Tampereen ammattikorkeakoulu

Turvallisuusluokitellut ympäristöt ja yhdyskäytäväratkaisut

Jukka Viertola

OPINNÄYTETYÖ
Marraskuu 2023

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

VIERTOLA, JUKKA:
Turvallisuusluokitellut ympäristöt ja yhdyskäytäväratkaisut

Opinnäytetyö 43 sivua, joista liitteitä 2 sivua
Marraskuu 2023

Opinnäytetyössä esitellään aluksi turvallisuusluokat määritelmineen, perusteet turvallisuusluokkien olemassaololle sekä tarpeet turvallisuusluokitelluille ympäristöille. Laki määrää viranomaisia, tuomioistuimia ja valitusasioita käsitteleviä lautakuntia luokittelemaan käsittelemänsä asiakirjat.

Työn painopiste on turvallisuusluokiteltuihin ympäristöihin kohdistuvien vaatimusten käsitteleminen ulkoministeriön julkaisemaan Katakri 2020 -teokseen viitaten. Katakrin käsittely on jaettu sen osa-alueiden mukaan: turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus. Osa-alueet esitellään ensiksi Katakrin kautta ja sen jälkeen yleisellä tasolla. Osa-alueita ei käydä läpi kohta kohdalta, vaan tehdään valittuja poimintoja lukijan kannalta tärkeimmistä ja mielenkiintoisimmista kohdista. Tavoitteena on luoda lukijalle yleisellä tasolla esitettävien esimerkkien kautta helposti lähestyttävä näkökulma Katakrin vaatimuksiin, mahdollistaen näiden käytön tietoturvan parantamiseksi muissakin kuin turvallisuusluokitelluissa ympäristöissä.

Viimeisessä varsinaisessa osiossa esitellään Katakrissa mainittuja yhdyskäytäväratkaisuja niissä käytettyjen laitteiden kautta. Yhdyskäytävä yhdistää tietoverkon toiseen toimien liikenteen solmukohtana näiden välillä. Verkon yhdyskäytävä voi sisältää yhden tai monissa tapauksissa useamman yhdyskäytävälaitteen muodostaen yhdyskäytäväratkaisun. Esiteltävät yhdyskäytävälaitteet ovat palomuuri, reititin, VPN ja datadiodi. Näiden osalta kuvataan ensiksi laitteiden toimintaperiaatteita lyhyesti, jonka jälkeen esitellään niiden käyttötarkoitusta osana yhdyskäytäväratkaisua toteutusesimerkkeineen yleisellä tasolla. Esimerkit ovat laadittu mukailemaan Katakrin vaatimuksia sekä tuomaan konkretiaa näiden mahdolliseen toteuttamiseen lukijan omassa ympäristössä.

Asiasanat: Katakri, turvallisuusluokka, yhdyskäytäväratkaisu

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

VIERTOLA, JUKKA:
Security Classified Environments and Gateway Solutions

Bachelor's thesis 43 pages, appendices 2 pages
November 2023

This thesis introduced the concepts of security classifications, the reasons for them and the demands for security classified environments. The requirements originate from the Finnish legislation, and they apply to the authorities, courts and boards dealing with appeals, mandating them to classify the documents they handle.

The emphasis of this thesis was on the requirements for security classified environments, as referred in the Katakri 2020 publication by the Finnish Ministry for Foreign Affairs. The chapter addressing Katakri was divided into its subchapters as introduced in the original publication: security management, physical security, and technical information security. Each subchapter first introduced its topic through Katakri, followed by a generalized overview of the subject.

The last part of this thesis introduced gateway solutions mentioned in Katakri 2020. A gateway connects a computer network to another, serving as a node for traffic to flow through. The network gateway may consist of one or multiple gateway devices, forming a gateway solution. The presented gateway devices in this chapter included firewalls, routers, VPN-devices, and data diodes. The operational principles of the devices were first briefly described, followed by an introduction to their purpose as part of a gateway solution.

Key words: katakri, security classification, gateway solution

SISÄLLYS

ERITYISSANASTO tai LYHENTEET JA TERMIT (valitse jompikumpi)

AAA	(eng. Authentication, authorization, and accounting) Pääsynhallintaan liittyvä käsite
CISA	(eng. Cybersecurity & Infrastructure Security Agency) Yhdysvaltojen valtion virasto
IDS	(eng. Intrusion Detection System) Laitteisto tai ohjelma joka etsii verkosta vahingollista toimintaa
IP	Internet Protokolla. Työssä tarkoitetaan IPv4 ellei toisin mainita.
IPS	(eng. Intrusion Prevention System) Laitteisto tai ohjelma joka etsii verkosta vahingollista toimintaa ja reagoi sen pysäyttämiseksi
Katakri	Kansallinen turvallisuusauditointikriteeristö
MFA	(eng. Multi-Factor authentication) Monivaiheinen tunnistautuminen
OSI-malli	(eng. Open Systems Interconnection model) Kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
TCP	(eng. Transmission Control Protocol) Yhteydellinen tietoliikenneprotokolla luotettavaan tiedonsiirtoon.
TL	Turvallisuusluokka
UDP	(eng. User Datagram Protocol) Yhteydetön tietoliikenneprotokolla.

1 JOHDANTO

Työssä käsitellään turvallisuusluokiteltuja ympäristöjä Suomessa viranomaisten määritysten mukaisesti. Tämän lisäksi käsitellään erilaisia yhdyskäytäväratkaisuja ja tekniikoita yleisesti. Turvallisuusluokiteltuja ympäristöjä käsitellään pääasiassa teknisten tietoturvallisuuden vaatimusten näkökulmasta. Tekninen tietoturvallisuus koostuu tietojärjestelmien, päätelaitteiden ja IP-verkkojen turvallisuusvaatimuksista. Yhdyskäytäväratkaisut ovat tapoja liikennöidä näistä verkoista sisään ja ulos tai niiden välillä. Yhdyskäytäviä voi olla myös verkon sisällä rajaamassa pääsyä verkon sisäpuolella.

Työn aihe on valittu kiinnostuksesta turvallisuusluokiteltuihin tietojenkäsittely-ympäristöihin ja näiden vaatimuksiin. Katakrin esittelemiä vaatimuksia ja toteutusesimerkkejä on mielenkiintoista suhteuttaa todellisiin ympäristöihin, niin turvallisuusluokiteltuihin kuin luokittelemattomiinkin. Varsinkin jälkimmäisten osalta on mielenkiintoista miettiä, mitkä vaatimukset voisivat tuoda lisäturvaa näiden suojaamiseen.

