SANASTOKESKUS TSK
TERMINOLOGICENTRALEN TSK

TSK 31

TIIVIS TIETOTURVASANASTO

KONCIS INFORMATIONSSÄKERHETSORDLISTA

COMPACT VOCABULARY OF INFORMATION SECURITY

Helsinki 2004

Julkaisija: Sanastokeskus TSK ry

© Sanastokeskus TSK ry

ISBN 951-628-412-4 (nid.)
ISBN 952-9794-17-7 (PDF)

ISSN 0359-5390 (painettu)
ISSN 1795-6323 (verkkojulkaisu)

ESIPUHE

Tietoturva on aihe, joka koskee kaikkia kansalaisia. Joitakin vuosia sitten asia saattoi vielä helposti jäädä ensisijaisesti asiantuntijoiden huoleksi, mutta nykyisin tietotekniikan sovellusalueiden ja tietoturvariskien jatkuvasti lisääntyessä jokaisen on oltava tietoinen riskeistä ja niiden torjunnasta. Aihealue ei kuitenkaan ole helppo. Monelle maallikolle tiedonhankinta on hankalaa, koska ensisijaisesti asiantuntijoille tarkoitettujen tietolähteiden hyödyntäminen edellyttää yleensä vähintään aihepiirin peruskäsitteiden hallintaa. Toisaalta tietolähteitä tarvitaan englannin lisäksi myös muilla kielillä. Erityisesti silloin, kun on kyse asiantuntijoilta maallikoille suunnatusta viestinnästä, englanninkielinen termistö ei riitä, vaan tarvitaan selkeitä termejä kansalliskielillämme suomeksi ja ruotsiksi.

Tietoturvakäsitteistön omaksumisen ja käytön helpottamiseksi Sanastokeskus TSK aloitti syksyllä 2003 hankkeen tietoturvasanaston laatimiseksi. Tavoitteena on ollut laatia tietoturvan peruskäsitteet kattava sanasto tietotekniikan peruskäyttäjille. Sanasto on myös osa hallituksen kansallista tietoturvastrategiaa, jolla pyritään edistämään tietoturvaa ja lisäämään kansalaisten ja yritysten luottamusta tietoyhteiskuntaan.

Valmiiseen sanastoon on koottu termitietueina ja käsitekaavioina tiedot noin 80:sta aihealueeseen liittyvästä käsitteestä. Sanastossa pyritään esittämään käsitteet selkeiden määritelmien ja esimerkkien avulla sekä antamaan suositukset suomenkielisiksi termeiksi. Lisäksi sanastossa annetaan ruotsin- ja englanninkieliset termivastineet. Koska tietoturvaan liittyvä ruotsin- ja englanninkielinen termistö ei ole aivan vakiintunutta, joissakin tietueissa on päädytty antamaan useita yleisesti käytössä olevia ruotsin- ja englanninkielisiä vastineita.

Tiivis tietoturvasanasto käsittelee paitsi yleisesti tietoturvaan liittyviä käsitteitä myös tietoturvauhkia ja tietoturvan keinoja. Lisäksi esitellään muutamia alan keskeisiä suomalaisia organisaatioita. Käsitteet on pyritty kuvaamaan määritelmien ja huomautuksiin sisältyvien esimerkkien avulla niin, että yhtäältä käsitteiden erottaminen toisistaan ja toisaalta käsitteiden välisten yhtymäkohtien löytäminen on mahdollista. Koska sanaston kohderyhmänä ovat tietotekniikan peruskäyttäjät, mukaan on valittu nimenomaan tietojärjestelmien ja tietoverkkojen tietoturvaan liittyviä käsitteitä. Myös joidenkin käsitteiden määritelmät on selvyyden vuoksi päädytty laatimaan rajauksen mukaisesta näkökulmasta. Tällaisia käsitteitä ovat esimerkiksi *hyökkäys* ja *tunkeutuminen*, jotka voitaisiin määritellä laajemmin myös hyökkäyksenä ja tunkeutumisena tilaan.

Sanastosta toivotaan olevan hyötyä paitsi jokaiselle tietoturva-asioita miettivälle myös alan ammattikielen käyttäjille, kuten kääntäjille, toimittajille ja tiedottajille.

Sanaston laatineeseen työryhmään ovat kuuluneet:

Lars Böhling, **Mika Härmä**, **Tuulia Sutinen** Elisa Oyj
Janne Kiiskinen, TeliaSonera Finland Oyj
Timo Lehtimäki, Viestintävirasto
Jouni Nupponen, Finnet-liitto ry
Mika Pehkonen, F-Secure
Juha Perttula, liikenne- ja viestintäministeriö
Mari Suhonen, Sanastokeskus TSK ry

Englanninkielisten termien tarkistukseen on lisäksi osallistunut **Päivi Ilves** TeliaSonera Finland Oyj:stä ja ruotsinkielisten termien tarkistukseen **Satu Närvä** Viestintävirastosta ja **Rune Skogberg** TeliaSonera Finland Oyj:stä.

Sanaston laatimiseen tarvittavan terminologisen työn rahoittivat
Elisa Oyj
Finnet-liitto ry
liikenne- ja viestintäministeriö
TeliaSonera Finland Oyj ja
Viestintävirasto.

Sanastosta pyydettiin huhtikuussa 2004 lausunnot alan asiantuntijatahoilta ja kielenhuoltajilta, joilta saatua palautetta käytettiin hyväksi sanastoa viimeisteltäessä. Kiitämme sanastotyöryhmän jäseniä ja lausunnonantajia heidän arvokkaasta työpanoksestaan.

SISÄLLYSLUETTELO

KÄSITEKAAVIOLUETTELO

TERMINOLOGISESTA SANASTOTYÖSTÄ

Tiivis tietoturvasanasto on laadittu terminologisten periaatteiden ja menetelmien mukaisesti. Näitä menetelmiä on kuvattu yksityiskohtaisesti muun muassa Sanastotyön käsikirjassa (TSK 14, SFS-käsikirja 50, 1989).

Terminologiselle sanastotyölle on ominaista käsitekeskeisyys. Sanakirjatyö tarkastelee sanoja ja niiden merkityksiä, kun taas terminologian lähtökohtana ovat käsitteet ja niiden väliset suhteet. **Käsitteet** ovat ihmisen mielessään muodostamia ajatusmalleja, jotka vastaavat tiettyjä ympäröivän todellisuuden kohteita, niin sanottuja **tarkoitteita**. Tarkoitteet voivat olla konkreettisia tai abstrakteja, ja niillä on erilaisia sisäisiä ja toisiin tarkoitteisiin liittyviä ominaisuuksia. Näistä ominaisuuksista muodostettuja ajatusmalleja kutsutaan **käsitepiirteiksi**. Käsitteen sisältö muodostuu joukosta erilaisia käsitepiirteitä, joista olennaiset ja erottavat kuvataan kielellisesti **määritelmän** avulla. **Termit** puolestaan ovat käsitteiden kielellisiä nimityksiä, joiden avulla voidaan lyhyesti viitata käsitteen koko sisältöön — edellyttäen, että se on tunnettu.

Terminologisista työmenetelmistä tärkein on käsiteanalyysi, jossa selvitetään kunkin käsitteen olennainen sisältö, käsitteiden väliset suhteet ja näiden suhteiden perusteella muodostuvat käsitejärjestelmät. Käsiteanalyysin tuloksia käytetään hyväksi kirjoitettaessa määritelmiä ja usein myös valittaessa termejä. Käsitejärjestelmät kuvataan usein myös graafisina kaavioina.

Käytännön terminologisessa käsiteanalyysissä eritellään yleensä kolmenlaisia käsitesuhteita. **Hierarkkinen suhde** vallitsee laajemman yläkäsitteen ja sitä suppeamman alakäsitteen välillä. Alakäsite sisältää tällöin kaikki yläkäsitteen piirteet sekä vähintään yhden lisäpiirteen, mutta sitä vastaa suppeampi joukko tarkoitteita kuin yläkäsitettä. Alakäsite voidaan siis ajatella yläkäsitteen erikoistapaukseksi. Esimerkiksi *julkisen avaimen menetelmä* on *salausmenetelmän* hierarkkinen alakäsite. Kustakin hierarkkisesta alakäsitteestä tulee aina voida osoittaa todeksi looginen lause "Y on eräänlainen X" (esim. "julkisen avaimen menetelmä on eräänlainen salausmenetelmä").

Koostumussuhteessa alakäsitteet ovat osia yläkäsitteenä olevasta kokonaisuudesta. Yläkäsitteen piirteet eivät kuitenkaan sisälly alakäsitteeseen kuten hierarkkisessa käsitejärjestelmässä. Esimerkiksi *hyökkäys* koostuu eri vaiheista, muun muassa *tunkeutumisesta*. Koostumussuhteisesta alakäsitteestä ei voida todeta lausetta "Y on eräänlainen X".

Funktiosuhteina kuvataan laaja joukko erilaisia käsitesuhteita, joita ei voida luokitella hierarkkisiksi tai koostumussuhteiksi. Niitä ovat esimerkiksi ajalliset, paikalliset, toiminnalliset, välineelliset sekä alkuperään ja syntyyn liittyvät suhteet. Funktiosuhteen tyyppi käy yleensä ilmi määritelmän kielellisestä muodosta; graafisissa kaavioissa tätä tyyppiä ei sen sijaan eritellä tarkemmin. Esimerkkejä erilaisista funktiosuhteista ovat *tietoturvan (1)* ja *luottamuksellisuuden* sekä *tietoturvariskin* ja *tietoturvauhan* väliset suhteet.

Käsitejärjestelmät ovat tavallisesti moniulotteisia ja sekakoosteisia. **Moniulotteisuudella** tarkoitetaan sitä, että yläkäsitteestä voidaan päästä eri jaotteluperusteita käyttäen erilaisiin alakäsitevalikoimiin. Yhden valikoiman mukaiset alakäsitteet ovat aina toisensa poissulkevia, ne eivät voi yhdistyä uudeksi käsitteeksi. Useasta eri valikoimasta poimittuja alakäsitteitä voidaan puolestaan yhdistää uusiksi käsitteiksi. Esimerkiksi *haittaohjelmat* voidaan ryhmitellä leviämistavan mukaan (*virus* ja *mato*) tai toiminnan mukaan (*vakoiluohjelma*). **Sekakoosteisuus** puolestaan tarkoittaa sitä, että samassa käsitejärjestelmässä esiintyy useita eri käsitesuhdetyyppejä.

Käsitejärjestelmien graafista kuvaamista esitellään kohdassa luvussa *Sanaston rakenne ja merkinnät*.

SANASTON RAKENNE JA MERKINNÄT

Sanasto on ryhmitelty aiheenmukaisesti jäsenneltyihin lukuihin. Kunkin luvun sisällä toisilleen läheiset käsitteet on pyritty sijoittamaan lähekkäin. Käsitekaaviot on sijoitettu sanastossa niiden käsitteiden jälkeen, joiden välisiä suhteita kyseisessä kaaviossa kuvataan. Sanaston lopussa on aakkosellinen hakemisto kullakin sanaston kielellä. Hakemistoissa termien perässä olevat numerot viittaavat termitietueen numeroon. Hakemistoihin on poimittu suositettavien ja hylättävien termien lisäksi määritelmiä täydentäviin huomautuksiin sisältyviä hakusanoja. Muut kuin suositettavat tai hylättävät termit on merkitty hakemistossa viittauksella päätermiin ja sen tietuenumeroon.

