikoina ollut erityisesti sähköinen kaupankäynti. Se pyrkii edistämään yhteisymmärrystä tieto- ja viestiverkkoja ja -tekniikoita koskevissa sääntelykysymyksissä, kuten esimerkiksi salakirjoitukseen liittyvissä asioissa. Pyrkimyksenä on kätkeä tiedon sisältö, varmistaa tiedon aitous, estää sen muuttaminen ja estää tiedon asiaton käyttö. Tämä tekniikka on välttämätön niin kansallisten kuin maailmanlaajuisten tietoverkkojen sekä verkkokaupan kehitykselle.

Kryptografiaohjeet muodostuvat kahdeksasta perusperiaatteesta, joita ovat:

- Kryptografisten menetelmien tulee olla uskottavia
- Käyttäjällä tulee olla oikeus valita, mitä menetelmää hän käyttää
- Kryptografisia menetelmiä tulee kehittää yksityisten henkilöiden, yritysten ja hallintojen tarpeisiin
- Menetelmissä käytettäviä standardeja, kriteerejä ja protokollia tulee kehittää kansallisella ja kansainvälisellä tasolla
- Kryptografiapolitiikassa tulee kunnioittaa yksityisen henkilön perusoikeuksia yksilönsuojaan
- Kansalliset kryptografiapolitiikat voivat sallia luvallisen pääsyn selväkieliseen tekstiin tai avaimiin ja salattuun sanomaan. Kansallisten käytäntöjen tulee ottaa näiden ohjeiden muut periaatteet huomioon
- Kryptografisia palveluja tarjoavien tai kryptografisia avaimia hallussaan pitävien yksilöiden tai elinten vastuut tulee ilmoittaa selvästi
- Eri maiden hallintojen tulee yhdessä koordinoida kryptografiapolitiikkaa ja poistaa tai välttää kryptografian nimissä luomasta epäoikeudenmukaisia kaupan esteitä

Edellä olevat suositukset on tarkoitettu pääasiassa eri maiden hallinnolle, mutta niitä odotetaan noudatettavan myös julkisella ja yksityisellä sektorilla.

4.8 Varmentaminen

Tiedostojen, erityisesti työtiedostojen, varmentaminen (backup) on yksi tärkeimmistä tietoturvarutiineista. Työskentelyn perusrutiineihin tulisi kuulua ensinnäkin välitallennukset, koska ohjelman käyttö saattaa päättyä virhetoimintoon eli ohjelma ns. kaatuu. Samoin koko järjestelmä saattaa kaatua, voi tulla sähkökatkos tai teet vahingossa tietoihin sellaisen ison muutoksen, joka ei ole ohjelman käskyllä peruutettavissa. Vahinko voi tulla monessa muodossa: vesivahinko, kovalevyn rikkoontuminen, varkaus, tai vain vahingossa tehty tiedoston poistaminen. Aiemmin varmuuskopioinnissa (backup) pääpaino on ollut varautumisessa tietokoneen tekniseen vikaan tai käyttäjän inhimilliseen erehdykseen. Nykyisin edellisten lisäksi on tullut merkittäväksi toipuminen virusten ja muiden haittaohjelmien aiheuttamista tuhoista.

Tietojen katoaminen ei välttämättä aina ole lopullista, mutta yksittäistenkin tietojen kuten esim. lomaketietojen tai CV:n kirjoittaminen uudestaan on vaivalloista ja aikaa vievää. Kotona tärkeistä työtiedostoista on hyvä ottaa versioita kovalevylle, mutta jos kovalevy rikkoontuu, niistä ei ole mitään hyötyä. Siksi erillisen varmuuskopion säännöllinen ottaminen erilliselle laitteelle voi säästää huomattavasti työtunteja. Kannattaa myös muistaa, että vakuutusyhtiöt eivät korvaa menetetyn tiedon arvoa.

Kopion voi ottaa suoraan kopioimalla yksittäisistä tiedostoista tai kansioista. Omaa työtä helpottaakseen kannattaakin tallentaa kaikki työtiedostot jokin tietyn kansiorakenteen alle, esim. 'Omat tiedostot' (My Documents). On huomattavasti helpompaa etsiä tiedostoja asiakohtaisista kansioista kuin epäselvistä tiedostoluetteloista. Tiedostojen nimeämiseenkin kannattaa kiinnittää huomiota: tiedostonimi "Hiihtomatkan 2012 ilmoittautumislomake" on huomattavasti kuvaavampi kuin pelkkä ilmoittautumislomake. Hyödyn huomaa varsinkin silloin, kun lähes samannimisiä tiedostoja on kertynyt useita kymmeniä.