Työn tavoitteena on koota saatavilla olevista viranomaislähteistä yleiskuva turvallisuusluokiteltuihin ympäristöihin ja vertailla eri turvallisuusluokkien vaatimuksia keskenään. Pääasiallinen lähde ja vertailun jaottelun lähde on ulkoministeriön julkaisema Katakri 2020. Vaatimuksia käsitellään työssä ainoastaan kansallisen tiedon näkökulmasta, eikä kansainvälisen tiedon käsittelyyn liittyvistä vaatimuksista. Työssä esiteltävät yhdyskäytäväratkaisut liittyvät Katakrin vaatimuksiin, ja ne on valittu käsitteiden ymmärtämiseksi. Näiden osalta on vaatimuksiin viittaamisen lisäksi esitelty yleisimpiä käyttötapauksia turvallisuusluokittelemattomiin ympäristöihin.

Kaikkia vaatimuksia ei käydä kohta kohdalta läpi, vaan työssä nostetaan esille niitä kohtia, jotka ovat tietoturvallisuuden kannalta mielenkiintoisimpia tai tärkeimpiä. Vaikka työ keskittyy turvallisuusluokiteltuihin verkkoihin viranomaisvaatimusten kautta, voidaan sitä hyödyntää myös muiden, luokittelemattomien verkkojen ja ympäristöjen suunnittelussa ja tietoturvan sisäisessä itseauditoinnissa. Tämä työ ei pyri olemaan täydellinen tietoturvan itsearvioinnin apuväline, vaan pikemminkin ohjeistus löytämään uusia näkökulmia sekä ohjaamaan viitattujen lähteiden pariin.

Lukija voi tätä työtä lukiessaan miettiä, miten oma tietojenkäsittely-ympäristö vertautuu turvallisuusluokiteltujen ympäristöjen vähimmäisvaatimuksiin.

2 TURVALLISUUSLUOKAT

Tässä luvussa esitellään turvallisuusluokkien määritelmä. Määritelmä on tärkeä ymmärtää, koska sillä on vaikutusta myöhemmin käsiteltävän Katakrin [(1), ulkoministeriö] vaatimusten kannalta. Lisäksi esitellään mistä tarve turvallisuusluokille tulee, sekä miten turvallisuusluokitus voidaan määrittää tietojenkäsittely-ympäristölle.

2.1 Määritelmä Suomen lainsäädännöstä

Tarve tietoaineistojen luokittelulle valtionhallinnossa turvallisuusluokkien mukaan on kirjattu Suomen lakiin. Julkisen hallinnon tiedonhallinnasta annetun lain 2019/906, jäljempänä tiedonhallintalaki, 18 § velvoittaa viranomaisia, tuomioistuimia ja valitusasioita käsittelemään perustettuja lautakuntia turvallisuusluokittelemaan ja merkitsemään käsittelemänsä asiakirjat. Tiedonhallintalain 18 §:ään on kirjattu turvallisuusluokan merkitsemisestä: ”Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.” Turvallisuusluokan merkitsemisen tulee osoittaa, mitä tietoturvallisuustoimenpiteitä asiakirjan käsittelyssä on noudatettava. Turvallisuusluokiteltujen asiakirjojen käyttöön ja merkitsemiseen liittyvät toimenpiteet säädetään tarkemmin valtioneuvoston ajankohtaisella asetuksella. [(2), tiedonhallintalaki]

2.2 Valtioneuvoston säädökset

Valtioneuvoston asetuksen 28.11.2019/1101 3 §:n mukaan turvallisuusluokat voidaan jakaa tasoihin I – IV. Turvallisuusluokka I on kaikista korkein suojaustaso. Suojaustasojen määritelmä tulee tietohallintolaista. [(3), valtioneuvosto]

TAULUKKO 1. Turvallisuusluokkien määritelmät.

Suojaustaso	Merkintätavat	Määritelmä tietohallintolain 18 §:ssä
Turvallisuus-luokka I	ERITTÄIN SALAINEN TL I	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa.
Turvallisuus-luokka II	SALAINEN TL II	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa.
Turvallisuus-luokka III	LUOTTAMUK-SELLINEN TL III	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa.
Turvallisuus-luokka IV	KÄYTTÖ RAJOITETTU TL IV	Asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa.

Valtioneuvoston “suositus turvallisuusluokiteltavien asiakirjojen käsittelystä” julkaisu esittää seuraavat turvallisuusluokkien merkitsemiseen suositellut mallit. [(4), valtiovarainministeriö]

Näiden lisäksi on olemassa vielä erillinen “salassa pidettävä” -leima ilman erillistä turvallisuusluokan tasoa, jota käytetään muun muassa julkisuuslaissa määritellyn

salassa pidettävän tiedon kanssa. Tietoja turvallisuusluokkien tarkemmasta määrityksestä ja turvallisuusluokiteltujen aineistojen merkitsemisestä löytyy valtiovarainministeriön ajantasaisista ohjeistuksista [(5), valtiovarainministeriö].

2.3 Tarkastus ja hyväksyntä

Yrityksen järjestelmä tai käyttöympäristö vaatii toimivaltaisen viranomaisen hyväksynnän ennen kuin siellä voidaan käsitellä tai säilyttää turvallisuusluokiteltua tietoa. Tarve käyttöympäristön hyväksynnälle voi tulla eteen esimerkiksi, kun viranomainen on tekemässä yrityksen kanssa sopimusta, jonka yhteydessä yritykselle luovutetaan viranomaisen luokiteltuja asiakirjoja. Turvallisuusselvityslaki määrittää toimivaltaiset viranomaiset yritysturvallisuusselvityksessä ja sen osa-alueiden tarkastuksessa. [(6), turvallisuusselvityslaki]

Hyväksynnässä kiinnitetään huomiota kohdeorganisaatioon henkilöstö-, yritys- (T) ja toimitilaturvallisuuden (F) sekä tietojärjestelmien ja tietoliikennejärjestelyiden turvallisuuden (I) osa-alueilta. Suluissa olevat merkinnät ovat viittauksia Katakrin kappaleisiin. T- ja F-osien osalta kansallista yritysturvallisuusselvitystä tehtäessä toimivaltainen viranomainen on Suojelupoliisi tai Pääesikunta, ja I-osassa Liikenne- ja viestintävirasto. Katakri on viranomaisauditointeja varten luotu työkalu, ja sen käytöstä kerrotaan tarkemmin luvussa 3.

Hyväksynnän edellytyksinä on tarkastuksen kohteen sitoutuminen turvallisuuden tason ylläpitämiseksi myös tarkastuksen jälkeen. Hyväksynnän voimassaolo voi myös raueta ennen aikojaan, mikäli kohteessa tapahtuu merkittävä turvallisuuteen vaikuttava muutos.