Sanaston termit, määritelmät ja niitä täydentävät huomautukset esitetään sanastossa termitietueina. Kukin termitietue sisältää yhden käsitteen tiedot. Esimerkiksi:

1 60
2 **varmenne**
3 mieluummin kuin: sertifikaatti
4 sv certifikat *n*; elektroniskt certifikat *n*; digitalt certifikat *n*
en certificate; digital certificate
5 sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä
6 Varmenne on yleensä ulkopuolisen *varmentajan* myöntämä.
Varmenne voi sisältää muun muassa henkilön julkisen avaimen, henkilötiedot, varmenteen voimassaolopäiväyksen sekä varmenteen myöntäjän *sähköisen allekirjoituksen*.
Henkilövarmenne vahvistaa yksityisen henkilön henkilöllisyyden. **Roolivarmenne** vahvistaa sekä henkilön henkilöllisyyden että oikeuden toimia jossakin roolissa, kuten tietyssä työtehtävässä. **Laatuvarmenne** täyttää sähköisistä allekirjoituksista annetussa laissa säädetyt vaatimukset ja sen on myöntänyt säädetyt vaatimukset täyttävä varmentaja. **Palvelinvarmenne** on palvelimelle myönnetty varmenne, jonka avulla henkilö tai tietojärjestelmä voi varmistua siitä, asioiko oikean palvelimen kanssa.

Termitietue sisältää tietueen numeron (1), käsitettä vastaavat suomenkieliset termit (2), mahdolliset hylättävät suomenkieliset termit (3), ruotsin- ja englanninkieliset termivastineet ja mahdolliset hylättävät termivastineet (4), käsitteen määritelmän (5) ja usein myös määritelmää täydentäviä tai termien käyttöön liittyviä huomautuksia (6).

Termeistä samanarvoiset **synonyymit** on erotettu toisistaan puolipisteellä. Jos termiä ei suositeta käytettäväksi esimerkiksi vierasperäisyytensä tai käsitteellisen epätarkkuutensa vuoksi, termejä edeltää merkintä "mieluummin kuin:" (ruotsiksi "hellre än:"). Jos termi on hylättävä siksi, että se viittaa muuhun kuin tietueessa määriteltävään käsitteeseen, sitä edeltää merkintä "ei:" (ruotsiksi "inte:", englanniksi "not:"). Määritelmissä ja huomautuksissa kursivoidut termit viittaavat tässä sanastossa toisaalla määriteltyihin käsitteisiin. Hakemistoon hakusanoiksi poimitut termit on esitetty huomautuksissa lihavoituina.

Termitietueissa määritellyille käsitteille on annettu vieraskieliset **vastineet** ruotsiksi ja englanniksi, ja vastineet on merkitty standardoiduin kielten tunnuksin (vrt. SFS-ISO 639 Kielten nimien tunnukset) seuraavassa järjestyksessä:

sv	ruotsi (yleisruotsi)
svFI	suomenruotsi
en	englanti (yleisenglanti)
enGB	britannianenglanti
enUS	amerikanenglanti.

Vastineiden suvut ja luvut on merkitty seuraavasti:

n	neutri (ruotsin ett-suku)
pl	monikko.

Termien ja erikielisten vastineiden yhteydessä on käytetty myös seuraavia merkintöjä:

- * termiehdotus
- † vanhentunut termi
- < termi tai vieraskielinen vastine viittaa määriteltyä käsitettä laajempaan käsitteeseen samanlaisessa käsitejärjestelmässä
- > termi tai vieraskielinen vastine viittaa määriteltyä käsitettä suppeampaan käsitteeseen samanlaisessa käsitejärjestelmässä
- ~ muu lähivastine, joka viittaa eri tavalla rajautuvaan käsitteeseen tai käsitteeseen toisentyyppisessä käsitejärjestelmässä.

Mikäli samannäköisellä termillä viitataan useaan eri käsitteeseen, on eri käsitteisiin viittaavat termit numeroitu käsitteiden erottamisen helpottamiseksi. Esimerkiksi termi *tietoturva (1)* viittaa järjestelyihin, joilla pyritään varmistamaan käytettävyys, tiedon eheys ja luottamuksellisuus. *Tietoturva (2)* puolestaan viittaa oloihin, joissa tietoturvariskit ovat hallinnassa.

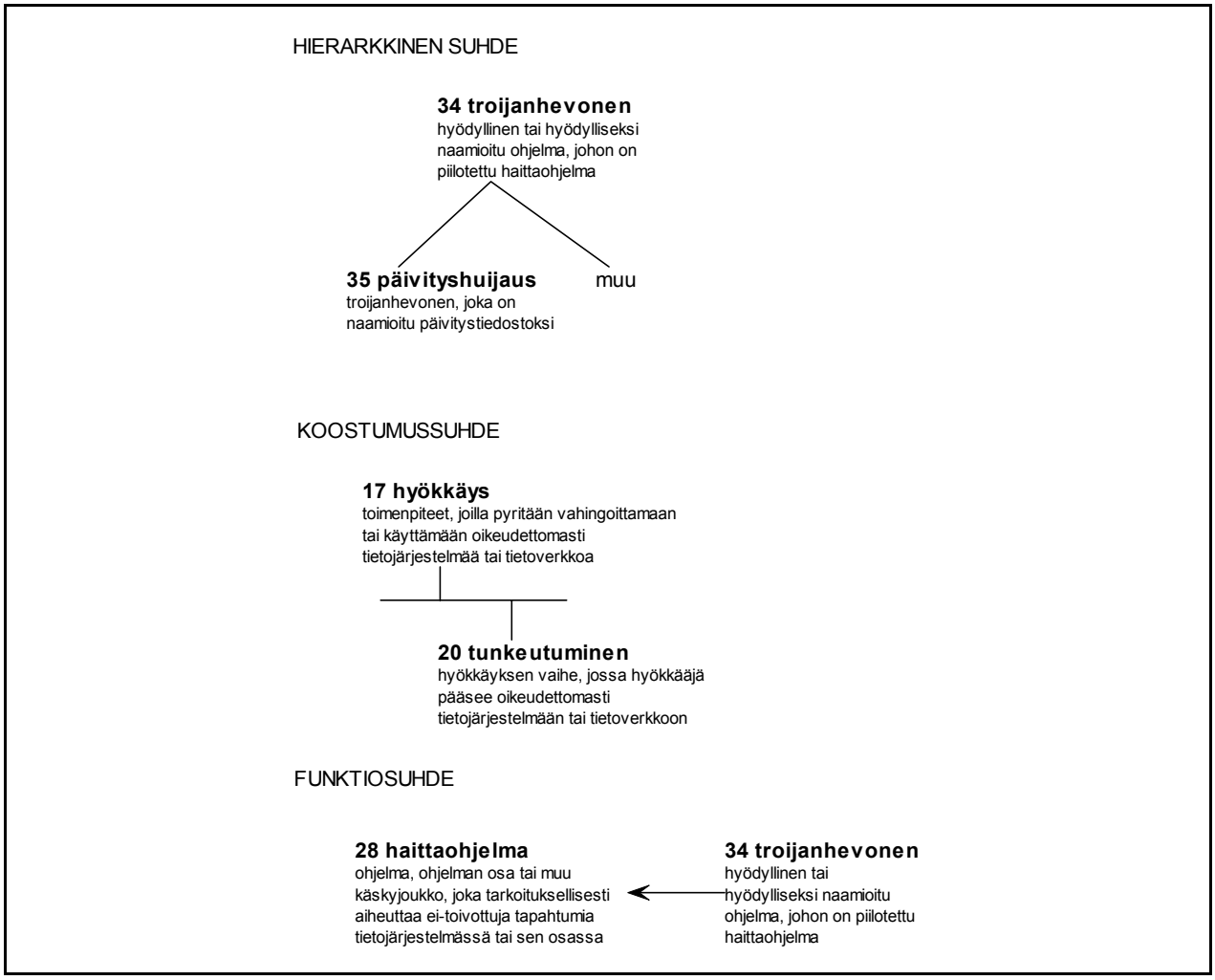
Käsitteiden sisältöä kuvaavat ja rajaavat **määritelmät** on laadittu terminologiassa käytettyjen yleisten periaatteiden mukaisesti. Määritelmät sisältävät vähimmäismäärän tietoa käsitteen yksilöimiseksi ja erottamiseksi muista käsitteistä. Määritelmät on yleensä pyritty muotoilemaan siten, että niiden avulla voidaan tunnistaa käsitteen paikka käsitejärjestelmässä. Kansainvälisten määritelmänkirjoitusperiaatteiden mukaisesti määritelmät alkavat pienellä kirjaimella eikä niiden lopussa ole pistettä.

Määritelmää täydentävissä **huomautuksissa** on muun muassa esitetty lisätietoja käsitteen sisällöstä, annettu esimerkkejä ja kerrottu käsitteeseen läheisesti liittyvistä muista käsitteistä. Lisäksi huomautuksissa voi olla tietoa sekä suomen- että vieraskielisten termien käytöstä. Huomautukset alkavat isolla kirjaimella, niiden lopussa on piste ja ne on erotettu määritelmistä sisennyksellä.

Sanastossa on mukana käsitteiden välisiä suhteita kuvaavia **käsitekaavioita**. Kaaviot eivät kuvaa mitään todellisuudessa esiintyvää yksittäistä tilannetta, tapahtumaa tai järjestelmää, minkä vuoksi käsitekaaviot eroavat muun muassa organisaatiokaavioista ja prosessikaavioista. Sen sijaan kaaviot kuvaavat, kuten käsitteiden sanalliset määritelmätkin, niitä yleistyksiä, joita ihmiset mielessään muodostavat joukosta samantyyppisiä todellisuuden ilmentymiä ja joita nimitetään käsitteiksi. Käsitekaavioissa kutakin käsitettä on kuvattu termin ja määritelmän avulla. Sanastossa omana termitietueenaan esiintyvien käsitteiden termit on esitetty lihavoituina. Määritelmät on esitetty termejä pienemmällä kirjasinkoolla. Kaaviot eivät sisällä termitietueiden huomautuksia. Numerot termien edessä viittaavat sanaston tietuenumeroihin.

