

TEKSTI: KIMMO ROUSKU
PIIROS: ERIC LERAILLEZ



1/6

Tietoturva
ja tietosuojaa

Kuusiosainen artikkelisarja opastaa sekä yksityis- että yrityskäyttäjää tietoturvan ja tietosuojan sokkeloissa.

Sarjan ensimmäisessä osassa pohditaan tietoturvarikkojen syitä ja tarkistetaan, mihin laki velvoittaa.

Jokainen tarvitsee TIETOTURVAA

Tietoturva- ja tietosuojakäsitteet menevät usein sekaisin. Vaikka ne sivuavat toisiinsa, niillä on merkitysero.

Tietoturvalla yleisesti tarkoitetaan asiointilaa, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuus, eheys ja käytettävyyt eivät ole merkittävästi uhattuina. Sillä tarkoitetaan myös keinoja ja toimenpiteitä, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissa.

Vastaavasti tietosuojalla tarkoitetaan tietojen valtuudettomien saannin estämistä ja tietojen luottamuksellisuuden säilyttämistä. Pääpaino on henkilötietojen suojaamisessa valtuudettomalta tai henkilöä vahingoittavalta käytöltä.

Tietoturva on paljolti tekniikkaa, siis laitteita ja ohjelmistoja, joilla voidaan saada aikaan riittävä tietosuojaa. Tietoturva liittyy teknologiaan, kun taas tietosuojaa liittyy aineistoon, yksilöön ja tietojärjestelmien sisältöön.

TIETOTURVAN PERUSPILARIT

Tietoturvasta puhuttaessa nostetaan yleensä esiin kolme keskeistä seikkaa: eheys, luottamuksellisuus ja käytettävyyt. Eheyden osalta pohditaan, miten voidaan varmistaa, että tieto on varmasti oikea, se säilyy muuttumattomana ja esimerkiksi tiedon siirrossa tiedon sisältöä ei päästä väärentämään. Esimerkiksi tavallisessa sähköpostissa viestin eheyttä ei pystytä varmistamaan, koska esimerkiksi digitaalinen allekirjoitus ja salaaminen vaativat erillisiä ohjelmistoja.

Tiedon luottamuksellisuu-
della viitataan tietoaineiston suojaukseen ja säilytykseen tietoluokittelun edellyttämällä tavalla, jolloin sitä pääsevät käsittelemään vain ne henkilöt, joilla on siihen oikeus. Tärkeä termi tässä yhteydessä on tietoaineistojen luokittelu: kaikki tieto pitäisi pystyä jaottelemaan julkiseen, siis kenen tahansa käyttöön tarkoitettuun, ja luottamukselliseen eli vain tietyn käyttöoikeustason omaaville tarkoitettuun.

Muun muassa valtionhallinnossa joudutaan hyvin tarkkaan valvomaan sitä, mikä on kaikille kansalaisille jaeltavissa

Tietoturvasivusto

www.mikropc.net/tietoturva

Sivuilla on muun muassa kattava [linkkikokoelma](#). Sivusto karttuu artikkelisarjan edetessä.

olevaa tietoa ja vastaavasti mikä on luottamuksellista tietoa.

Käytettävyydellä tarkoitetaan sitä, että esimerkiksi tietojärjestelmä on käytettävissä siten kuin on sovittu. Joidenkin tietojärjestelmien kohdalla tämä tarkoittaa esimerkiksi normaalia työaika klo 8.00–17.00 arkipäivinä, ja osalle järjestelmistä tämä tarkoittaa 24/7-tasoa, jonka mukaan järjestelmän pitää olla käytettävissä aina.

Näiden kolmen termin ohella tietojärjestelmiin liitetään vielä ajantasaisuus: kuinka ajantasaisia tietojärjestelmässä säilytettävien tietojen tulee olla. On selvää, että esimerkiksi pankkien tietojärjestelmien ajantasaisuuden tulee olla eri tasolla kuin vaikkapa jonkin yhdistyksen

TURVAA VAI SUOJAA

Tietoturva

- Tietojen
- luottamuksellisuus: Ovatko käyttöoikeusrajoitukset kunnossa?
 - eheys: Onko tieto säilynyt muuttumattomana?
 - saatavuus: Pysyykö järjestelmä toimintakunnossa ja tieto tallessa?

Tekniset näkökohdat painottuvat. "Turvassa tuholta"

Tietosuojaa

- Tietojen luottamuksellinen säilyttäminen.
- Tietojen valtuudeton käyttö estetään.
- Henkilötiedot suojataan väärältä käytöltä.

Pääpaino on tietosisällössä. "Suojassa sivullisilta"

jäsenrekisterin.