Liikenne- ja viestintäviraston hyväksyntäprosessi tietojärjestelmälle on nähtävillä liitteessä 1.

3 KATAKRI

Luvussa 3 käsitellään turvallisuusluokkien välisiä eroja Katakrin osa-alueiden kautta. Tämän lisäksi nostetaan kohtia esille, joita voidaan pitää yleisesti merkittävimpinä muidenkin kuin turvallisuusluokiteltujen ympäristöjen ja tietojärjestelmien suojaamiseksi. Nostojen tarkoitus on tuoda konkretiaa Katakrin kohtien ja oman ympäristön arvioinnin välille eri näkökulmista.

3.1 Katakri viranomaisen auditointityökaluna

Katakri eli kansallinen turvallisuusauditointikriteeristö on tietoturvallisuuden auditointityökalu. Se sisältää kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset viranomaisen salassa pidettävän tiedon käsittelemiseksi, ja siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön sekä kansainvälisiin turvallisuusvaatimuksiin. Katakriin koottujen vaatimusten lähteinä ovat laki julkisen hallinnon tiedonhallinnasta (906/2019) sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019).

Katakrin käytöllä auditoiva viranomainen sekä auditoitava kohdeorganisaatio voivat pyrkiä varmistamaan, että jälkimmäisen turvallisuusjärjestelyt ovat riittävällä tasolla kaikissa niissä ympäristöissä, joissa viranomaisen salassa pidettäviä tietoja käsitellään.

Ensimmäinen Katakri valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Katakrin ylläpito ja hallinnointi on vuodesta 2014 eteenpäin kuulunut ulkoministeriössä toimivalle kansalliselle turvallisuusviranomaiselle (NSA). Uusin Katakri on julkaistu vuonna 2020. [(1), ulkoministeriö]

Katakri on jaettu kolmeen osa-alueeseen:

- Osa-alue T: Turvallisuusjohtaminen sisältää hallinnon tietoturvallisuuden ja henkilöstöturvallisuuden.
- Osa-alue F: Fyysinen turvallisuus kattaa yleiset fyysisen turvallisuuden vaatimukset, turvallisuusalueiden vaatimukset sekä tietoaineistoturvallisuuden vaatimukset.
- Osa-alue I: Tekninen tietoturvallisuus sisältää tietoliikenneturvallisuuden, tietojärjestelmäturvallisuuden ja käyttöturvallisuuden kappaleet.

Luvuissa 3.2–3.4 nostetaan esille Katakri 2020 -julkaisun kolmen osa-alueen vaatimusten eroavaisuuksia eri turvallisuusluokkien välillä kansallisen tiedon näkökulmasta. Tämän lisäksi tuodaan esille yleisesti tärkeimpiä kohtia, joita olisi tärkeää noudattaa muissakin kuin viranomaisen auditoimista ympäristöistä, esimerkiksi oman yrityksen turvallisuustoimien itsearvioinnissa.

3.2 Osa-alue T: Turvallisuusjohtaminen

Turvallisuusjohtamisen luvussa käsitellään Katakrin T-osa-aluetta Katakrin näkökulmasta sekä yleisellä tasolla. Osa-alue kattaa hallinnollista ja henkilöturvallisuuteen liittyviä näkökulmia. Turvallisuusjohtamisen osa-alue esitellään hyvin pintapuolisesti, sillä tämän työn kannalta se on vähiten kiinnostava.

3.2.1 Turvallisuusjohtaminen Katakrista

Katakrin Tuvallisuusjohtamisen osa-alue käsittelee pääosin tietoturvaan ja yleisesti turvallisuuteen liittyviä hallinnollisia vastuita, vastuiden jakoa, riskienhallintaa ja henkilöstön ohjeistuksia. Osa-alue pitää sisällään 13 kohtaa, joiden alle on listattu näiden osalta Suomen lakiin perustuvat vaatimukset salassa pidettävän tiedon käsittelemiseksi. Turvallisuusjohtamisen kohdat T-01 – T-13 Katakri 2020 -julkaisussa ovat:

- T-01 – Johdon tuki, ohjaus ja vastuu – turvallisuusperiaatteet
- T-02 – Turvallisuustyön tehtävien ja vastuiden määrittäminen
- T-03 – Tietoturvallisuusriskien hallinta
- T-04 – Turvallisuusohjeistus
- T-05 – Turvallisuustyön resurssit

- T-06 – Toimintahäiriöt ja poikkeustilanteet
- T-07 – Turvallisuuspoikkeamien hallinta
- T-08 – Tietojen luokittelu
- T-09 – Työsuhteen aikaiset muutokset turvallisuusluokiteltujen tietojen käsittelyssä
- T-10 – Henkilöstön luotettavuuden arviointi
- T-11 – Salassapito- ja vaitiolovelvollisuus
- T-12 – Turvallisuuskoulutus
- T-13 – Tiedonsaantitarve ja käsittelyoikeudet

Vaatimuksia voi olla yksi tai enemmän per kohta. Esimerkiksi kohdan T-11 Salassapito- ja vaitiolovelvollisuus alle on listattu yksi vaatimus, jonka täyttymiseksi turvallisuusluokiteltua tietoa käsittelevälle henkilölle tulee selvittää tietojen suojaamista koskevat turvallisuusvelvoitteet, sekä hänen on tuotava ilmi tietoisuus häntä koskevista vastuistaan tietojen suojaamiseksi. Useimmin tämä vaatimus toteutetaan salassapitosopimuksen allekirjoittamisella.

Turvallisuusjohtamisen osa-alueessa melkein kaikki vaatimukset ovat samoja turvallisuusluokista riippumatta. Ainoastaan kohta T-13 Tiedonsaantitarve ja käsittelyoikeudet listaa eroavan vaatimuksen: Organisaation on pidettävä ajantasaista luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan II tai III tietoja.

3.2.2 Turvallisuusjohtaminen yleisellä tasolla

Jos Turvallisuusjohtamisen osa-aluetta käytetään organisaation itseauditoinnin apuna ilman lain määräämiä velvoitteita tietojen käsittelystä, yleisesti tärkeimpänä ja eniten tietoturvaa parantava kohtana voidaan pitää T-02: Turvallisuustyön tehtävien ja vastuiden määrittäminen. Kohdan vaatimus kuuluu ”organisaatio on määritellyt tietoturvallisuuden hoitamisen tehtävät ja vastuut”. Tämän yksiselitteisen kohdan tarkoitus on määrittää turvallisuuden keskeisimpiin osa-alueisiin tekijät, heidän valtuutensa ja vastuunsa. Katakri tarkentaa, että vastuut tulisi määritellä erityisesti tietoturvallisuusohjeiden ylläpidosta, riskienhallinnasta, varautumisesta sekä tietoturvallisuuden kokonaisvastuussa olevasta henkilöstä.