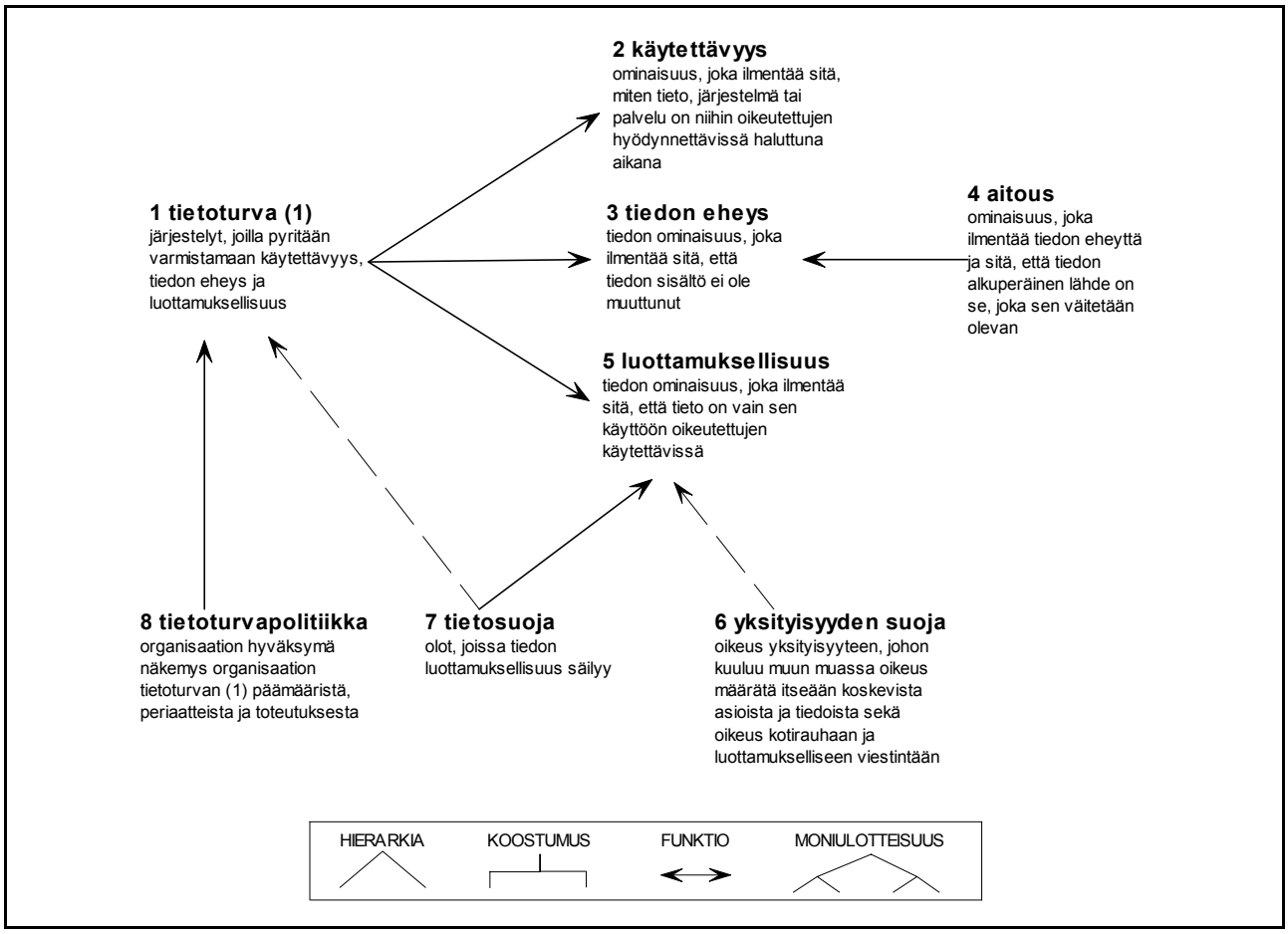
Käsitekaavioissa on käytetty terminologisten käsitesuhteiden Suomessa vakiintuneita merkintätapoja. **Hierarkkisia käsitesuhteita** kuvataan pysty- ja vinoviivoin piirrettävinä puudiagrammeina. **Koostumussuhteita** kuvataan pysty- ja vaakaviivoista muodostettuina kampadiagrammeina. Kaksoisviivan käyttö koostumussuhteessa viittaa tilanteeseen, jossa kokonaisuuteen tarvitaan tyypillisesti monta kyseisenlaista osaa. Hierarkia- ja koostumussuhteiden piirrossuunta on yleensä joko ylhäältä alaspäin tai vasemmalta oikealle. **Funktiosuhteita** kuvataan nuolilla. **Moniulotteisuus** on esitetty paksunnetuilla viivoilla. Lisäksi jaotteluperuste on merkitty ulottuvuusviivan viereen. Katkoviivoilla on merkitty käsitesuhteita, jotka ovat käsitteen ymmärtämisen kannalta tärkeitä mutta määrittelyn kannalta epäolennaisia.

Seuraavalla sivulla on esitetty esimerkkejä erilaisista käsitesuhteiden merkintätavoista.



Esimerkkejä käsitesuhteiden merkintätavoista

1 PERUSKÄSITTEITÄ



Kaavio 1. Tietoturva

1
tietoturva (1); **tietoturvallisuus (1)**
sv informationssäkerhet (1); > datasäkerhet (1) (tietoaineistoturvallisuudesta)
inte: dataskydd *n* (1)
en information security (1); > data security (1) (tietoaineistoturvallisuudesta)

järjestelyt, joilla pyritään varmistamaan *käytettävyys*, *tiedon eheys* ja *luottamuksellisuus*

Tietoturvan (1) järjestelyjä ovat esimerkiksi *salaus* ja varmuuskopiointi sekä *palomuurin*, *virustorjuntaohjelman* ja *varmenteiden* käyttö.

Tietoturvaan (1) kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.

Yhdyssanojen osana suositetaan käytettäväksi sanaa tietoturva.

2
käytettävyys
mieluummin kuin: saatavuus; palveluvarmuus
sv tillgänglighet; > informationstillgänglighet
en availability

ominaisuus, joka ilmentää sitä, miten tieto, järjestelmä tai palvelu on niihin oikeutettujen hyödynnettävissä haluttuna aikana

Tästä käsitteestä suositetaan käytettäväksi ainoastaan termiä käytettävyys. Termi saatavuus on tietoturvan yhteydessä vakiintunut viittaamaan vain tiedon hyödynnettävyyteen. Termi palveluvarmuus on puolestaan vakiintunut viittaamaan vain palvelujen ja järjestelmien hyödynnettävyyteen.

Suomen kielessä käytettävyys-termiä käytetään myös tarkoitettaessa esimerkiksi ohjelmiston helppokäyttöisyyttä. Englanninkielinen vastine on tällöin **usability**.

3
tiedon eheys; **eheys**
sv dataintegritet; informationsintegritet; integritet (1) ; ~informationskvalitet
en data integrity; integrity

tiedon ominaisuus, joka ilmentää sitä, että tiedon sisältö ei ole muuttunut

4
aitous
sv autenticitet; riktighet
en authenticity; genuineness

ominaisuus, joka ilmentää *tiedon eheyttä* ja sitä, että tiedon alkuperäinen lähde on se, joka sen väitetään olevan

Tiedon lähde voi olla esimerkiksi henkilö tai jokin muu taho.

Alkuperäisyys-sanaa käytetään toisinaan samassa merkityksessä kuin aitous-termiä.

5
luottamuksellisuus
sv konfidentialitet; sekretess (1)
en confidentiality

tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä

6
yksityisyyden suoja; **yksityiselämän suoja**
sv integritetsskydd *n*; skydd *n* av personlig integritet; skydd *n* för personlig integritet; skydd *n* för privatlivet; integritet (2); personlig integritet
en privacy protection; protection of privacy

oikeus yksityisyyteen, johon kuuluu muun muassa oikeus määrätä itseään koskevista asioista ja tiedoista sekä oikeus kotirauhaan ja luottamukselliseen viestintään, vrt. *luottamuksellisuus*

Esimerkiksi oikeudeton henkilötietojen käsittely tai kameravalvonta tai *roskapostin* lähettäminen sähköpostitse voi loukata henkilön yksityisyyden suojaa.

7
tietosuoja
sv dataskydd *n* (2); datasekretess; sekretesskydd; sekretess (2)
enGB data protection
enUS > confidentiality of personal information

olot, joissa tiedon *luottamuksellisuus* säilyy

Tietosuojaan kuuluvia luottamuksellisia tietoja ovat esimerkiksi henkilötiedot.

Tietosuoja pyritään toteuttamaan muun muassa *tietoturvalla (1)*.

8
tietoturvapolitiikka
sv informationssäkerhetspolicy; > datasäkerhetspolicy
en information security policy; < information security management system policy; < ISMS policy

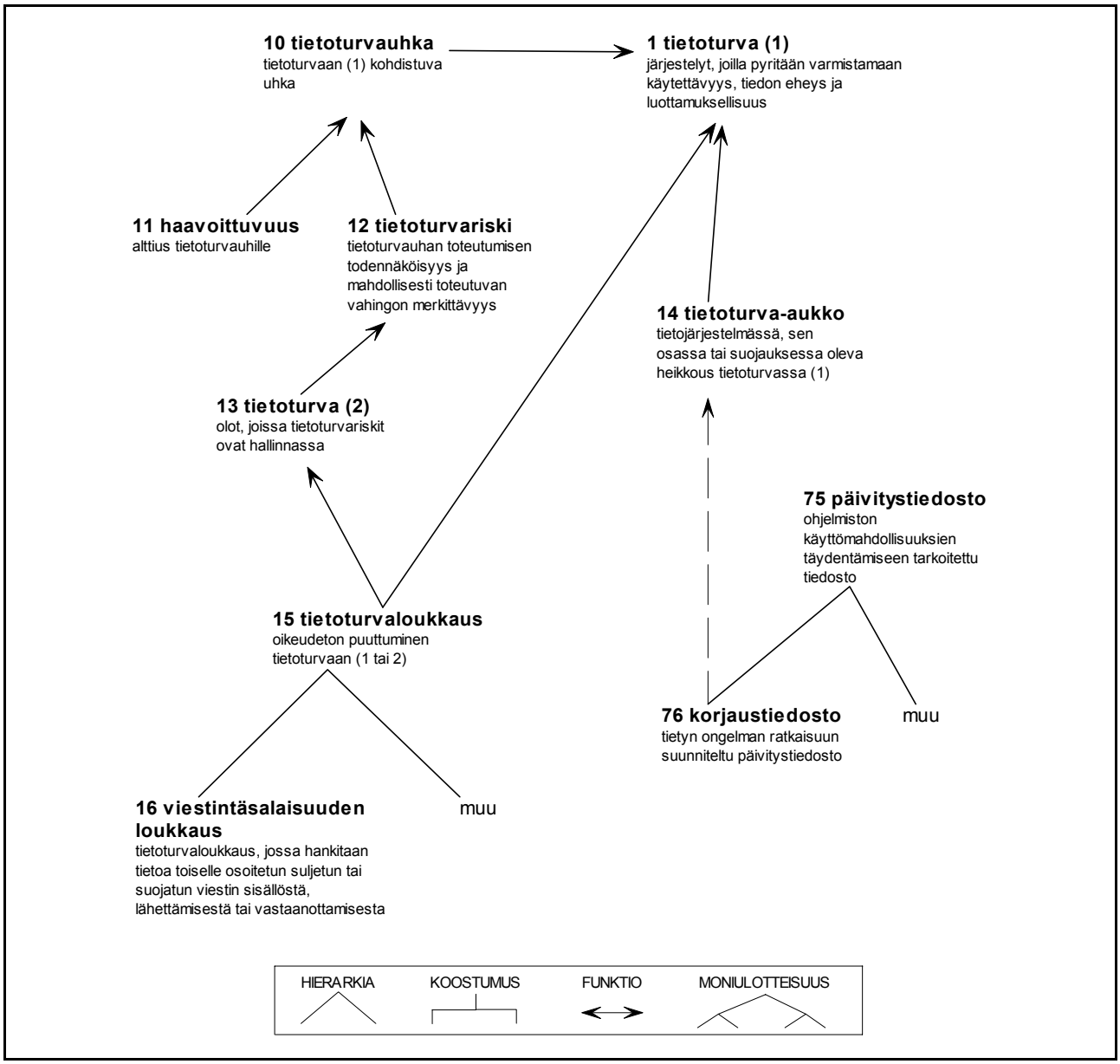
organisaation hyväksymä näkemys organisaation *tietoturvan (1)* päämääristä, periaatteista ja toteutuksesta

9
kiistämättömyys
sv oavvislighet; obestridlighet
en non-repudiation

ominaisuus, joka ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen

Kiistämättömyyteen voidaan pyrkiä muun muassa käyttämällä *sähköistä allekirjoitusta* tai tapahtuma-ajan vahvistavaa teknistä menetelmää, kuten aikaleimaa.