Varsinainen varmistaminen tarkoittaa kopion ottamista kovalevystä erilliselle laitteelle, kuten esim. muistitikulle, CD:lle, DVD:lle tai jos käytössäsi on kaksi kiintolevyä, voi toiselle (ulkoiselle) kiintolevylle tehdä varmuuskopioita. Yrityskäytössä jossa yleensä on käytössä suurempia tietomassoja kuin kotikoneella, varmistukset otetaan usein erilaisille nauhoille ja varmuuskopio muuttuneista tiedoista tulee ottaa päivittäin. Pk-yrittäjille on tarjolla myös varmuuskopiopalvelua, joissa tiedot tallennetaan palvelua tarjoavan yrityksen tietokoneille Internetin kautta.

Voit myös käyttää Windowsin varmuuskopiointiohjelmaa. Windows7:ssa varmuuskopioinnin työvälineet löytyvät Control Panel | System and Security tai avaamalla toimintokeskuksen (Action Center) työpöydältä Tehtäväpalkista olevasta lippu-kuvakkeesta. Oletuksena varmuuskopiointiohjelma ei ole aktiivinen, mutta voit halutessasi ajastaa varmuuskopioinnin säännöllisesti tapahtuvaksi.

Ajastetun varmistuksen ohella voit tehdä tietokoneesta myös erikseen levykuva -tyyppisen (image) varmuuskopion, jolla voit palauttaa koko tietokoneen käyttöjärjestelmän ohjelmistoineen (Palautuksen lisämenetelmät = Advanced recovery methods). Ongelmatilanteissa (esim. päivitysten, asetusten muuttamisen jälkeen) kannattaa kuitenkin kokeilla ensin järjestelmän palauttamista aiempaan ajankohtaan (Järjestelmän palauttaminen = System Restore).

Oleellista varmuuskopioinnissa on myös testata, ovatko tiedostot todella tallentuneet ja pystytäänkö ne palauttamaan.

4.9 Windows 7 suojaus

Käyttöjärjestelmäversioiden uudistuessa on tietoturvallisuus otettu huomioon yhä enenevässä määrin. Uusimmissa Windows-versioissa on mukana mm. virustorjunta ja palomuuri. Se onkin aiheellista, koska juuri Windowsia vastaan on eniten haittaohjelmia ja muita hyökkäyksiä.

Windows 7 -käyttöjärjestelmän ylläpitämiseksi ja suojaamiseksi on valmiina käyttöjärjestelmän mukana tai ladattavissa ilmaiseksi netistä mm. seuraavia ohjelmia:

- Windows palomuuri ja Defender tai Security Essentials (ilmainen) –virustorjuntaohjelma. Microsoft kerää Defenderin avulla tietoja Microsoft Security Intelligence Report (SIR) -raporttia varten. Löydät uusimman raportin osoitteesta http://www.microsoft.com/sir

- Haittaohjelmien poistaminen - MSRT. Ei tule win7:n mukana, mutta on ladattavissa osoitteesta http://www.microsoft.com/security/malwareremove/default.aspx. Huomaa että MSRT ei korvaa virustorjuntaohjelmaa.
- CCleaner, käytön jälkien siivomainen ja levytilan vapauttamien. Ladattavissa valmistajan sivuilta http://ccleaner.com (HUOM. Kun asennat ohjelmaa, kannattaa ottaa rasti pois kohdasta ”Asenna CCleaner Yahoo!” -työkalupalkkiin)
- Eraser, tiedostojen tietoturvallinen poistaminen ladattavissa esim. osoitteesta http://eraser.heidi.ie/index.php#download
- Secunia PSI, sovellusten tietoturvallisuuden tarkastaminen löytyy esim. osoitteesta http://secunia.com/vulnerability_scanning/personal/
- Selaimen suojaus IE:ssa: Suojaus | InPrivate-selaus on merkityksellinen yksityisyyden suojauksen kannalta. Kannattaa käyttää yhteiskäytössä olevilla koneilla. Otettava erikseen käyttöön (Safety | InPrivate Browsing tai näppäinyhdistelmällä Ctrl+vaihto+P).
- IE:n SmartScreen-suodatus (varoittaa haitallisista www-sivuista) ja XSS-suodatukset (pyritään estämään tietokoneesi ja tietojesi väärinkäyttö) ovat merkityksellisiä tietoturvan kannalta. Otettava erikseen käyttöön (Safety | InPrivate Filtering, valitse asetus Block for me eli Estä)
- Windows Update. Esimerkiksi Microsoftin tietoturva- ja muut ohjelmapäivitykset, laiteohjelmapäivitykset, Service Pack -huoltokorjaukset ja päivitykset mm. Office-ohjelmia varten. Kaikki kriittiset päivitykset tulee asentaa heti kun niitä on saatavissa. Tarkista haulla **Win: upd** tai valitse sivupalkista Tarkista päivitysten saatavuus (Check for updates).
- Organisaatioissa kannattaa käyttää ilmaista Windows Softare Update Services (WSUS) palvelinohjelmistoa. Lisätietoja osoitteesta http://technet.microsoft.com/en-us/wsus/default.aspx
- Levyn eheyttäminen (Defrag, Disk Defragmenter)
- BitLocker (salakirjoitusohjelma Windows7 Enterprise- ja Ultimate-versioissa)
- Järjestelmän palautus -apuohjelma (system restore)
- Varmuuskopiointi esim. ulkoiselle muistille (kuten ulkoiselle kiintolevylle), joka voidaan ajastaa automaattiseksi.