Toinen turvallisuusjohtamisen kaikkiin organisaatioihin yleispätevä kohta on T-04: Turvallisuusohjeistus. Tätä kohtaa voi soveltaa myös turvallisuusluokittelemattoman tiedon käsittelyssä. Jos T-02 kohdan esimerkin mukaisesti turvallisuusohjeiden ylläpidolle on määritetty vastuulliset ja ohjeet ovat sekä ajan tasaisia että saatavilla, voidaan vaikuttaa siihen, ettei turvallisuuden kannalta keskeiset asiat ja niiden soveltaminen ole henkilöriippuvaista. Ilman yhtenäistä turvallisuusohjeistusta voi syntyä helposti väärinkäsityksiä, miten ja missä yrityksen tai sen asiakkaiden tietoja voidaan käsitellä.

Katakrin kohdan T-13: tiedonsaantitarve ja käsittelyoikeudet voidaan nähdä olevan yleiskäyttöinen ja varteenotettava ihan kaikissa ympäristöissä. Kohta listaa vaatimuksia liittyen henkilöstön oikeuksiin eri turvallisuusluokan tietoihin ja näiden kirjanpidolliseen ylläpitoon. Yleisellä tasolla ajateltuna voi syntyä riski, jos yrityksessä ei ole mietitty ja luokiteltu tietoja tiedonsaantitarpeen mukaan. Esimerkki tällaisesta voisi olla, ettei yrityksen henkilöstöosaston tietoja ole rajoitettu käsittelytarpeen mukaan, vaan näihin on kaikilla pääsy.

3.3 Osa-alue F: Fyysinen turvallisuus

Fyysisen turvallisuuden luvussa käsitellään tietojen fyysistä turvaamista käsittelyympäristössä, säilytysympäristössä ja näiden ulkopuolella. Luku 3.3.1 käsittelee aihepiiriä turvallisuusluokkien näkökulmasta Katakrin kautta ja 3.3.2 yleisellä tasolla.

3.3.1 Fyysinen turvallisuus Katakrista

Katakrin osa-alue F: Fyysinen turvallisuus koostuu kahdeksasta vaatimuksesta ja niiden soveltamisesta. F-osion kohdat F-01 – F-08 alakohtineen ovat järjestyksessä seuraavat:

- F-01 – Fyysisten turvatoimien tavoite
- F-02 – Fyysisten turvatoimien riskien arviointi
- F-03 – Fyysisten turvatoimien valinta (monitasoinen suojaus)
- F-04 – Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella
- F-05 – Hallinnollinen alue

    - F-05.1 – Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)
    - F-05.2 – Pääsyoikeuksien myöntäminen
    - F-05.3 – Vierailijat
    - F-05.4 – Äänieristys
    - F-05.5 – Tunkeutumisen ilmaisujärjestelmät
    - F-05.6 – Salaa katselun estäminen
    - F-05.7 – Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)
    - F-05.8 – Tiedon käsittely ja säilyttäminen
- F-06 – Turva-alue
    - F-06.1 – Alueen raja ja rakenteet (seinät, ovet ja ikkunat sekä lattia- ja kattorakenteet)
    - F-06.2 – Kulunvalvonta
    - F-06.3 – Pääsyoikeuksien myöntäminen
    - F-06.4 – Vierailijat
    - F-06.5 – Turvallisuusohjeet
    - F-06.6 – Äänieristys
    - F-06.7 – Tunkeutumisen ilmaisujärjestelmät
    - F-06.8 – Salaa katselun estäminen
    - F-06.9 – Tila- ja laitetarkastukset (ainoastaan TL II / EU-S)
    - F-06.10 – Tiedon käsittely ja säilyttäminen
- F-07 – Teknisesti suojattu turva-alue
- F-08 – Tietoaineistoturvallisuus
    - F-08.1 – Tietojen välitys postilla ja kuriirilla
    - F-08.2 – Turvallisuusluokiteltujen tietojen kopioiminen
    - F-08.3 – Turvallisuusluokiteltujen tietojen kirjaaminen
    - F-08.4 – Ei-sähköisten tietojen tuhoaminen

Katakrin F-osio käsittelee tietojen suojaamiseksi vaadittavia fyysisiä toimia. F-osio on jäsennelty kahdentyyppisiin turvallisuusalueisiin ja näiden eroavaisuuksiin: hallinnollisiin alueisiin (F-05) sekä turva-alueisiin (F-06). Hallinnolliset alueet ovat tavalliseen työskentelyyn tarkoitettuja alueita, esimerkiksi toimistotiloja. Hallinnollisella alueella tulee olla selkeästi määritetyt näkyvät rajat ja alueelle pääsy on rajoitettu viranomaisen valtuuttamilla henkilöillä. Turva-alueet ovat hallinnollisia alueita tarkemmin suojattuja työskentelytiloja, joissa turvallisuusluokiteltuja

tietoja käsitellään ja säilytetään. Turva-alueilla kulkua sisään ja ulos tulee valvoa kulkuluvilla tai henkilökohtaisesti tunnistamalla. Lisäksi alueelle pääsy ilman saattajaa tulee olla rajattu henkilöihin, joiden luotettavuus on varmistettu ja joilla on erikseen myönnetty lupa tulla alueelle.

Fyysisten turvatoimien tavoite kuvataan ensimmäisessä osiossa F-01. Tavoite on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin säilyttämällä ja käsittelemällä näitä asianmukaisesti, varmistaa ketkä pääsevät näihin turvallisuusselvitysten mukaisesti käsiksi, ehkäistä ja havaita luvattomat toimet sekä estää ja viivästyttää muiden kuin oikeutettujen pääsy tunkeutumalla käsiksi tietoihin. Fyysisten turvatoimien tavoite tulee täyttyä ennen turvallisuusalueiden hyväksyntää.

Fyysisten turvatoimien tavoitteen määrittämisen jälkeen tulee riskien arviointi (F-02), jonka perusteella valitaan fyysiset turvatoimet (F-03 – F-04) sekä toteutetaan turvallisuusalueiden vähimmäisvaatimukset (F-05 – F-07). Fyysisten turvatoimien riskien arvioinnissa tulee huomioida sekä auditoivan että auditoitavan tahon näkemykset riskeistä, valituista turvatoimista sekä hyväksyttävästä jäännösriskistä.