2 TIETOTURVAUHKIA



Kaavio 2. Tietoturvauhka

10
tietoturvauhka
sv hot *n* mot informationssäkerhet; informationssäkerhetshot *n*; > hot *n* mot datasäkerhet; < säkerhetshot *n*
en information security threat

tietoturvaan (1) kohdistuva uhka

Tietoturvauhka voi olla sisäinen tai ulkoinen. **Sisäisellä uhkalla** tarkoitetaan organisaation oman henkilökunnan toiminnasta muodostuvaa tietoturvauhkaa ja **ulkoisella uhkalla** organisaation ulkopuolisesta seikasta, kuten *viruksesta*, muodostuvaa tietoturvauhkaa.

11
haavoittuvuus
sv sårbarhet
en vulnerability

alttius *tietoturvauhille*

Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön.

Haavoittuvuus-termiä käytetään toisinaan *tietoturva-aukon* merkityksessä.

12
tietoturvariski
sv informationssäkerhetsrisk; < säkerhetsrisk; > datasäkerhetsrisk
en information security risk

tietoturvauhan toteutumisen todennäköisyys ja mahdollisesti toteutuvan vahingon merkittävyys

Riskin suuruus riippuu mahdollisen vahingon suuruudesta ja vahinkotapahtuman todennäköisyydestä.

13
tietoturva (2); **tietoturvallisuus (2)**
sv informationssäkerhet (2); > datasäkerhet (2) (tietoaineistoturvallisuudesta)
en information security (2); > data security (2) (tietoaineistoturvallisuudesta)

olot, joissa *tietoturvariskit* ovat hallinnassa

14
tietoturva-aukko
sv säkerhetshål *n*; säkerhetslucka
en security hole; security flaw; security loophole

tietojärjestelmässä, sen osassa tai suojauksessa oleva heikkous *tietoturvassa (1)*

Tietoturva-aukko mahdollistaa esimerkiksi tietojärjestelmään *tunkeutumisen*. Muun muassa *madot* ja *hakkerit* voivat hyödyntää tietoturva-aukkoja.

15
tietoturvaloukkaus
sv brott *n* mot informationssäkerhet; < säkerhetsbrott *n*; > brott *n* mot datasäkerhet
svFI kränkning av informationssäkerhet
en security breach; security violation

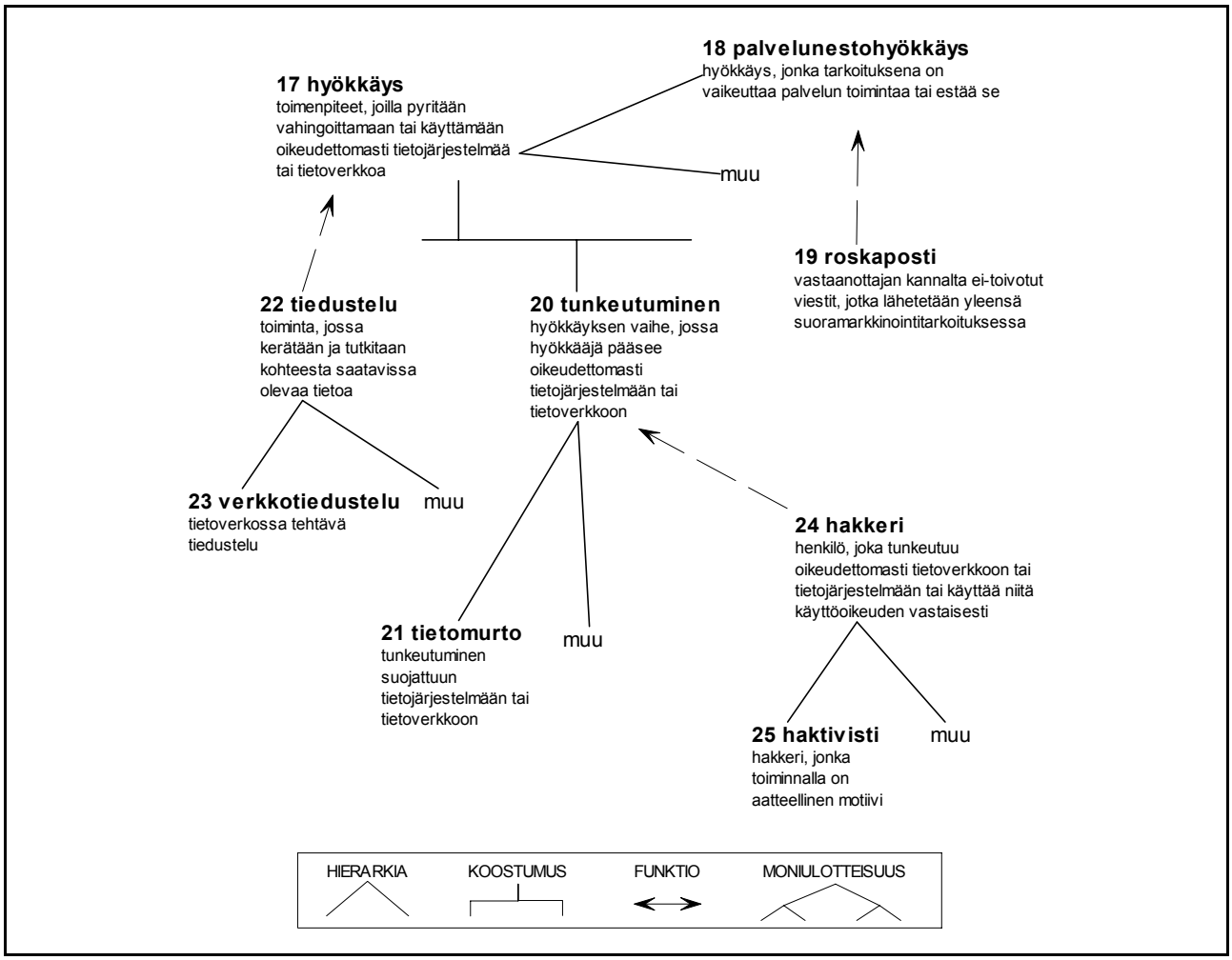
oikeudeton puuttuminen *tietoturvaan (1 tai 2)*

Esimerkiksi *tietomurto* on tietoturvaloukkaus.

16
viestintäsalaisuuden loukkaus
sv brott *n* mot kommunikationshemlighet
svFI kränkning av kommunikationshemlighet
en breach of communications confidentiality; violation of communications confidentiality; breach of communications secrecy; violation of communications secrecy

tietoturvaloukkaus, jossa hankitaan tietoa toiselle osoitetun suljetun tai suojatun viestin sisällöstä, lähettämisestä tai vastaanottamisesta

Viestintäsalaisuuden loukkaus uhkaa erityisesti *luottamuksellisuutta*.



Kaavio 3. Hyökkäys

17
hyökkäys
sv attack
en attack

toimenpiteet, joilla pyritään vahingoittamaan tai käyttämään oikeudettomasti tietojärjestelmää tai tietoverkkoa

Hyökkäys voidaan toteuttaa esimerkiksi **verkkohyökkäyksenä** tietoverkon kautta.

18
palvelunestohyökkäys
sv blockeringsattack
en denial-of-service attack; DoS attack

hyökkäys, jonka tarkoituksena on vaikeuttaa palvelun toimintaa tai estää se

Palvelunestohyökkäys voi esimerkiksi lamaannuttaa sähköpostipalvelun suurella määrällä sähköpostiviestejä tai palvelimen tai reitittimen liian suurella määrällä palvelupyyntöjä.

Palvelunestohyökkäys on yleensä **hajautettu palvelunestohyökkäys**, eli se toteutetaan yhtä aikaa useista eri lähteistä.

19
roskaposti
sv skräppost; spam
en spam; junk mail; unsolicited commercial email; UCE

vastaanottajan kannalta ei-toivotut viestit, jotka lähetetään yleensä suoramarkkinointitarkoituksessa

Yleensä roskapostia lähetetään suurelle vastaanottajajoukolle yhdellä kertaa.

Roskapostia voidaan käyttää myös esimerkiksi *palvelunestohyökkäykseen*.

20
tunkeutuminen
sv intrång *n*
en intrusion; penetration

hyökkäyksen vaihe, jossa hyökkääjä pääsee oikeudettomasti tietojärjestelmään tai tietoverkkoon

Tunkeutumisen tavoitteena voi olla esimerkiksi päästä käsiksi tietojärjestelmässä olevaan tietoon.

21
tietomurto
sv dataintrång *n*
en data system break-in; data trespass; cracking; hacking

tunkeutuminen suojattuun tietojärjestelmään tai tietoverkkoon

Tietomurtoon saatetaan käyttää erityistä **tietomurto-ohjelmaa**.

Tietomurto on määrätty rangaistavaksi rikoslaissa.

22
tiedustelu
sv kartläggning
en gathering intelligence; intelligence

toiminta, jossa kerätään ja tutkitaan kohteesta saatavissa olevaa tietoa

Tiedustelu voi edeltää *hyökkäystä* tai olla itse hyökkäys.

Tiedustelu voi loukata *luottamuksellisuutta*.

23
***verkkotiedustelu**
mieluummin kuin: skannaus
sv kartläggning av datanät; skanning
en scan; scanning; > port scanning; > footprinting

tietoverkossa tehtävä *tiedustelu*

Verkkotiedustelu voidaan toteuttaa esimerkiksi *vakoiluohjelman* avulla.

24
hakkeri; **krakkeri**
sv knäckare
en hacker; cracker; computer hacker; computer cracker

henkilö, joka tunkeutuu oikeudettomasti tietoverkkoon tai tietojärjestelmään tai käyttää niitä käyttöoikeuden vastaisesti, vrt. *tunkeutuminen*

Hakkeri saattaa esimerkiksi muuttaa luvatta ohjelmaa tai palvelua.

Suomenkielinen termi hakkeri ja englanninkielinen termi hacker ovat kaksimerkityksisiä. Termit viittaavat myös innokkaaseen tietokoneharrastajaan.