Huomio!

Paraskaan turvaohjelma ei suojaa holtittomalta nettikäyttäytymiseltä tai muuten vastuuttomalta koneen käytöltä. Siksi aina on käytettävä torjuntaohjelmia. Virustorjunta- ja haittaohjelmien poisto-ohjelmia on lukuisia, joten valinnassa on varaa. Pelkkään Defender-ohjelmaan ei tule luottaa.

Perussääntö on, että vain yksi palomuuri ja virustorjuntaohjelma käytössä yhtä aikaa. Eli jos asennat toisen palomuurin ja virustorjunta -ohjelman, poista Windowsin omat ohjelmat aktiivisesta käytöstä.

Muistilista

1. Tarkista, että tietokoneen käyttöjärjestelmä on ajan tasalla.
2. Varmista, että virustorjunta ja palomuuri toimivat
3. Muista ottaa varmuuskopiot
4. Tarkista, että varmuuskopiointi on onnistunut
5. Testaa onnistuuko tietojen palautus tietokoneelle
6. Sijoita varmuuskopiot eri paikkaan kuin tietokone, mieluummin paloturvalliseen kaappiin

5 Lähteitä

Anon., 1999. Results of the Distributed-System Intruder Tools Workshop. Pittsburgh , Pennsylvania USA , November 2-4, 1999 . CERT ® Coordination Center, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213, December 7, 1999.

Boström Mika 2003. Kotimikron tietoturva

BS 7799-1:fi. Standardi. -Tietoturvallisuuden hallinta. Osa 1: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje. Suomen standardisoimisliitto SFS, 15.2.1999. (Käännös alkuperäisestä standardista BS 7799, 1995)

BS 7799-2:fi. Standardi. -Tietoturvallisuuden hallinta. Osa 2: Tietoturvallisuuden hallintajärjestelmiä koskeva menettelyohje. Suomen standardisoimisliitto SFS, 15.2.1999. (Käännös alkuperäisestä standardista BS 7799, 1995)

Freeman Edward H. 2000. State Control of Unsolicited E-mail: State of Washington v. Heckel. Auerbach, Information Systems Security. Vol. 9, no. 3., 12-16.

Hakala, Mika Vainio, Mika Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. Docendo

Hedemalm Gunvald, 2000. Tietoverkon perusteet

ISO-IECJTC1-SC27,1995. Guidelines for the Management of IT Security.

Järvinen, P. 2010. Yksityisyys. Turvaa digitaalinen kotirauhasi. Jyväskylä: Docendo

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo.

Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen

Kajava Jorma. Tietoturva - perusluonne ja tasot

Kerttula, E. 2000. Tietoverkkojen tietoturva: tarpeet ja teknologiat, internet-tietoturva, suljettujen IP-verkkojen tietoturva, julkisen avaimen infrastruktuuri.

Kiviniemi Pekka, 2000. Oikeutetusta puuttumisesta luottamukselliseen viestiin, Sähköposti ja muut viestit. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja, Rikos- ja prosessioikeuden julkaisusarja B:18, ISBN 951-29-1834-X.

Korpela, Jukka 2005. Turvallisesti netissä: kodin tietoturvaopas

Rahnasto, I. 2002. Internet-oikeuden perusteet. Helsinki: Kauppakaari.

Ruohonen, Mika. 2002. Tietoturva. Jyväskylä: Docendo.

Saarenpää Ahti. 2008. Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan. Lapin yliopisto. Oikeusinformatiikan instituutti.

Thomas, Tom. 2005. Verkkojen tietoturva - perusteet. Edita Publishing Oy

Valtiovarainministeriö: Valtion tietohallinnon Internet-tietoturvallisuusohje, Vahti 1/2003 [verkkodokumentti/online]. Helsinki: Valtiovarainministeriö, 2003 Saatavissa: http://www.vm.fi/tiedostot/pdf/fi/39681.pdf

Vanto, Jarno J. 2011. Henkilötietolaki käytännössä