Liitteessä 2 on taulukko kansallisen turvallisuusluokitellun tiedon käsittelystä ja säilytyksestä turvallisuusluokissa TL II – TL IV turvallisuusalueiden ulkopuolella, hallinnollisella alueella ja turva-alueella. Tässä huomion arvoista ovat erot tiedon säilytykseen liittyen.

3.3.2 Fyysinen turvallisuus yleisellä tasolla

Katakrin F-osion merkitys yleisellä tasolla turvallisuusnäkökulmiin on helposti nähtävissä yrityksen toimialasta riippumatta. Fyysisten turvatoimien riskien arviointi on hyvä olla jokaisella yrityksellä fyysisten turvatoimien valinnan lähtökohtana. Mitä suuremman riskin fyysinen tunkeutuminen voi aiheuttaa, sitä paremmin sitä vastaan tulisi varautua. Monitasoisella fyysisellä suojauksella, joka ottaa käyttöön joukon toisiaan täydentäviä turvatoimia, on mahdollista saavuttaa parempi suojautuminen kuin vähimmäistason suojauksella. Suojauksen tasojen lisääminen sekä ylläpito aiheuttaa kiinteitä ja jatkuvia kustannuksia, joten turvatoimien valinnassa kannattaa käyttää riskiarviota.

Monitasoisen fyysisen suojaamisen kokonaisuus koostuu useista tekijöistä. Fyysiseen alueen rajaamiseen liittyvät esimerkiksi aidat, seinät, ikkunat, lattiat ja kattorakenteet. Näiden tarkoitus on estää sivullisten pääsy fyysisesti suojatun alueen sisäpuolelle. Näiden osalta oleellisinta on tuntea heikoin kohta, sillä tunkeutuja pyrkii pääsemään sen kautta sisälle. Tästä syystä koruliikkeiden näyteikkunoissa on nähtävillä usein kalterit vahvistamassa muuten heikointa rakennetta. Ulkorajojen heikkouksia voidaan jossain määrin vahvistaa alueen sisäisillä rajoilla, kuten kulkurajoitetuilla ovilla, holveilla tai kassakaapeilla.

Yksi keino millä voi parantaa lähes jokaisen yrityksen fyysistä turvallisuutta on pohtia, voisiko tiedon säilytykseen ja käsittelyyn liittyviin käytäntöihin ottaa Katakrista mallia. Tiedon luokitteluun perustuvat ohjeistukset yrityksen tietojen käsittelystä voivat selkeyttää työntekijöille, mitkä tiedot ovat tärkeimpiä pitää ulkopuolisten ulottumattomissa. Esimerkiksi yrityssalaisuuksia sisältävät tekniset piirustukset ovat tarpeen säilyttää käsittelyn ulkopuolella paremmassa suojassa kuin yrityksen sisäiset, ulkopuoleisen toimijan näkökulmasta arvottomat tiedotteet.

Vierailijaohjeiden laatiminen on toinen yleisesti helposti käyttöönotettava keino fyysisen turvallisuuden parantamiseksi. Monien yritysten tiloissa asioi myös yrityksen ulkopuoleisia henkilöitä, esimerkiksi kiinteistöhuoltoa, ulkoistettua siivousta tai muita vierailijoita. Tällaisten henkilöiden on mahdollista päästä käsiksi yrityksen tietoihin mikäli näitä säilytetään miten sattuu, esimerkiksi työpöydillä ilman valvontaa. Vierailijoiden luotettavalla tunnistamisella, kirjaamisella ja vierailun isännän valvonnalla voidaan pienentää vierailijoiden tuomia riskejä vierailun aikana, sekä tarvittaessa selvittää jälkikäteen alueilla liikkuneet ulkopuoliset henkilöt.

3.4 Osa-alue I: Tekninen tietoturvallisuus

Katakrin osa-alue I: tekninen tietoturvallisuus kuvaa turvallisuusjärjestelyihin liittyviä vaatimuksia sähköisissä käyttöympäristöissä. Luku 3.4 on jaettu käsittelemään näitä näkökulmia Katakrin kautta sekä yleisellä tasolla.

3.4.1 Tekninen tietoturvallisuus Katakrista

Katakrin osa-alue I: tekninen tietoturvallisuus kuvaa vaatimukset, joiden kautta pyritään varmistamaan sähköisen käyttöympäristön suojaamisen turvallisuusvaatimukset. Teknisen tietoturvallisuuden kohdat I-01 – I-21 Katakrissa ovat järjestyksessä seuraavat:

- I-01 – Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – verkon rakenteellinen turvallisuus
- I-02 – Vähimpien oikeuksien periaate - tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt ko. Turvallisuusluokan sisällä
- I-03 – Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan – suodatus- ja valvontajärjestelmien hallinnointi
- I-04 – Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – hallintayhteydet
- I-05 – Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - langaton tiedonsiirto
- I-06 – Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi
- I-07 – Monitasoinen suojaaminen – tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä
- I-08 – Vähimmäistoimintojen ja vähimpien oikeuksien periaate – järjestelmäkovennus
- I-09 – Monitasoinen suojaaminen – haittaohjelmasuojaus
- I-10 – Monitasoinen suojaaminen – turvallisuuteen liittyvien tapahtumien jäljitettävyys
- I-11 – Monitasoinen suojaaminen – poikkeamien havainnointikyky ja toipuminen
- I-12 – Tietoturvallisuustuotteiden arviointi ja hyväksyntä – salausratkaisut
- I-13 – Monitasoinen suojaaminen koko elinkaaren ajan – ohjelmistojen suojaaminen verkkohyökkäyksiltä
- I-14 – Monitasoinen suojaaminen – hajasäteily (tempest) ja elektroninen tiedustelu
- I-15 – Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä – tiedon sähköinen välitys
- I-16 – Turvallisuusluokitellun tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – muutoshallintamenettelyt

- I-17 – Turvallisuusluokiteltujen sähköisessä muodossa olevien tietojen käsittely fyysisesti suojattujen alueiden sisällä - fyysinen turvallisuus
- I-18 – Turvallisuusluokiteltujen tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - etäkäyttö ja etähallinta
- I-19 – Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – ohjelmistohaavoittuvuuksien hallinta
- I-20 – Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – varmuuskopiointi
- I-21 – Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen

Katakrin I-osion käsittely on jaettu tietoliikenneturvallisuuden, tietojärjestelmäturvallisuuden ja käyttöturvallisuuden otsikoiden alle niihin liittyvien Katakrin kohtien perusteella.