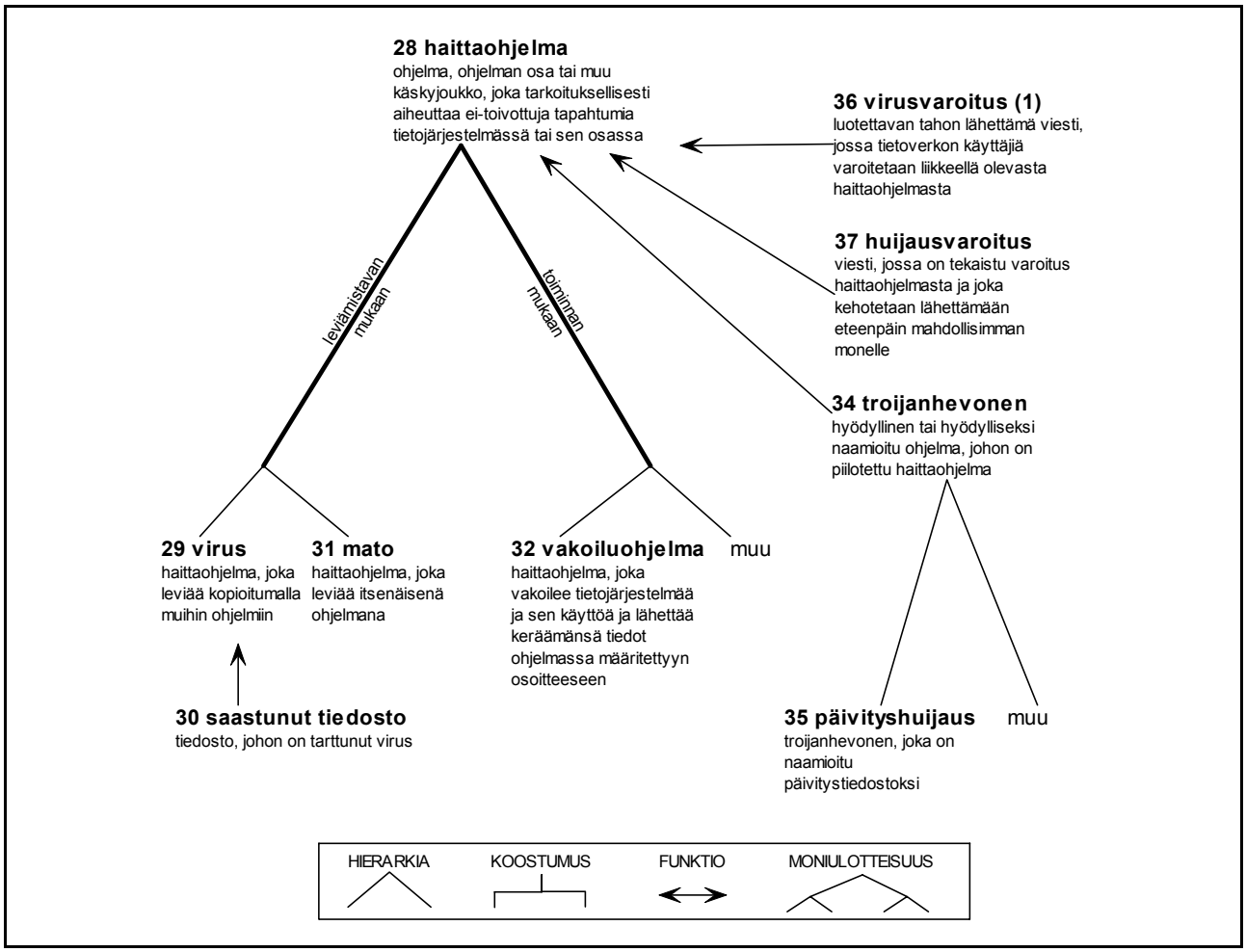
25
haktivisti
sv hacktivist
en hactivist; hacktivist

hakkeri, jonka toiminnalla on aatteellinen motiivi

26
käyttäjän manipulointi
sv social ingenjörskonst
en social engineering

toiminta, jossa toinen henkilö erehdytetään luovuttamaan luottamuksellista tietoa tai toimimaan muutoin *tietoturvaa (1)* heikentävällä tavalla, vrt. *luottamuksellisuus*

Käyttäjän manipuloinnilla voidaan pyrkiä selvittämään esimerkiksi käyttäjän *salasana*.



Kaavio 4. Haittaohjelma

27
informaatiosodankäynti; **tietosodankäynti**
sv informationskrigsföring; informationskrig *n*
en information warfare; IW; I-warfare; info-warfare

vihamielinen vaikuttaminen valitun kohteen päätöksentekoon, toimintakykyyn ja mielipiteisiin informaation tai tietojenkäsittelyn avulla sekä suojautuminen toisten vastaavilta vaikuttamisyrityksiltä

Informaatiosodankäynti voi tapahtua esimerkiksi valtioiden tai organisaatioiden välillä. Informaatiosodankäynti voi vaikuttaa varsinaisen suunnitellun kohteen ulkopuolellakin, kuten sivullisten henkilöiden tai organisaatioiden tietojenkäsittelyjärjestelmissä.

Informaatiosodankäynnissä voidaan käyttää hyväksi esimerkiksi *haittaohjelmia*.

28
haittaohjelma
sv skadligt program *n*; sabotageprogram *n*; fientligt program *n*
en malicious software; malware; malicious program; malicious logic; malicious code

ohjelma, ohjelman osa tai muu käskyjoukko, joka tarkoituksellisesti aiheuttaa ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa

Haittaohjelmia ovat esimerkiksi *virukset* ja *madot* sekä näiden yhdistelmät.

29
virus; **tietokonevirus**
sv datavirus *n*; virus *n*
en virus; computer virus

haittaohjelma, joka leviää kopioitumalla muihin ohjelmiin

Virus voi levitä esimerkiksi tiedoston, sähköpostin tai WWW-sivun välityksellä. Viruksen leviäminen vaatii yleensä tietokoneen käyttäjän toimintaa, esimerkiksi surffausta Internetissä tai sähköpostin liitteenä olevan *saastuneen tiedoston* avaamista.

Osa viruksista on muuntautumiskykyisiä.

Virukset voivat heikentää tietojärjestelmien *käytettävyyttä*, *tiedon eheyttä* ja *luottamuksellisuutta*, koska ne voivat tuhota, muuttaa tai muokata tietojärjestelmien sisältämiä tietoja. Virukset voivat myös haitata tietojärjestelmän muuta toimintaa, kuten hidastaa tai vaikeuttaa tietojärjestelmän tai käyttöjärjestelmän toimintaa.

Virus-termiä käytetään yleisesti *haittaohjelma*-termin sijaan erityisesti yhdyssanojen osana. Tällainen käyttö on vakiintunut esimerkiksi termeissä *virusvaroitus*, *virustarkistus*, *virustorjuntaohjelma*.

30
saastunut tiedosto
sv infekterad fil
en infected file

tiedosto, johon on tarttunut *virus*

31
mato
sv mask
en worm

haittaohjelma, joka leviää itsenäisenä ohjelmana

Madot leviävät tietoverkon välityksellä. Ne voivat levitä esimerkiksi *tietoturva-aukkojen* kautta tai sähköpostitse lähettämällä itse itsensä kaikkiin sähköpostiosoitteisiin, joita tietojärjestelmästä löytyy. Mato voi päästä suojaamattomaan tietokoneeseen ilman koneen käyttäjän toimintaa periaatteessa aina, kun Internet-yhteys on auki.

Mato saattaa haitata tietojärjestelmän tai yksittäisen tietokoneen toimintaa kuluttamalla näiden käsittelykapasiteettia. Mato voi myös levittää muita *haittaohjelmia*.

32
vakoiluohjelma
sv spionprogram *n*
en spyware; spy software; > key logger

haittaohjelma, joka vakoilee tietojärjestelmää ja sen käyttöä ja lähettää keräämänsä tiedot ohjelmassa määritettyyn osoitteeseen

Vakoiluohjelmaa voidaan käyttää esimerkiksi käyttäjien toimintojen kartoittamiseen tai *hyökkäyksen* valmisteluun.

33
nuuskijaohjelma
mieluummin kuin: snifferi
sv snifferprogram *n*; sniffer; avlyssningsprogram
en sniffer; sniffer software; sniffer program

ohjelma, joka lukee tietoverkon liikennettä

Nuuskijaohjelmaa voidaan käyttää sekä tietoverkon käytön vakoilemiseen että luvalliseen tietoverkon liikenteen analysointiin.

34
troijanhevonen; **troijalainen**
sv trojansk häst; trojan; trojansk kod
en Trojan horse; Trojan

hyödyllinen tai hyödylliseksi naamioitu ohjelma, johon on piilotettu *haittaohjelma*

Troijanhevosen sisältämä haittaohjelma asentuu ja toimii käyttäjän tietämättä.

Troijanhevonen saattaa esimerkiksi mahdollistaa *hyökkäyksen* tietojärjestelmään tai sen osaan tai sitä voidaan käyttää *palvelunestohyökkäyksessä* tai tietojen hankkimisessa tietojärjestelmästä.

35
päivityshuijaus
sv falsk programfix
en update hoax

troijanhevonen, joka on naamioitu *päivitystiedostoksi*

Päivityshuijaus lähetetään usein sähköpostiviestin liitetiedostona.

36
virusvaroitus (1)
sv virusvarning
en virus alert

luotettavan tahon lähettämä viesti, jossa tietoverkon käyttäjiä varoitetaan liikkeellä olevasta *haittaohjelmasta*

Luotettavalla taholla tarkoitetaan esimerkiksi CERT-FI-ryhmää (vrt. *CERT*).

37
huijausvaroitus; **virushuijaus**
ei: virusvaroitus (2)
sv falsk virusvarning; virusbluff; bluffvirus *n*
en virus hoax; hoax virus; hoax

viesti, jossa on tekaistu varoitus *haittaohjelmasta* ja joka kehotetaan lähettämään eteenpäin mahdollisimman monelle

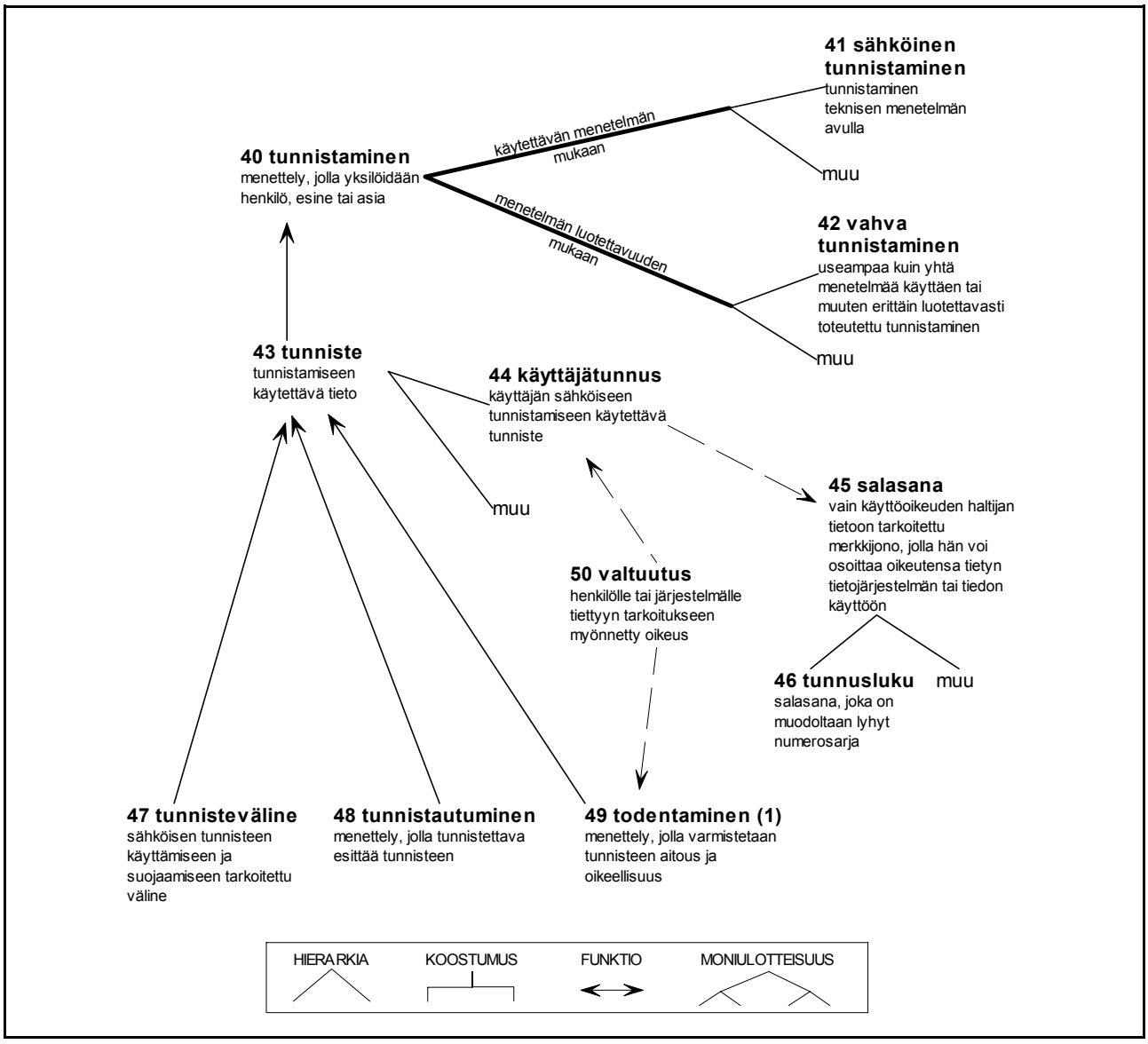
38
tietotekniikkarikos; **tietoverkkorikos**
sv databrott *n*
en computer crime; computer-related crime; network crime; cybercrime

tietojärjestelmään kohdistuva tai sen avulla tehty rikos

Tietotekniikkarikoksia voivat olla esimerkiksi *tietomurto*, tietoliikenteen häirintä, vaaran aiheuttaminen tietojenkäsittelylle ja *viestintäsalaisuuden loukkaus*.

