Timo Kiravuo
Markus Peuhkuri
27.1.2012

Lausunto dokumentista "Teknisen ICT-ympäristön tietoturvataso-ohje" versiosta 1.0 25.10.2011

Sivu 6, kuva

Kuvan laidassa oleva "Ydintoiminnan vaatimukset" voisi nostaa "Organisaation tietoturvallisuus" -tekstin sijaan ja tietoturvallisuus-tekstin siirtää kuvan otsikoksi. Olemme törmänneet useamman kerran asenteeseen "tietoturvaa tehdään noudattamalla Vahdin ohjeita, Katakria ja ISO27001:tä". Näkemyksemme mukaan tämä on huono tapa tehdä tietoturvaa ja mielekkäämpää olisi ensin analysoida toiminnan vaatimukset ja sitten katsoa miten ohjeet auttavat toteuttamaan toiminnan vaatimaa tietoturvaa.
Suosituksien ja sopimusten järjestyksen voisi vaihtaa, mikäli kuva pyrkii kuvaamaan näiden tärkeysjärjestystä. Pääsääntöisesti sopimukset ohittavat suositukset.
Organisaation tietoturvallisuus-palkki on syytä ulottaa lepäämään myös ydintoiminnan vaatimusten varassa, nehän ovat tietoturvan perusta, jota ilman tietoturvaa ei olisi mielekästä tehdä. Vielä parempi olisi asettaa ydintoiminnan vaatimukset koko kuvan levyiseksi palkiksi, koska lakeja, sopimuksia ja suosituksia sovelletaan organisaation ydintavoitteen saavuttamiseksi.

1. Johdanto

Edelliseen kommenttiin viitaten, vaikka dokumentti fokusoituu tekniseen toteutukseen, johdannossa olisi hyvä tuoda korostetusti esille, että tietoturvan lähtökohta on organisaation toiminnan tavoitteet ja näitä vastaan kohdistuva uhkakuva. Julkishallinnossa tavoitteet on usein määritelty yleisesti jopa asetustasolla ja tarkempi määrittely löytyy organisaation strategiasta ja muista johtodokumenteista. Uhkakuva ja käsitys siitä "Mitä tapahtuu jos tässä tietojärjestelmässä oleva tieto joutuu ulkopuolisten käsiin/on väärää/ei ole käytettävissä?" ovat usein heikosti hallinnassa. Kun dokumentissa korostetaan myöhemmin tietojärjestelmän omistajan vastuuta, vastuu realisoituu juuri tavoitteiden ja uhkakuvien määrittelyssä. Teknisen ratkaisun toteuttajalla ei oletusarvoisesti ole tätä ymmärrystä eikä välttämättä kykyä tai mahdollisuutta hankkia sitä.
Joten lisäämällä johdantoon esimerkiksi sivulle 7, 2. kappaleen jälkeen "Ohje keskittyy tietoturvallisuutta ylläpitävien teknisten ratkaisujen toteutukseen ja ohjeen käyttö edellyttää laajemman tietoturvasuunnittelun toteutusta ennen teknistä toteutusta." Mahdollisesti myös "Tietoturvallisuuden toteuttamista teknillisissä ratkaisuissa ei voida suorittaa mielekkäästi ja kustannustehokkaasti ilman kuvausta organisaation toiminnan tavoitteista ja uhkakuvista."

Sivu 7, kuva

Kuva korostaa tietoaineiston suojaamista, mutta jättää huomioimatta pääsyn mahdollistamisen. Jos tietoaineisto ei ole saatavilla, se on hyödytöntä.