3.4.2 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden alaisissa kohdissa I-01 – I-05 käsitellään sähköisen tiedonsiirron toteuttamiseen ja suojaamiseen liittyviä vaatimuksia. Kohdan I-01 vaatimuksina tietojenkäsittely-ympäristöjen suojattuun yhteen liittämiseen mainitaan TL IV:n ympäristön osalta erottaminen muista ympäristöistä, yhdyskäytävän sisältävän vähintään palomuuriratkaisun sekä turva-alueen ulkopuolelle menevän liikenteen salaamisen turvallisuusluokkaan hyväksytyllä salausratkaisulla. Edellä mainittujen TL IV:n vähimmäisvaatimusten lisäksi TL III tai TL II ympäristön yhdistäminen muun turvallisuusluokan ympäristöön edellyttää hyväksyttyä yhdyskäytäväratkaisua, esimerkiksi yksisuuntaisen liikenteen sallivaa datadiodia. Datadiodi on esitetty luvussa 4.5.

Tietoliikenneverkon vyöhykkeistämisellä ja suodatussäännöillä (I-02) pyritään suojaamaan tietoliikenneverkkoa vähimpien oikeuksien ja monitasoisen suojaamisen periaatteiden mukaisesti. Vyöhykkeistämisellä tarkoitetaan verkon jakamista erillisiin verkkoalueisiin, kuten esimerkiksi työasema- ja palvelinverkkoerottelua. Suodatussäännöt on toteutettava vähimpien oikeuksien periaatteella, eli myös turvallisuusluokan sisällä eri verkkoalueiden välisessä liikenteessä sallitaan vain tarpeelliset yhteydet, ja muut yhteysyritykset havaitaan. Yleisesti vähimpien

oikeuksien periaatteessa tulisi estää oletuksena kaikki (“default-deny”), ja erikseen sallia tarvittaessa (lähde, kohde, protokolla). Suojaamiseen kuuluu myös yleisiin verkkohyökkäyksiin varautumista, esimerkiksi vain tarpeellisten toiminnallisuuksien pitämisellä päällä verkko- ja muissa laitteissa.

Tietoliikenneturvallisuudessa on huomioitava ja varauduttava myös ympäristön turvallisuuteen koko elinkaaren ajan (I-03), ympäristöjen suojattu yhteenliittäminen (I-04) sekä suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella (I-05). Kohdassa I-05 on syytä huomioida, että radiorajapinnan, esimerkiksi WLAN-verkon käyttö tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Vastaavanlaiseksi poistumiseksi lasketaan myös langattomien oheislaitteiden käyttö. Poistuminen turvallisuusalueelta vaatii toimivaltaisen viranomaisen hyväksymän salausratkaisun käytön.

3.4.3 Tietojärjestelmäturvallisuus

Tietojärjestelmäturvallisuuteen kuuluu pääsyoikeuksien hallinnointia ja käyttäjien tunnistamista (I-06 – I-07), järjestelmäkovennuksia ja haittaohjelmasuojausta (I-08 – I-09), tapahtumien jäljitettävyys ja poikkeamien havainnointikyky (I-10 – I-11), hyväksytyt salausratkaisut (I-12), ohjelmistojen suojaaminen ja varautuminen elektroniseen tiedusteluun (I-13 – I-14).

Käyttöoikeuksien hallinnoinnin tavoite on, että ainoastaan oikeutetuilla käyttäjillä on pääsy suojattuun tietoon. Tavoite pyritään täyttämään määrittämällä tietojärjestelmille käyttöoikeudet, myöntämällä käyttöoikeuksia nimettyjen vastuuhenkilöiden kautta ja tarkastamalla käyttöoikeuden saajan olevan oikeutettu oikeuksiin. Henkilöstömuutoksista ilmoittamiseen ja pääsyoikeuksien hallintaan tulee olla selkeä ja toimiva tapa sekä käyttö- ja pääsyoikeuksia tulee säännöllisesti katselmoida. Käyttöoikeudet tulee myös rajata vain tarpeen edellyttämään laajuuteen niin käyttäjä- kuin ylläpitorooleissa olevilta. Ylläpitorooleissa korostuu tehtävien erottelun riittävä toteutus, joka useissa järjestelmissä on järjestelmän ylläpitoroolien ja lokien valvontaan osallistuvien roolien välinen. Valvontamekanismi tahallisen tai tahattoman väärinkäytön varalle voi olla myös kriittisiin ylläpitotehtäviin vaadittava kahden tai useamman henkilön hyväksyntä.

Tietojenkäsittely-ympäristön toimijoiden tunnistaminen sisältää niin henkilöt, laitteet kuin tietojärjestelmätkin. Katakrissa I-07 -kohdassa on toteutusesimerkki TL IV -ympäristössä henkilöiden, laitteiden ja tietojärjestelmien tunnistamiseen vähimmäisvaatimusten täyttämiseksi. Esimerkissä on kahdeksan kohtaa, joita täydennetään kahdella kohdalla TL III – TL II -ympäristön vaatimuksista. Henkilöiden tunnistamisen vaatimuksia on edellä mainitussa esimerkissä muun muassa yksilölliset henkilökohtaiset käyttäjätunnukset sekä käyttäjän tunnistuksen epäonnistumisesta seuraava tunnuksen lukitseminen.

Järjestelmäkovennukset pyrkivät toteuttamaan vähimpien oikeuksien periaatetta palvelimien, työasemien, verkkolaitteiden, tulostimien ja muiden tietojärjestelmiksi käsitettävien laitteiden osalta. Järjestelmäkovennuksilla tarkoitetaan tässä yhteydessä laitteiden ominaisuuksien ja käyttäjien oikeuksien rajoittamista tarpeen mukaan ottamalla ainoastaan tarvittavat palvelut, rajapinnat ja yhteydet käyttöön. Kovennusten tarkoituksena on pienentää hyökkäyspinta-alaa järjestelmää kohtaan.

Katakrin vaatimusten täyttämiseksi järjestelmäkovennukset on tehtävä vähintään komponentin valmistajan kovennussuosituksen mukaisesti. Ulkoisista kovennusohjeita tarjoavista tahoista yksi tunnetuimmista ja laajan hyväksynnän saaneista on Center for Internet Security (CIS). CIS tarjoaa useisiin järjestelmiin konfiguraatio-ohjeita [(7), CIS]. Esimerkiksi työasemaa kovennettaessa voi olla tarve ottaa huomioon muun muassa seuraavat komponentit:

- Työaseman raudan kovennus (kameroiden, mikrofonien, langattomien verkkokorttien poisto fyysisesti)
- Laiteohjelmiston kovennus (BIOS)
- Käyttöjärjestelmän kovennus (esim. Windows-kovennukset)
- Käyttäjäkovennukset (esim. salasanarajoitteet)
- Ohjelmistokovennukset (mm. päivitysten ajantasaisuuden ylläpito)

Kovennusten toteutus tulee räätälöidä järjestelmäkohtaisesti ottaen huomioon käyttötarkoituksen, riskianalyysin sekä sovellettavan turvallisuusluokan vaatimukset. Kovennuksien toteuttamisessa ja käyttöönotossa voidaan käyttää apuna

konfiguraationhallintatyökaluja, kuten esimerkiksi Microsoftin Group Policy Manager Console, jolla voidaan hallita Group Policy objektien (GPO) kautta käyttöjärjestelmän asetuksia yrityksen laajuudella [(8), Microsoft].