Tietotekniikkarikos liittyy olennaisesti tietotekniikan hyödyntämiseen esimerkiksi rikoksen teon välineenä.

3 TIETOTURVAN KEINOJA



Kaavio 5. Tunnistaminen

39
pääsynvalvonta
sv åtkomstkontroll; säkerhetskontroll; < behörighetskontroll; < behörighetsadministration
en access control

menettely, jolla pyritään rajaamaan pääsyä tietojärjestelmään tai tietoihin

Pääsynvalvonnassa voidaan käyttää hyväksi esimerkiksi *tunnistamista* ja *valtuutuksia*. Pääsynvalvonta saatetaan toteuttaa esimerkiksi siten, että tietojärjestelmään pyrkivältä käyttäjältä vaaditaan *käyttäjätunnusta* ja *salasanaa*.

40
tunnistaminen; **tunnistus**
sv identifiering (1); identifikation; igenkänning
en recognition; identification (1)

menettely, jolla yksilöidään henkilö, esine tai asia

Tunnistaminen voi perustua *tunnistautumiseen* tai olla **passiivista tunnistamista**, joka ei edellytä tunnistettavalta toimintaa ja jossa tunnistettava henkilö ei välttämättä tiedä tulevansa tunnistetuksi.

Tunnistaminen voi perustua siihen, mitä henkilö on, mitä hänellä on hallussaan tai mitä hän tietää.

41
sähköinen tunnistaminen; **sähköinen tunnistus**
sv elektronisk identifiering; elektronisk identifikation
en electronic identification; electronic recognition

tunnistaminen teknisen menetelmän avulla

Sähköisessä tunnistamisessa voidaan käyttää esimerkiksi *käyttäjätunnuksia*, *salasanoja*, *varmenteita* ja henkilön biometrisiä ominaisuuksia.

42
vahva tunnistaminen
sv stark identifiering; säker identifiering
en strong identification

useampaa kuin yhtä menetelmää käyttäen tai muuten erittäin luotettavasti toteutettu *tunnistaminen*

Vahvaa tunnistamista on esimerkiksi se, kun pankkikortilla maksettaessa maksajalta vaaditaan sekä pankkikorttia että siihen liittyvän *tunnusluvun* tietämistä.

43
tunniste
sv identifierare; identifikator
en identifier; label

tunnistamiseen käytettävä tieto

44
käyttäjätunnus
sv användarnamn *n*; användaridentifikation
en username; user identifier; user ID

käyttäjän *sähköiseen tunnistamiseen* käytettävä *tunniste*

Käyttäjätunnusten avulla käyttäjät erotellaan toisistaan.

Käyttäjätunnusta käytetään yleensä yhdessä *salasanan* kanssa.

45
salasana; **salalause**
sv lösenord *n*; lösenfras
en password; passphrase

vain käyttöoikeuden haltijan tietoon tarkoitettu merkkijono, jolla hän voi osoittaa oikeutensa tietyn tietojärjestelmän tai tiedon käyttöön

Salasana voi olla kertakäyttöinen, määräaikainen tai pysyvä.

46
tunnusluku; **PIN**; **PIN-koodi**
sv personlig kod; personligt kodnummer *n*; personlig säkerhetskod; PIN-kod; PIN
en personal identification number; personal identity number; PIN; PIN code

salasana, joka on muodoltaan lyhyt numerosarja

Tunnuslukua käytetään yleensä yhdessä jonkin *tunnistevälineen*, kuten matkapuhelimen tai toimikortin, kanssa.

47
***tunnisteväline**
sv informationsbärare; token *n*
en token

sähköisen *tunnisteen* käyttämiseen ja suojaamiseen tarkoitettu väline

Tunnistevälineitä ovat esimerkiksi SIM-kortti, USB-laite ja sirukortti.

48
tunnistautuminen
sv identifiering (2)
en identification (2)

menettely, jossa tunnistettava esittää *tunnisteen*

49
todentaminen (1); **todennus (1)**
mieluummin kuin: autentikointi
sv autentisering
inte: autenticering
en authentication (1); verification (1)

menettely, jolla varmistetaan *tunnisteen aitous* ja oikeellisuus

Todentamisessa (1) voidaan esimerkiksi tarkistaa, hyväksyykö järjestelmä käyttäjän antaman *salasanan* ja *käyttäjätunnuksen* tai onko järjestelmä se, johon käyttäjä haluaa yhteyden.

50
valtuutus
sv behörighet
en authorization; authorisation

henkilölle tai järjestelmälle tiettyyn tarkoitukseen myönnetty oikeus

Valtuutuksen avulla voidaan esimerkiksi myöntää vain tietyille henkilöille pääsy tietojärjestelmän tiettyihin osiin. Esimerkiksi tietojärjestelmä voi tarkistaa käyttäjän valtuutuksen *käyttäjätunnuksen* avulla.

Valtuutus tarkistetaan yleensä *todentamisen (1)* jälkeen.

51
todentaminen (2); **todennus (2)**
mieluummin kuin: verfikaatio
sv verifiering
en verification (2); authentication (2)

menettely, jolla varmistutaan *tiedon eheyden* säilymisestä

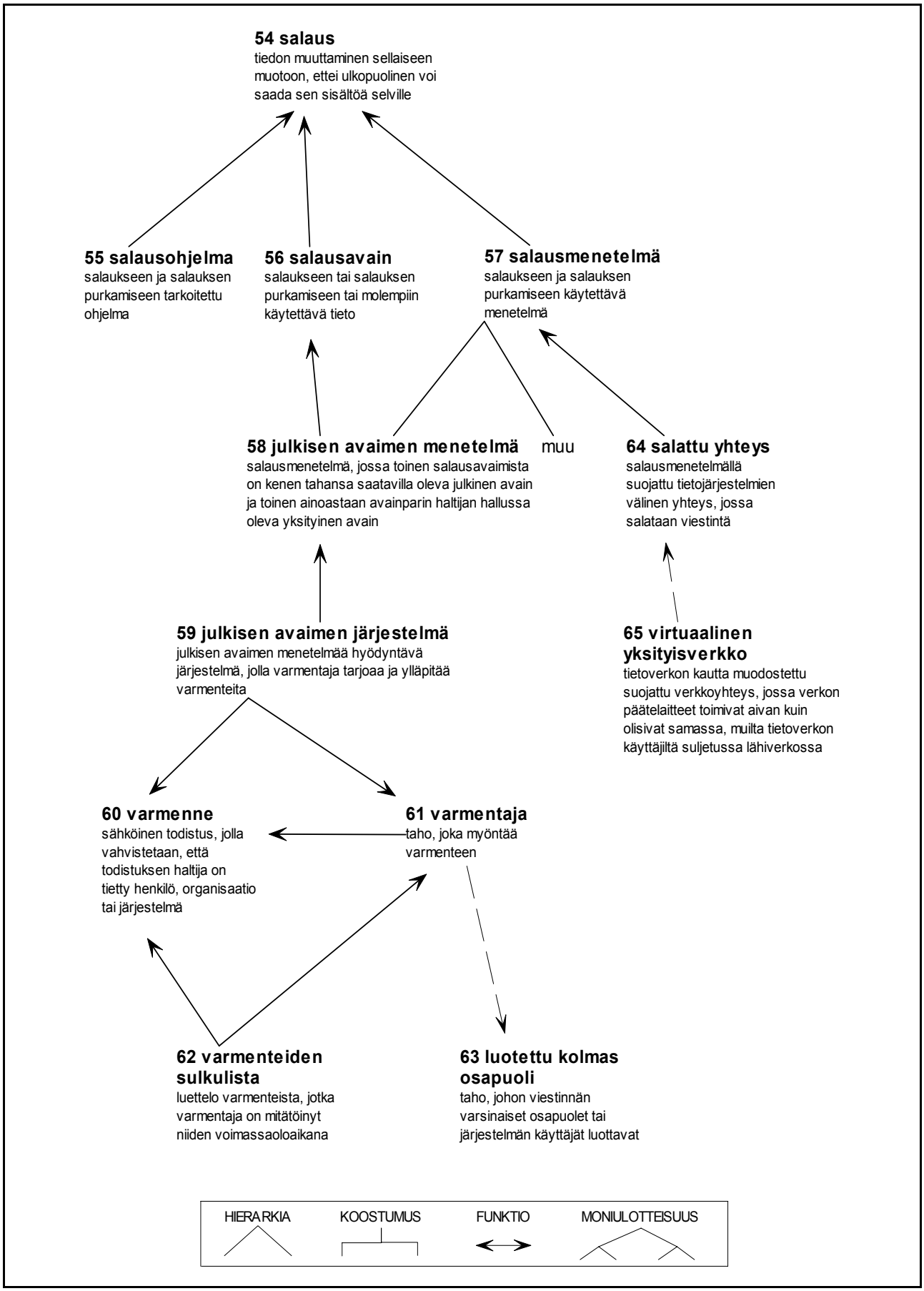
Todentamiseen (2) käytetään muun muassa *tarkistussummaa*.

Termiä **sanoman todentaminen** voidaan käyttää viitattaessa sanoman eheyden tarkistamiseen.

52
tarkistussumma; **varmistussumma**
sv kontrollsumma; kondensat *n*; hashvärde *n*
en checksum; control data; proof total; secure hash

tiedon sisällön perusteella laskettu arvo, joka liitetään tietoon *tiedon eheyden* tarkastamiseksi

Tarkistussummaa voidaan käyttää esimerkiksi tietoverkossa siirrettävän, järjestelmään tallennetun tai pakatun tiedon eheyden tarkastamiseen.



Kaavio 6. Salaus

53
sähköinen allekirjoitus
sv elektronisk signatur; digital signatur; elektronisk underskrift
en electronic signature; digital signature

sähköisessä muodossa oleva allekirjoitus

Sähköinen allekirjoitus voidaan toteuttaa teknisesti monella eri tavalla. Tietyt laissa määritetyt vaatimukset täyttävää sähköistä allekirjoitusta kutsutaan **kehittyneeksi sähköiseksi allekirjoitukseksi**.