TIETOTURVA JA -SUOJA KOSKETTAVAT JOKAISTA

Miltä tuntuisi, jos kirpputorilta voisi ostaa rompun, josta löytyy teleoperaattorin kaikkien asiakkaiden nimet, henkilönumerukset, puhelinnumerot, osoitetiedot ja laskutustiedot parilta vuodelta?

Uutisissa kerrottiin hiljattain, kuinka Venäjällä paikallisen teleoperaattorin vastaavat tiedot olivat vuotaneet katukauppaan kenen tahansa saataville.

Tietoturva ja -suoja eivät

ole tärkeitä asioita siksi, että lait ja asetukset niistä määräävät, vaan siksi, että ne koskettavat meitä kaikkia yksilöinä, tietojärjestelmien käyttäjinä tai ylläpitäjinä.

Yrityksille ja viranomaisille tietoturva ja -suoja, "titus" on yksi olemassaolemisen perusta, sillä useimmat yritykset ovat sekä asiakkaita että palveluntarjoajia. Kannattaakin pohtia, millaisen kuvan asiakkaat saavat yrityksestä, jonka asiakastiedot ovat vuotaneet nettiin jonkin -- yleensä etukäteen torjuttavissa olleen -- tietoturvaloukkauksen seurauksena.



Tietosuoja -valtuutetun toimiston sivuilla on paljon hyödyllistä tietoa suomeksi.

www.tietosuoja.fi



MITÄ SINUSTA TIEDETÄÄN?

Rekisterinpitäjät ovat velvollisia kertomaan, mitä tietoja si eri rekistereissä on.

- Kaupakettujen kanta-asiakasrekisterit
- Kirjaston lainarekisteri
- Pankki, jonka kautta hoidat maksut
- jne.

Yritys, jonka tietoturva- ja politiikka on moitteeton ja jonka ohjeistus ja muut toiminnot näiden asioiden kunnioitusta ja valvontaa, antaa myös asiakkailleen luotettavan kuvan toiminnastaan.

KETKÄ KRAKKEROIVAT JA MIKSI?

Jos kaikkien maailman ihmisten etiikka- ja moraalikäsitteet olisivat kunnossa, ei palomureja, salasanoja ja virustentorjuntaohjelmia lainkaan tarvittaisi. Ketkä sitten syyllistyvät tietomurtoihin ja miksi?

Murtautujat voidaan oman kokemukseni mukaan jakaa neljään eri kategoriaan:

- satunnainen "vahingosamurtautuja", usein firman oma työntekijä
- innokas kotiharrastelija eli nörtti
- kehittyneempi script kiddie
- ammattikrakeri.

Satunnainen murtautuja on käyttäjä, joka vahingossa pääsee tietojärjestelmään, johon hänellä ei ole käyttöoikeutta. Syy saattaa olla esimerkiksi väärin määritetyissä käyttöoikeuksissa. Tavallaan tilaisuus tekee varkaan.

Innokkaat nörtit saattavat uteliaina kokeilla jotain netistä löytämäänsä ohjelmaa tai ohjetta tietämättä kokeilunsa vaikutuksia. Liika into ja niukka osaaminen voivat tuottaa vahinkoa.

Script kiddies, "skriptikakarit" lähestyvät oikeita tietomurtautujia siinä mielessä, että he pyrkivät järjestelmällisemmin hyödyntämään netissä olevaa tietoutta jonkin kohteen murtaamiseen.

Ammattikrakerit tai -ryhmittymät ovat kaikkein huolestuttavin kategoria, koska heillä on yleensä käytössä myös riittävät kontaktipinnat lisätiedon ja ohjelmien saamiseksi, jos kohteen suojaus ei aikaisemmin opituilla keinoilla murrukaan.

MIKÄ ON ERI RYHMIEN MOTIIVI?

Usein murtautujan motiivi voidaan luokitella tiedon jankoksi tai omien taitojen esittelyksi. Luultavasti vain murto-osa tietomurtautujista saa taloudellista hyötyä touhuistaan, poikkeuksena tietysti teollisuusvakoilu ja valtiollisen krakeroiminen tai vakoi-lu.

Valtiollisen krakeroimisen tavoitteena on tietojen kerääminen jonkin valtion tieduste-

Malli

Rekisteriseloste

Henkilötietolaki (523/99) 10§ Laadittu: 14.02.2003 Kimmo Anka

1. Rekisterinpitäjä:

Nimi: Roope Anka Oyj, LY: 1313999-1
Yhteystiedot: PL 13130, 13001 Ankkalinn, puhelin (013)13001

2. Rekisteriasioista vastaava henkilö:

Nimi: Tietohallintopäällikkö lines Anka
Yhteystiedot: Kuten kohdassa 1.