Haittaohjelmasuojaus on syytä toteuttaa turvallisuusluokitellussa ympäristössä monitasoisesti, jotta voidaan ennaltaehkäistä, estää, havaita ja viimeistään korjata tilanteet haittaohjelmauhkan realisoituessa. Haittaohjelmasuojauksen toteuttamisessa ei tule luottaa pelkästään torjuntaohjelmistojen käyttöön, vaan se on kaikkien muiden turvallisuusaspektien summa, aina henkilöstön turvatietoisuuden varmistamisesta (T-12) järjestelmien kovennusmenettelyihin (I-08). Kattavan monitasoisen suojaamisen toteuttamisen lisäksi oleellinen osa haittaohjelmia vastaan suojautumiseksi on pitää torjuntaohjelmistot toimintakykyisinä, päivitettynä haittaohjelmatunnisteilla ja asennettuna kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille. Järjestelmiin, jotka ovat eristettyjä julkisista verkoista voidaan haittaohjelmatunnisteet tuoda esimerkiksi käsin siirtämällä erillisestä internettiin kytketystä järjestelmästä 1–3 kertaa viikossa. Haittaohjelmasuojauksen tarkoitus on estää ja havainnoida tietojen luvattoman muuttamisen tai käsittelyn. Haittaohjelmasuojauksen lisäksi ohjelmistojen suojaaminen verkkohyökkäyksiltä on tärkeässä roolissa. Ohjelmistoihin liittyviä riskejä voidaan arvioida niiden käyttötarkoitusten perusteella: esimerkiksi palomuuriohjelmiston turvallisuuden arviointi on erittäin kriittistä, koska sen turvallisuutta toteuttavan roolin takia ohjelmiston haavoittuvuudesta voi seurata valtava uhka koko ympäristölle. Ohjelmistojen turvallisuuden varmistamiseksi tulee hyödyntää tarkentavia ohjeita ja standardeja.

Turvallisuuteen liittyvien tapahtumien jäljitettävyyden vaatimukset ja tavoitteet on esitetty Katakrin kohdassa I-10. Jäljitettävyydellä tai lokituksella tarkoitetaan tapahtumien kirjaamista muodossa, josta tarvittaessa voidaan selvittää tapahtumien kulku jälkikäteen. Oleellisia tietoja lokituksessa ovat: mitä on tehty, kuka on tehnyt ja mitä vaikutuksia teolla on ollut. Lokitus on toteutettava kattavalla tasolla, vähintään työasemien, palvelinten ja verkkolaitteiden suhteen. Lokeja kerätään tyypillisesti kirjautumistapahtumista, sekä verkkolaitteiden ja palvelimien suhteen mitä toimenpiteitä näille on tehty, milloin ja kenen toimesta. Lokit on syytä turvata jäljitettävyyden varmistamisesti, ja suositeltu tapa tähän on ohjata keskeiset lokit

vahvasti suojatulle lokipalvelimelle. Lokien vaaditaan säilytettäväksi turvallisuusluokan IV ympäristössä vähintään 6 kuukautta ja turvallisuusluokan III – II ympäristössä vähintään 5 vuotta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.

Pelkkä lokien kerääminen ei riitä, vaan poikkeamat tulee myös havaita luotettavasti tietojenkäsittely-ympäristössä. Poikkeamien havainnointikyky edellyttää useimmissa ympäristöissä käytännössä automatisoituja havainnointi- ja hälytystyökalujen käyttöä. Poikkeamien havainnointikyky pohjautuu yleensä lokien lisäksi verkkoliikenteessä näkyviin tapahtumiin ja verkon työasemilla ja palvelimilla näkyviin tapahtumiin. Verkkoliikenteestä voidaan havaita poikkeamia tapahtumista, joista ei ole saatavilla hyökkäysten tunnistetietoja, mikäli tunnetaan verkkoliikenteen normaali tila. Kun verkon normaali tila on tunnettu, voidaan esimerkiksi odottamattomasta ja epätavallisesta verkkoliikenteen määrän kasvusta havaita poikkeama.

Tietojen luvattoman paljastumisen ja muuntelun estämiseksi käytetyt salausratkaisut vaativat toimivaltaisen viranomaisen hyväksynnän turvallisuusluokalle (I-12). Ensimmäinen kohta salausratkaisujen käytön vaatimuksille on tunnistaa organisaatiossa salausratkaisujen käyttötapaukset eli kaikki tilanteet, joissa turvallisuusluokitellun tiedon suojaaminen vaatii salausratkaisun käyttöä. Näitä käyttötapauksia ovat muun muassa liikennöinti matalamman turvallisuusluokan verkon kautta (mukaan lukien internet), tiedon välitys organisaatiosta toiseen ja turvallisuusalueiden ulkopuolelle vietävät päätelaitteet. Salausratkaisuna tulee käyttää joko toimivaltaisen viranomaisen ennalta [(9), NCSA] tai tapauskohtaisesti hyväksymää tuotetta hyväksyjän käyttöpolitiikassa mainituin asetuksin. Myös salauksessa käytettäviä kryptografisesti vahvoja avaimia tulee hallita ja ne tulee dokumentoida asianmukaisesti.

3.4.4 Käyttöturvallisuus

Käyttöturvallisuus kuvaa sitä, miten turvallisuusluokiteltuja tietoja käsitellään sähköisessä ympäristössä. Katakrin I-osion kohdat I-15 – I-21 kuvaavat käyttöturval-

lisuuden vaatimuksia niin tietojen välityksen, käsittelyn, varmuuskopioinnin ja tuhoamisen kannalta. Lisäksi käyttöturvallisuuden vaatimuksiin kuuluu tietojenkäsittely-ympäristön suojaus (I-16) sekä ohjelmistohaavoittuvuuksien hallinta (I-19).