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574

Sivu 10	Sanastoon: ICT, ratkaisu. Sanastosta voisi lyhentää osaa selityksistä ja tekstikopioista ja jättää vain viittaukset lainsäädäntöön.
s 10, 19	Suojaustasokuvaukset eroavat keskenään vähän ja toistavat toisaan
s 12, kuva	Termejä CRM ja ICT ei ole avattu, tämä heikentää ymmärrettävyyttä. Kuva ei muutenkaan ole kovinkaan helposti ymmärrettävissä. Voisiko näille laittaa nimet ja selittää "Käyttäjän näkemä Outlook-sähköpostipalvelu sisältää myös kalenterin, joten yksi palvelu sisältää kaksi tietojärjestelmää, sähköpostijärjestelmän ja kalenterijärjestelmän. Asiakastietoja sisältävä järjestelmä on erillinen palvelu." Kuvan nuolien merkitys on syytä avata, onko eri palveluiden välillä riippuvuuksia, jotka vaikuttavat suojattaviin kohteisiin Kuvan hyödyllisyyttä lisäisi myös, jos siinä olisi yhteys Internetiin ja kuvattu infrastruktuuripalvelut vaikkapa yhtenä kokonaisuuden toiminnalle välttämättömänä pakettina.
s 13, 1.3	"liitteessä viisi" oletettavasti pitäisi olla "luvussa viisi" (Liite 5 on "järjestelmien väliset riippuvuudet")
s 14, 2.1	Kohta "1) viranomaisen toimintaan liittyvät tietoturvariskit kartoitetaan" on rinnasteinen muiden kohtien kanssa. Tämä vaikuttaa kuitenkin tällä hetkellä olevan olennainen ongelma julkishallinnossa. Teknistä tietoturvaa tehdään sangen usein ilman uhkakuvaa, tai uhkakuva on "Internet on täynnä hakkereita". Mielekkään uhkakuvan muodostaminen on kuitenkin välttämätön edellytys riskianalyysille ja siitä edelleen suojauskeinojen valinnalle. Ohjeistus ja sääntely jättävät edelleenkin paljon tilaa toteutukselle. Tämä tulee esille esimerkiksi jos vertaillaan hätäkeskuslaitosta, jolle tiedon saatavuus on ensisijainen tavoite vaikkapa verohallinnon tiedotuspalveluun, jolle WWW-palvelun toimimattomuus ei ole katastrofi, mutta väärä tieto palvelussa voi aiheuttaa merkittävät taloudelliset vahingot. Dokumentissa ei oteta kantaa jäännösriskin käsittelyyn. Eroavuudet tässä johtavat mahdollisesti eri turvallisuustasoihin organisaatioissa esimerkiksi resurssien eri määrän takia. Sama tietoturvataso ei tarkoista sitä, että jäännösriski on määritelty samalle tasolle.
s 15, kohta 4	Poikkeuksellisten tilanteiden kohdalla on mainittava sairaustapaukset ja lomat. Nämä aiheuttavat nykyään edelleenkin kohtuuttoman määrän tietoturvapoikkeamia. Kun käyttäjätunnuksia ja salasanoja jaellaan ristiin organisaatiossa, muuttuu myös väärinkäytöksien kohdistaminen ja kiistämättömyyden osoittaminen mahdottomaksi. Menetelmänä tässä voi tuoda esille myös oikeuksien ylittämisen kirjaamisen. Järjestelmä erottaa henkilön normaalit hallinnolliset oikeudet poikkeustilanteen vaatimista oikeuksista (esim. sihteerillä on pääsy esimiehen tiedostoihin poikkeustilanteessa) ja poikkeama sallitaan teknisesti, mutta kirjataan myöhempää käsittelyä varten.
s 17, kohta 9	Säännöllinen (vuosittainen) web-pohjainen itsetesti on edullinen tapa jokaiselle työntekijälle tarkistaa oma osaaminen, toimia muistutuksena tietoturva-asioista

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574

sekä tarjota organisaatiolle benchmark-tietoa henkilökunnan tietoturvatietämyksestä. Tämä tulisi olla osa vuosittaista toimintaa työkuvan mukaan räätälöitynä esimerkiksi kehityskeskustelujen yhteydessä.

s 19-21 — Kuvat 5-8 esittävät samaa asia eri kulmilta. Kannattaa kokeilla asioiden esittämistä yhdessä tai korkeintaan kahdessa kuvassa. Esimerkiksi kuvien 5 ja 6 ero ei avaudu. Todennäköisesti paras tapa olisi yhdistää kuvien 7 ja 8 sisältö (salaisempaa tietoa on vähemmän ja suojataan tarkemmin) ja kuvata kuvin 5&6 asua tähän.

s 24, 3.1 — Suojattavien kohteiden määrittämisessä valittaviin kohteisiin voi vaikuttaa myös organisaation käytettävissä olevat resurssit. Vaikka tämä ei ole ensisijainen peruste määrittää suojattavat kohteet tämä piilosyy on myös tunnistettava ja mahdollisuuksien mukaan eliminoitava.

s 25 — Mikä tulkitaan viranomaisen tietoverkoksi: viranomaisen omistama fyysinen yhteys, operaattorilta vuokrattu fyysinen yhteys, operaattorilta vuokrattu siirtoyhteys vai operaattorilta vuokrattu verkkopalvelu? [Onko määritelty Vahti 3/2010 ja miten suhtautuu asetukseen?] Tällä kysymyksellä on käytännön merkitystä, esim. MPLS-VPN ei ole kovinkaan vahva suojaus.

s 26, kuva 9 — Jälleen eri esitystapa kuvassa 2 olevista asioista, onko tarpeen?

s 25 — Jo sanastossa esitellyt suojaustasot kuvataan uudestaan, turhaa toistoa jommassakummassa

s 30, k 14 — Kolme laatikkoa: merkitys organisatiolle, asiakkaalle ja yhteiskunnalle on syytä asettaa rinnakkaisiksi, koska suojattavan kohteen luokittelussa on valittava näistä korkein

s 33 4.2.1 — Tarkentavia kommentteja koko listaan:

- tietoliikennelaitteiden asetusten varmuuskopiointi on myös osa toimivaa konfiguraationhallintaa
- palvelimen ja tietokannan kahdentaminen ei vielä tuo vikasietoisuutta, sana muoto voisi olla "kahdentamiseen perustuvalla vikasietoisella järjestelmällä", kokonaisuuden on tuettava korkeaa käytettävyyttä
- virtuaaliympäristöissä on myös otettava huomioon muut samassa fyysisessä laitteistossa ajettavat palvelut. Voisi todeta että samassa fyysisessä laitteistossa ei saa olla eri turvatasojen palveluita

s 34 — Kohdassa "kiintolevyn salaaminen" on muistutettava että organisaatiolla on oltava pääsy salattuun materiaaliin "key escrown" tai muun vastaavan menettelyn kautta. Esimerkiksi salattu materiaali varmuuskopioidaan säännöllisesti organisaation tietojärjestelmille siten salattuna, että se voidaan avata sopivalla menettelyllä.

s 35 — Esitetty lista teknisistä keinoista ei saata riittää antamaan lukijalle riittävää ymmärrystä ratkaisujen valitsemiseksi. Esim. käynnistysasetukset eivät vaikuta mikäli hyökkääjä pystyy irrottamaan massamuistin laitteesta. Luettelon sijaan voisi kuvata muutaman ratkaisun yksityiskohtaisesti ja viitata alan kirjallisuu-

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574

teen. Keskeinen huomioitava asia on palveluiden tietoliikenteen dokumentointi, minkä avulla voidaan laatia mahdollisimman tarkat pääsylistat.

Luku 4 — Tiedon elinkaaren hallinta tietovarastoissa ja -palveluissa on huomioitava suunnittelussa.

s 37 — Pääteistunto ei kuitenkaan suojaa kehittyneiltä kohdennetuilta hyökkäyksiltä koska hyökkääjä pystyy näkemään kaiken mitä käyttäjäkin sekä tallentamaan käyttäjän syötteet. Erityisesti tulee huolehtia, että käytetty autentikaatiomenetelmä ei mahdollista toistohyökkäystä kuten esimerkiksi perinteinen salasana-autentikaatio. Mikäli autentikaatiotiedot onnistutaan varastamaan, on käytännössä koko tietoaineisto kuitenkin hyökkääjän ulottuvilla. Tätä voidaan vaikeuttaa mutta ei kokonaan eliminoida esimerkiksi päätelaitetunnistuksella.

s 37, 4.2.2. — luvussa 4.2.2. ja 4.3.2 on aiheellista huomauttaa että tietoliikenteen salausavaimia ei tule tallettaa organisaatiolle, koska oman tietoliikenteen avaaminen jälkikäteen ei ole normaalisti tarpeellista, mutta talletettaessa tietoa organisaatiolle on varmistettava pääsy tietovarastoon (joko key escrow tai varmistettava että sama tieto on muualla saatavilla).
Tämän luvun voisi myös jakaa kahtia "salaus tietoa siirrettäessä" ja "salaus tietoa talletettaessa".
Tiedonsiirron salauksesta voisi suoraan listata tässä tai liitteessä yleiset mekanismit kuten TLS, SSH ja IPsec ja mihin kukin soveltuu, sekä viitata niiden asetuksiin, kuten avaimenpituuksiin tai sopivaan lähteeseen aiheesta.

s 37 4.2.3 — Pääteistuntoratkaisun tulee varmistaa luottamuksellisen tiedon suojaamisen lisäksi että tunnistautumistiedot eivät jää koneen muistiin saataville.

s 43, 4.3.4 — Ratkaisussa tulee suosia järjestelyä, missä salassa pidettävää tietoa ei tallenneta etätyöpisteessä olevalle laitteelle. Koska jatkuva ja varmasti toimivia tietoliikenneyhteyksiä ei ole käytettävissä, tulee kannettavissa laitteissa olla mekanismi mikä tuhoaa luotettavasti siihen salattuina tallennetut tiedot mikäli se joutuu vääriin käsiin. Tällöin ei voida luottaa etäyhteyden saamiseen laitteeseen vaan sen on toimittava autonomisesti.
Tähän voidaan vaikuttaa esim. sovellusarkkitehtuurilla, käsitelläänkö tietoa lokaalisti vai palvelimella.

Luku 4.4 — Lisäksi on tietosisältöjen talletusta ulkoistettaessa varmistauduttava tiedon saamisesta takaisin organisaation hallintaan kun sopimuksesta luovutaan tai jos palveluntarjoaja esimerkiksi menee konkurssiin. Myös varmuuskopioinnista on varmistauduttava, kuten Amazonin ja Tiedon viimevuotiset tapaukset osoittivat. Palveluntarjoajan konkurssi saattaa myös vaikuttaa palvelun jatkuvuuteen ja tähän voidaan varautua esim. sopimalla lähdekoodin saamisesta organisaation käyttöön konkurssitapauksessa.