3. Rekisterin nimi: Roope Anka Oyj sähköpostin käyttäjähakemisto

4. Rekisterin käyttötarkoitus:

Hakemisto sisältää kaikki yrityksen sähköpostikäyttäjät ja samalla yrityksen lähiverkon käyttöoikeuden omaavat käyttäjät.

5. Rekisterin tietosisältö:

Hakemistoon tallennetaan käyttäjän etunimi, sukunimi, sähköpostiosoite, puhelinnumerot, kirjautumisnimi, salasana sekä käyttäjäryhmät.

6. Säännönmukaiset lähteet:

Tiedot saadaan suoraan työntekijältä.

7. Säännönmukaiset tietojen luovutukset ja tietojen siirto EU:n tai Euroopan talousalueen ulkopuolelle:

Tietoja ei luovuteta Roope Anka Oyj:n ulkopuolelle.

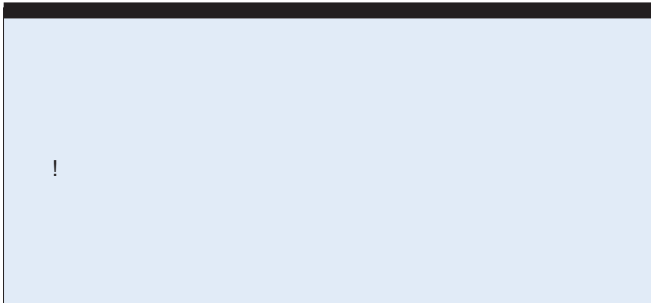
8. Rekisterin suojauksen periaatteet:

Manuaalinen aineisto: Ei synny.
Elektroninen aineisto: Noudatetaan Roope Anka Oyj:n tietoturvaohjeistoa.

9. Tarkastusoikeus:

Hakijalla on henkilötietolain 26 §:n mukaan oikeus tarkastaa, mitä häntä koskevia tietoja on tallennettu hakemistoon. Tarkastuspyyntö lähetetään kohdassa 2 mainitulle henkilölle kirjallisesti ja omakätisesti allekirjoitettuna.

Sen sijaan haktivistit saattavat syyllistyä rikokseen kohdistamalla palvelunestohyökkäysten kaltaisia toimia kohteensa www-sivustolle tai sähköpostipalvelimelle.



lupalvelulle sekä valtion kaupallisten etujen valvominen ja parantaminen salakirjoitusteknologioita kehittämällä ja niitä purkamalla.

Usein käytetty sana "hakkeri" ei oikeastaan tarkoita tietoturmutautujaa. Hakkeri on omalla toiminnallaan luonut ja innovoinut uusia tietotekniikan käyttömahdollisuuksia. Hakkerit ja alan gurut ovat siis "hyviä voimia", jos edellisessä luettelossa olevat edustavat "pahoja voimia".

Viime vuosien aikana esillä ovat olleet myös verkkoaktivistit ja verkkohaktivistit. Aktivistit ovat ryhmittymiä, jotka käyttävät internetin tarjoamia mahdollisuuksia toiminnassaan ja vaikuttavat keinoilla, jotka ovat vielä lain mukaan sallittuja. Tällaisia voisivat olla esimerkiksi jäsenten aktiivinen osallistuminen keskustelupalstoille tai sähköpostitse tapahtuva kohteen pommittaminen.

On todettu, että käyttäjät ovat organisaatioissa kaikkein merkittävin tietoturvariski. Yleensä tieturvahinkoja tutkittaessa on huomattu, että käyttäjät eivät ole tienneet, mitä he väärällä toiminnallaan saattavat saada aikaan.

Tämän takia tietoturvaohjeistuksella ja -koulutuksella

on erittäin suuri merkitys tietotason nostamisessa. Yksinkertaisimmillaan ohjeistus on pari A4-sivua, jossa kerrotaan selkeästi, mitä saa tehdä ja ennen kaikkea mitä ei saa tehdä. Parin tunnin tietoiskulla keran vuodessa saadaan hyvin

kerrattua keskeiset toimintaohjeet ja hyvät käytännöt tietoturvan noudattamiseksi.

Jotta organisaation titusasiat olisivat hyvin hallinnassa, niihin liittyvät toimintatavat on otettava huomioon kaikessa toiminnassa. Pelkkä virustarkistus tai palomuri ei riitä, vaan tietoturvapoliitikan tulee alkaa aina yrityksen ulko-ovelta ja ulottua yrityksestä lähtevään sähköpostiviestiin ja hävitettäväksi tarkoitettuun paperimateriaaliin.

Jotta tämä kaikki toteutuu, pitää organisaation johdon ymmärtää näiden asioiden merkitys sekä sitoutua omalla esimerkillään myös niitä noudattamaan ja tukemaan.

Loppujen lopuksi vastuunkantajat ainakin teoriassa löytyvät tietoturva- ja tietosuojaloukkauksissakin talon johdosta.