Sähköistä allekirjoitusta voidaan käyttää sitoumusten antamiseen, *tiedon eheyden* varmistamiseen ja allekirjoittajan henkilöllisyyden todistamiseen.

54
salaus; **salakirjoitus**
mieluummin kuin: kryptaus; enkryptointi
sv kryptering
hellre än: chiffrering
en encryption; ciphering

tiedon muuttaminen sellaiseen muotoon, ettei ulkopuolinen voi saada sen sisältöä selville

Salaustekniikoiden käyttöä ja niiden tutkimista kutsutaan **kryptografiaksi**, salauksen purkamista ja purkamismenetelmien tutkimista **kryptoanalyysiksi** ja kryptografiaa ja kryptoanalyysiä tutkivaa tieteenalaa **kryptologiaksi**.

55
salausohjelma
sv krypteringsprogram *n*
en cryptographic program; > encryption program (salauksesta); > decryption program (salauksen purkamisesta)

salaukseen ja salauksen purkamiseen tarkoitettu ohjelma

56
salausavain; **salakirjoitusavain**
sv krypteringsnyckel; > dekrypteringsnyckel (salauksen purkamisesta)
en cryptographic key; CK; > encryption key (salauksesta); > decryption key (salauksen purkamisesta); > cipher key (salauksesta); > decipher key (salauksen purkamisesta)

salaukseen tai salauksen purkamiseen tai molempiin käytettävä tieto

57
salausmenetelmä; **salakirjoitusmenetelmä**
sv krypteringsteknik; krypteringsmetod
en > encryption method (salauksesta); > decryption method (salauksen purkamisesta); > ciphering method (salauksesta); > deciphering method (salauksen purkamisesta)

salaukseen ja salauksen purkamiseen käytettävä menetelmä

Symmetrinen salaus tarkoittaa salausmenetelmää, jossa salaukseen ja salauksen purkamiseen käytetään samaa *salausavainta*. **Epäsymmetrinen salaus** tarkoittaa salausmenetelmää, jossa salaukseen ja salauksen purkamiseen käytetään eri salausavaimia.

58
julkisen avaimen menetelmä
sv kryptering med öppen nyckel; öppen nyckel-kryptering; kryptering med publik nyckel; publik nyckel-kryptering
en public key encryption; public key cryptography; public key method

salausmenetelmä, jossa toinen *salausavaimista* on kenen tahansa saatavilla oleva julkinen avain ja toinen ainoastaan avainparin haltijan hallussa oleva yksityinen avain

Julkisen avaimen menetelmää voidaan käyttää tiedon sisällön *salaukseen luottamuksellisuuden* varmistamiseksi tai *sähköisen allekirjoituksen* toteuttamiseen *tiedon eheyden* tarkastamiseksi.

59
julkisen avaimen järjestelmä; **julkisen avaimen infrastruktuuri**
sv infrastruktur för kryptering med öppen nyckel; öppna nyckelns infrastruktur; öppen nyckel-system *n*; infrastruktur för kryptering med publik nyckel; publika nyckelns infrastruktur; publik nyckel-system *n*; PKI
en public key infrastructure; PKI

julkisen avaimen menetelmää hyödyntävä järjestelmä, jolla *varmentaja* tarjoaa ja ylläpitää *varmenteita*

Julkisen avaimen järjestelmässä *varmentaja* tuottaa käyttäjille *salausavaimet*, varmentaa ne *sähköisellä allekirjoituksellaan* ja jakaa ne käyttäjille sekä ylläpitää varmennehakemistoa ja *varmenteiden sulkulistaa* ja mahdollisesti tarjoaa muita varmenteiden käyttöön liittyviä palveluja.

60
varmenne
mieluummin kuin: sertifikaatti
sv certifikat *n*; elektroniskt certifikat *n*; digitalt certifikat *n*
en certificate; digital certificate

sähköinen todistus, jolla vahvistetaan, että todistuksen haltija on tietty henkilö, organisaatio tai järjestelmä

Varmenne on yleensä ulkopuolisen *varmentajan* myöntämä.

Varmenne voi sisältää muun muassa henkilön julkisen avaimen, henkilötiedot, varmenteen voimassaolopäiväyksen sekä varmenteen myöntäjän *sähköisen allekirjoituksen*.

Henkilövarmenne vahvistaa yksityisen henkilön henkilöllisyyden. **Roolivarmenne** vahvistaa sekä henkilön henkilöllisyyden että oikeuden toimia jossakin roolissa, kuten tietyssä työtehtävässä. **Laatuvarmenne** täyttää sähköisistä allekirjoituksista annetussa laissa säädetyt vaatimukset ja sen on myöntänyt säädetyt vaatimukset täyttävä varmentaja. **Palvelinvarmenne** on palvelimelle myönnetty varmenne, jonka avulla henkilö tai tietojärjestelmä voi varmistua siitä, asioiko oikean palvelimen kanssa.

61
varmentaja
mieluummin kuin: varmenneviranomainen
sv certifikatutfärdare; certifikatutgivare; > certifieringsorgan *n*
hellre än: certifieringsmyndighet
en certification authority; certificate authority; CA; certifier; < certification service provider; < CSP

taho, joka myöntää *varmenteen*

Varmentaja voi olla joko luonnollinen henkilö tai oikeushenkilö. Varmentaja voi olla esimerkiksi *luotettu kolmas osapuoli*.

62
varmenteiden sulkulista; **sulkulista**
sv spärrlista; revokeringslista
en certificate revocation list; CRL; < revocation list

luettelo *varmenteista*, jotka *varmentaja* on mitätöinyt niiden voimassaoloaikana

Varmenteiden sulkulistalla oleva varmenne ei ole luotettava.

63
luotettu kolmas osapuoli; **luotettu taho**
sv betrodd tredje part
en trusted third party; TTP; trusted party

taho, johon viestinnän varsinaiset osapuolet tai järjestelmän käyttäjät luottavat

Esimerkiksi viranomainen tai yritys voi luotettuna kolmantena osapuolena todentaa asioinnin osapuolet tai jonkun osapuolista. Vrt. *todentaminen (1)*.

64
salattu yhteys
sv säker förbindelse; krypterad förbindelse
en encrypted connection; secure connection

salausmenetelmällä suojattu tietojärjestelmien välinen yhteys, jossa salataan viestintä

65
virtuaalinen yksityisverkko
sv virtuellt privat nät *n*; virtuellt nät *n*; VPN
en virtual private network; VPN

tietoverkon kautta muodostettu suojattu verkkoyhteys, jossa verkon päätelaitteet toimivat aivan kuin olisivat samassa, muilta tietoverkon käyttäjiltä suljetussa lähiverkossa

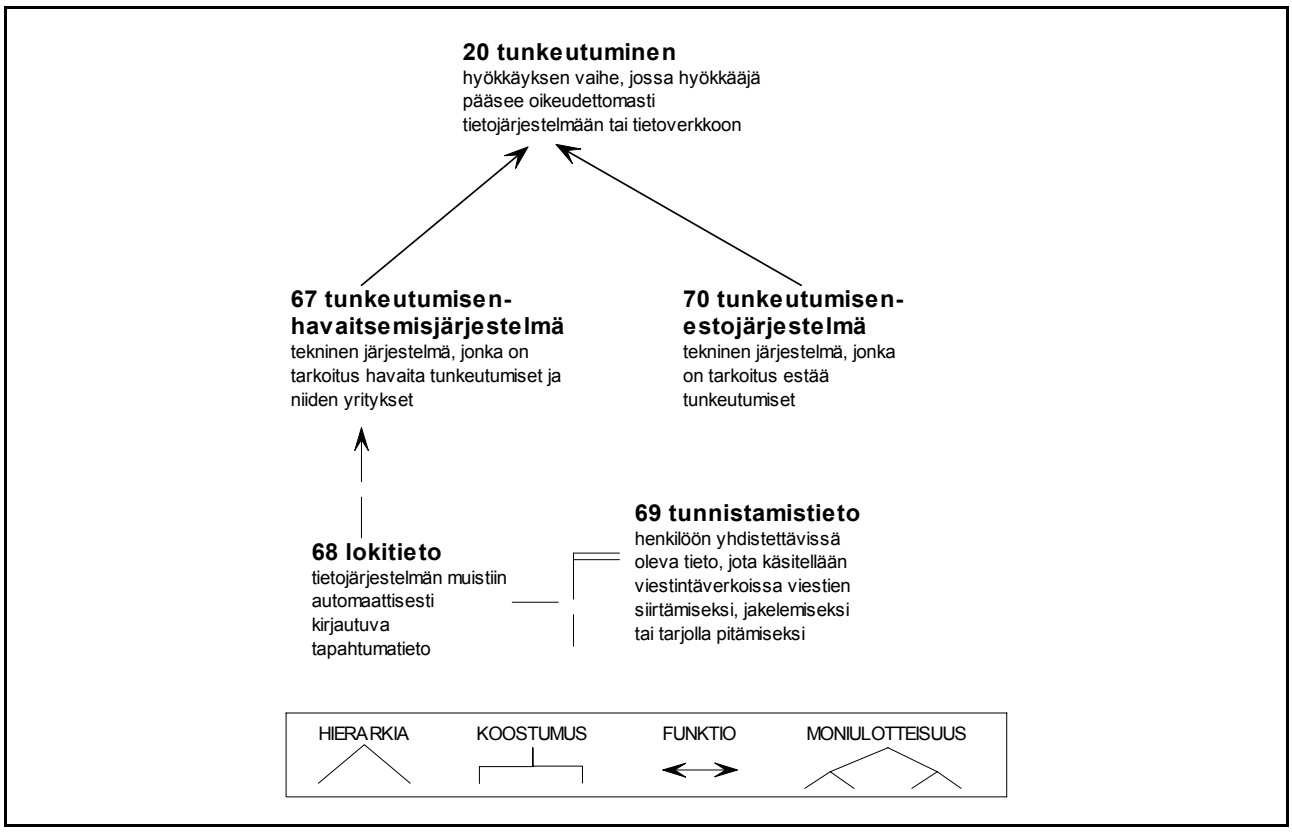
Virtuaalinen yksityisverkko toteutetaan yleensä yleisen tietoverkon, kuten Internetin, kautta *salattuna yhteytenä*. Virtuaalisessa yksityisverkossa käytetään myös erilaisia *pääsynvalvonnan* menetelmiä.

Virtuaalista yksityisverkkoa voidaan käyttää esimerkiksi yrityksen etätyöntekijöiden verkkoyhteyksien suojaamisessa.

66
steganografia; **piilokirjoitus**
sv steganografi
en steganography

tiedon suojauksen menetelmä, jossa tieto piilotetaan niin, ettei sen olemassaoloa huomaa

Tieto voidaan piilottaa muun muassa tekstiin, kuvaan tai äänitallenteeseen esimerkiksi tekijänoikeuden osoittamiseksi.



Kaavio 7. Tunkeutumisen estäminen

67
tunkeutumisenhavaitsemisjärjestelmä
mieluummin kuin: IDS-järjestelmä
sv inträngsdetekteringssystem *n*; IDS
en intrusion detection system; IDS

tekninen järjestelmä, jonka on tarkoitus havaita *tunkeutumiset* ja niiden yritykset

Tunkeutumisenhavaitsemisjärjestelmä voi olla ohjelmisto tai laitteisto tai rakentua näistä molemmista.