Ulkoistuksessa on huolehdittava myös riittävän sanktiomahdollisuuden olemassa olosta, jolloin rangaistuksen uhka estää niin yritystä kuin yrityksessä työskenteleviä henkilöitä vuotamasta tietoja. Mikäli ulkoistus (tai ulkoistuksen

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574

alihankinan alihankinta) tapahtuu maahan, missä ei ole asianmukaisia tietosuojalakeja, tämä riski on merkittävä.

Ulkoistetut palvelut tarvitsevat usein myös asiakasohjelmiston työasemaan ja näitä ohjelmistoja on päivitettävä. Tällöin työasemassa on ulkopuolisen tahon ylläpitämä ohjelmisto, jota suoritetaan käyttäjän normaaleilla oikeuksilla ja jolla on pääsy työaseman kaikkiin tiedostoihin ja mahdollisuus tietoliikenteeseen. Tämä saattaa muodostaa joissakin tapauksissa kohtuuttoman riskin. Tällaisessa yhteydessä on myös huomattava että toimittajan prosessit ja auditoinnit eivät yleensä suojaa asiakasta ensisijaisesti.

s 49, 1 — Dedikoitu ympäristö - organisaation itse tuottama palvelun etuvertailu. Tämän etu ei useinkaan ole mahdollisuus nopeisiin muutoksiin koska muutoksen tekeminen edellyttää usein laitehankintoja sekä niiden käyttöönottoja mikä on huomattavasti hitaampaa pilvipalveluun verrattuna.

s 50 — Mitä ovat "ns. Hyppykoneet- ja palvelimet"?

s 54 — Sosiaalisen median palveluita hyödynnettäessä on myös huomioitava niihin sisältyvä tekeytymismahdollisuus. Esimerkiksi miltä näistä sivustolta löytää tietoja säteilytilanteesta Suomessa http://i.imgur.com/5sSZs.png ? Viranomaisen palvelujen saatavuudesta on pidettävä huolta ja viranomaisen omassa hallinnassa olevien sivustojen tulee olla ensisijainen viestintäkanava. Viranomaisen tiedotuspalvelun on myös oltavissa selvästi tunnistettavissa viranomaisen tiedotuspalveluksi ja sen on erottava muusta viestinnästä. Viranomaisen roolista riippuen julkinen www-palvelin voi siis olla korkean tason palvelu nimenomaan saatavuuden osalta. Sosiaalisen median palveluita voidaan käyttää lisäksi apuna tiedon jakeluun, mutta ensisijainen lähde ne eivät voi olla.

s 54 — Pilvipalveluista on syytä huomioida myös Googlen palvelut, kuten gmail, kalenterit ja Docs (jota käytetään usein yhteistyökaluna ja johon talletetaan tietoa) ja Microsoftin vastaavat

s 59 ja 61 — Kuvat 26 ja 28 eivät eroa toisistaan tämä kannattaa todeta kuvatekstissä ("eri turvatasojen vaatimat ratkaisut saattavat olla identtisiä") tai esittää kuvissa eroavat ratkaisut

Koko dokumentti

Käytettäessä värejä kuvissa ja Exel-lomakkeissa on syytä huomioida esteettömyys ja esim. LVM:n esteettömyysohjelma: http://www.lvm.fi/web/fi/julkaisu/view/1225363 On myös hyvä olettaa että kaikilla ei ole käytettävissä väritulostinta ohjeen tulostukseen.

Osa kuvista on vaikealukuisia ja tyyli epäyhtenäinen, näihin voisi ehkä käyttää graafikkoa?

Teksti käyttää paikoitellen sinä-muotoa ja passivia. Aktiivinen tekstimuoto jossa toimijana on organisaatio tai sen toimijat olisi suositeltavampi.

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574

Tiedon elinkaari on käsitelty 2/2010:ssä, mutta sitä ehkä olisi hyvä avata mitä se tarkoittaa ict-järjestelmien kannalta.

Onko jossain dokumentissa mainittu taustastandardeja ja -malleja mihin Tietoturvataso-malli perustuu (CCM-SSE etc.)? Tämä voisi helpottaa valtiohallinnon ulkopuolelta tulevien asiantuntijoille TTT:n omaksumista.

Aalto-yliopisto
ComNet
timo.kiravuo@aalto.fi

Postiosoite
PL 13000
00076 AALTO

Käyntiosoite
Otakaari 5
Espoo

Puhelin 09 470 26221
Faksi 09 470 22474
Y-tunnus 2228357-4

www.aalto.fi
Kotipaikka Helsinki
VAT FI22283574