68
lokitieto
sv loggdata *pl*
en log data; logged data; log entry

tietojärjestelmän muistiin automaattisesti kirjautuva tapahtumatieto

Lokitieto voi sisältää erilaisia *tunnistamistietoja*. Lokitieto voi koskea muun muassa sitä, kuka järjestelmää on käyttänyt tai miten ja milloin järjestelmää on käytetty. Lokitiedoista voivat selvitä esimerkiksi järjestelmän virhetilanteet, yhteydenotot tietokoneelta Internetiin sekä tietokoneelle Internetistä tulleet yhteydenottopyynnöt.

Lokitietoja voidaan hyödyntää *tunkeutumisenhavaitsemisjärjestelmässä*.

69
tunnistamistieto
mieluummin kuin: teletunnistetieto
sv identifieringsuppgift; identifieringsinformation; identifieringsdata *pl*; identifikationsuppgift; identifikationsinformation; identifikationsdata *pl*
en identification information; identification data

henkilöön yhdistettävissä oleva tieto, jota käsitellään viestintäverkoissa viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi

Viestintäverkoissa välitettävästä viestinnästä tallentuvat tunnistamistiedot voivat liittyä esimerkiksi viestinnän reititykseen, kestoon tai ajankohtaan, siirrettävän tiedon määrään, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon tai yhteyden alkuun, loppuun tai kestoon.

Tunnistamistietojen käsittelyssä pitää huomioida *tietosuoja* ja *tietoturva (1)*.

70
tunkeutumisenestojärjestelmä
sv system *n* för förhindrande av intrång; intrångsförhindrande system *n*; IPS
en intrusion prevention system; IPS

tekninen järjestelmä, jonka on tarkoitus estää *tunkeutumiset*

Tunkeutumisenestojärjestelmä voi olla ohjelmisto tai laitteisto tai rakentua näistä molemmista.

Tunkeutumisen estoon voidaan käyttää paitsi erityistä tunkeutumisenestojärjestelmää myös esimerkiksi *palomuuria*, *virustorjuntaohjelmaa*, *todentamista (1)* tai *salausta*.

71
palomuuri
sv brandvägg
en firewall

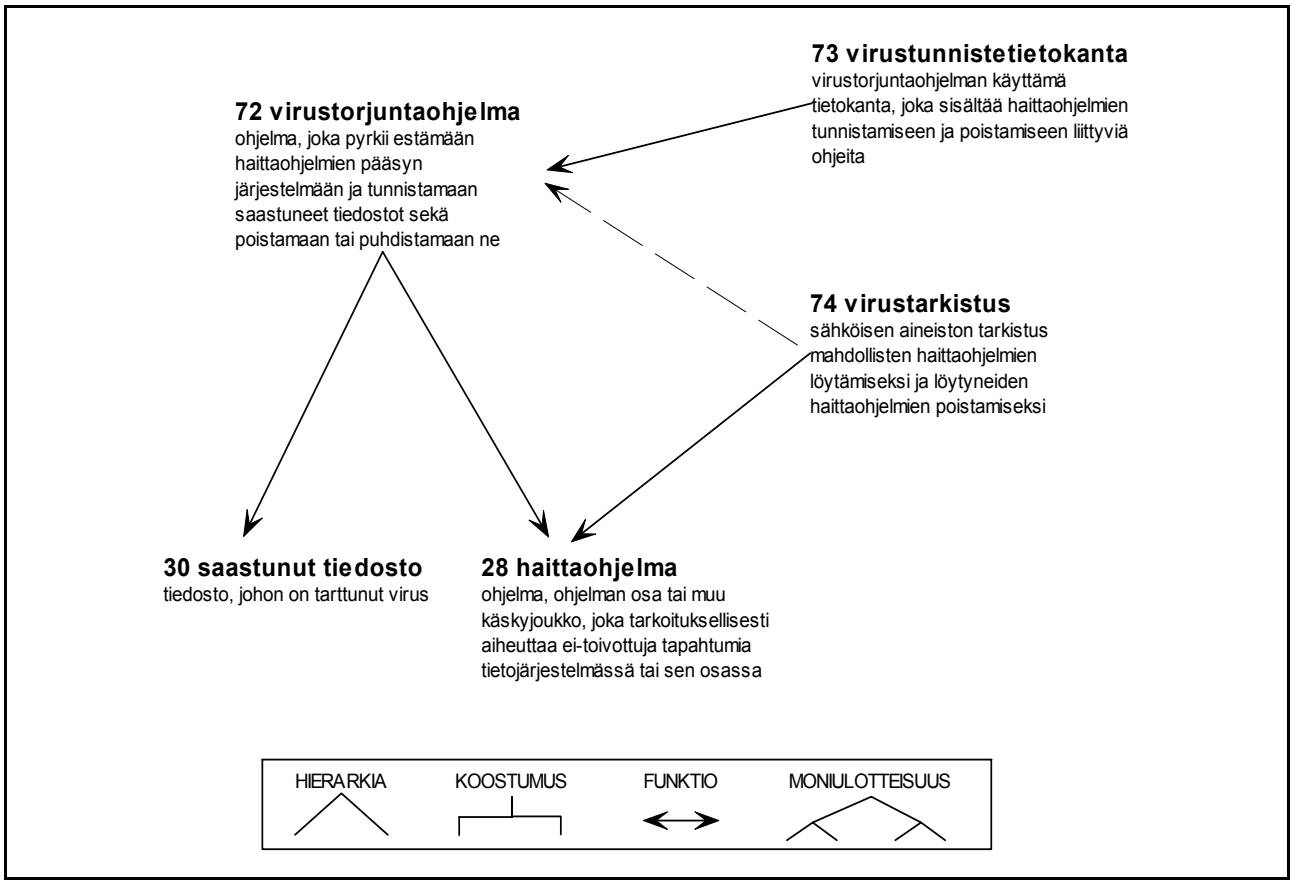
tekninen järjestely, jonka on tarkoitus hallita tietoliikennettä verkosta toiseen tai verkon ja yksittäisen järjestelmän välillä

Palomuuri voi esimerkiksi rajoittaa liikennettä ennalta määriteltyjen sääntöjen mukaisesti, kuten tietyistä osoitteista.

Palomuuri voi olla ohjelmisto tai laite.

Usein palomuuria käytetään Internetin ja esimerkiksi yrityksen lähiverkon välillä.

Henkilökohtaiseksi palomuuriksi kutsutaan palomuuria, joka asennetaan erikseen jokaiseen verkkoon yhdistettyyn koneeseen.



Kaavio 8. Haittaohjelmien torjunta

72
virustorjuntaohjelma
sv antivirusprogram *n*; virusskyddsprogram *n*
en antivirus software; antivirus program; virus scanner; virus protection software; virus scanning software

ohjelma, joka pyrkii estämään *haittaohjelmien* pääsyn järjestelmään ja tunnistamaan *saastuneet tiedostot* sekä poistamaan tai puhdistamaan ne

73
virustunnistetietokanta; **viruskuvaustietokanta**
ei: virustietokanta
sv virusdatabas
en virus description database; virus definition database

virustorjuntaohjelman käyttämä tietokanta, joka sisältää *haittaohjelmien* tunnistamiseen ja poistamiseen liittyviä ohjeita

Virustunnistetietokannan täytyy olla ajan tasalla, jotta virustorjuntaohjelma toimisi riittävän tehokkaasti.

74
virustarkistus
sv viruskontroll
en virus scan; virus scanning

sähköisen aineiston tarkistus mahdollisten *haittaohjelmien* löytämiseksi ja löytyneiden haittaohjelmien poistamiseksi

Virustarkistus voidaan tehdä esimerkiksi *virustorjuntaohjelmalla*.

75
päivitystiedosto
sv uppdateringsfil; < systemuppdatering
en update file

ohjelmiston käyttömahdollisuuksien täydentämiseen tarkoitettu tiedosto

Käyttäjät voivat usein hakea päivitystiedoston käyttöönsä Internetin välityksellä.

76
korjaustiedosto
sv programfix; fix; rättelse; < fixpack
en hot fix; patch file

tietyn ongelman ratkaisuun suunniteltu *päivitystiedosto*

Korjaustiedostoja voidaan suunnitella esimerkiksi *tietoturva-aukon* tai ohjelmavirheen korjaamista varten.

4 TIETOTURVA-ALAN ORGANISAATIOITA

77
tietosuojavaltuutettu
sv dataombudsmannen
en data protection ombudsman

Suomessa viranomainen, jonka tehtävänä on ohjata ja valvoa henkilötietojen käsittelyä kansalaisten yksityisyyden suojaamiseksi sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista, vrt. *yksityisyyden suoja*

78
tietosuojalautakunta
sv datasekretessnämnden
en data protection board

Suomessa valtioneuvoston nimittämä elin, joka käsittelee henkilötietojen käsittelyyn liittyviä periaatteellisesti tärkeitä kysymyksiä ja käyttää päätösvaltaa *tietosuojaan* liittyvissä asioissa

Tietosuojalautakunta voi myöntää rekisterinpitäjille lupia henkilötietojen käsittelyyn ja antaa henkilötietojen käsittelyä koskevia määräyksiä.

79
Viestintävirasto
ei: † Telehallintokeskus; † THK
sv Kommunikationsverket
inte: † Teleförvaltningscentralen; † TFC
en Finnish Communications Regulatory Authority; FICORA
not: † Telecommunications Administration Centre; † TAC

Suomessa sähköisen viestinnän ja tietoyhteiskuntapalvelujen valvontaviranomainen

Viestintäviraston nimi oli 31.8.2001 asti Telehallintokeskus.

80
CERT
sv CERT
en CERT

organisaatio, joka pyrkii havainnoimaan ja ennaltaehkäisemään *tietoturvaloukkauksia* sekä jakamaan tietoa niistä

CERT-organisaatioita on useissa maissa. Keskeinen suomalainen CERT on nimeltään **CERT-FI**, joka kuuluu *Viestintävirastoon*.

CERT on lyhenne sanoista Computer Emergency Response Team.

81
keskusrikospoliisi; **KRP**
sv centralkriminalpolisen; CKP
en National Bureau of Investigation; NBI

Suomen poliisin valtakunnallinen yksikkö, jonka tehtävänä on vastata vakavan rikollisuuden tutkinnasta ja torjunnasta

Keskusrikospoliisi tutkii ja torjuu erityisesti ammattimaista, järjestäytynyttä ja kansainvälistä rikollisuutta. Yksi keskusrikospoliisin pääasiallisista tutkimuskohteista on törkeät *tietotekniikkarikokset*.

82
Tietoturva – Finnish Information Security Association ry (FISA); **Tietoturva ry** (epävirallinen nimi); **TTry** (epävirallinen nimi)
en Finnish Information Security Association (epävirallinen nimi); FISA (epävirallinen nimi)

suomalainen yhdistys, jonka tarkoituksena on muun muassa tukea jäsentensä pyrkimyksiä kehittää ja ylläpitää tietoturvatoiminnan ammattitaitoa ja laatua, edistää *tietoturvaa (1)* ja hyvien tietoturvatapojen noudattamista tietoturvan (1) kaikilla eri osa-alueilla

SUOMENKIELINEN HAKEMISTO

RUOTSINKIELINEN HAKEMISTO / SVENSKT REGISTER

ENGLANNINKIELINEN HAKEMISTO / ENGLISH INDEX