Fyysisesti suojattujen alueiden välillä tapahtuva tiedonsiirto tulee toteuttaa I-12 kohdan mukaisesti turvallisuusluokalle hyväksyttyjen salausratkaisujen avulla. Tämän lisäksi vastaanottaja tulee pystyä varmistamaan riittävän tietoturvallisella tavalla. Fyysisesti suojattujen alueiden sisäpuolella tapahtuvaan tiedonsiirtoon riittää puolestaan alemman tason suojaus riskienhallintaprosessin perusteella. Esimerkiksi HTTPS voidaan käyttää verkkoliikenteen salaamisessa toimivaltaisen viranomaisen erillishyväksynnällä turva-alueiden sisäpuolella.

Muutoshallintamenettelyt (I-16) kuvaa tietojenkäsittely-ympäristön suojaamisesta sen koko elinkaaren ajan. Turvallisuuden jatkuva varmistaminen, määräajoin suoritettavat arvioinnit, tarkastukset ja uudelleentarkastelut sekä turvallisuusasiakirjojen jatkuva kehittäminen ovat muutoshallintamenettelyiden vaatimuksia. Tietojenkäsittely-ympäristön turvallisuuden varmistaminen edellyttää muun muassa näiden sisältämien järjestelmien elinkaarihallintaa, uusien järjestelmien tai ohjelmistopäivitysten käyttöönoton yhteydessä tapahtuvaa kattavaa testausta ja muutoslokien tarkastelua, sekä automatisoituja skannauksia sekä konfiguraatiovertailuja ympäristössä. Ympäristön tekninen rakenne tulee olla tiedossa ja ajan tasalla, kattaen siihen kuuluvat laitteistot, näiden ohjelmistoversiot sekä muut ohjelmistot. Erityisen tärkeää muutoshallintamenettelyissä on muutosten jäljitettävyys.

Sähköisten turvallisuusluokiteltujen tietojen käsittelyyn ja etäkäyttöön liittyy paljon vaatimuksia riippuen turvallisuusluokasta sekä tiedonomistajasta. Kansainvälisen tiedon käsittelyyn liittyy enemmän rajoitteita kuin kansallisen tiedon käsittelyyn. Yleisiä TL IV vaatimuksia käsittelyyn ja säilytykseen liittyen ovat:

- Tietojen suojaaminen sivullisilta
- Tietoja käsitellään ja säilytetään turvallisuusalueilla tai toimivaltaisen viranomaisen hyväksymillä menetelmillä näiden ulkopuolella
- Tietovarannot ovat sijoitettu hyväksytyille turvallisuusalueille

Etäkäytön ja -hallinnan vaatimuksia TL IV:

- Käyttäjät ja päätelaitteet tunnistetaan riittävän luotettavasti

- Turvallisuusalueiden välinen etäkäyttö vaatii hyväksyttyjen korvaavien menettelyjen käytön
- Tietoja ja niihin pääsyä on suojattava sivullisilta, sekä henkilöstö on koulutettu turvalliseen etäkäyttöön
- Turvallisuusalueiden ulkopuolella tietovälineet tulee salata turvallisuusluokalle hyväksytyin menetelmin tai pidettävä jatkuvasti valvottuna. Päätelaitteet tulee olla salattuja.
- Etäkäyttö vaatii turvallisuusluokan mukaisen liikenteen salauksen

Näiden lisäksi TL III – TL II tuo mukanaan lisärajoitteita, kuten esimerkiksi kansainvälistä TL III tai korkeampaa tietoa ei saa säilyttää turvallisuusalueiden ulkopuolella, ja kansallistakin vain rajoituksin. Kansallisten turvallisuusluokiteltujen tietojen käsittelyn ja säilytyksen rajoitteet on kuvattu liitteessä 2.

Ohjelmistohaavoittuvuuksien hallinnan tulee tähdätä tarkan tilannekuvan muodostamiseen ja ympäristön seurantaan ja seurannan kehittämiseen. Ohjelmistohaavoittuvuuksia voi hallita seuraamalla viranomaisten, laite- ja ohjelmistovalmistajien tai CERT-toimijoiden tietoturvatiedotteita. Haavoittuvuuksia korjaavat turvapäivitykset asennetaan tarpeen mukaan hallitusti. Ohjelmistopäivitysten asentumista ja onnistumista seurataan säännöllisesti. Verkkoa ja sen palveluita, palvelimia, työasemia ja muita laitteita skannataan haavoittuvuuksien löytämiseksi säännöllisin välein, ja myös merkittävien muutosten käyttöönottojen jälkeen korjauskohteiden löytämiseksi.

Varmuuskopioinnin vaatimuksia on turvallisuusluokiteltuja tietoja sisältävien kopioiden suojaaminen vähintään samalla tasolla, miten alkuperäiset tiedot on suojattu. Mikäli varmuuskopiot luodaan usean eri tiedonomistajan suhteen samaan varmistusjärjestelmään, on otettava huomioon tiedonomistajien tarkastusoikeuksiin mahdollistava erittely tietojärjestelmässä. Hävitettävät varmistusmediat ja muu sähköinen turvallisuusluokiteltu tieto tulee hävittää turvallisuusluokan käytäntöjen ja vaatimusten mukaisesti. Sähköisten tallennusmedioiden, kuten magneettisten kiintolevyjen, SSD-kiintolevyjen, USB-muistien ja optisten medioiden osalta käytetään silppuamista tuhoamiseksi. Kyberturvallisuuskeskuksen ylikirjoitusohjeessa [(10), NCSA] on sähköisten tietojen tuhoaminen kuvattu yksityiskohtaisemmin.

3.4.5 Tekninen tietoturvallisuus yleisellä tasolla

Tekninen tietoturvallisuus on Katakrin kolmesta osa-alueesta se, joka vahvimmin mielletään ja yhdistetään tietoturvaan yleisellä tasolla. Tietoliikenneturvallisuus, tietojärjestelmäturvallisuus ja käyttöturvallisuus kattavat valtavan kokonaisuuden, jonka sisäistäminen ja omakohtainen toteuttaminen korkealla turvallisuuden tasolla vaativat valtavasti laaja-alaista osaamista. Kuten turvallisuusjohtamisen ja fyysisen turvallisuuden näkökulmista, myös teknisen turvallisuuden toteuttaminen omaan käyttötarkoitukseen tulee suhteuttaa omaan riskiarvioon tasolla, jossa jäännösriskit voidaan hyväksyä.

Monitasoisella suojaamisella (defence in depth) voidaan oma tietojenkäsittelyympäristö suojata parhaiten myös teknisen tietoturvallisuuden näkökulmasta. Monitasoisen suojaamisen tehokkuus on toisistaan riippumattomien turvatoimien toteuttaminen tavalla, jossa yksittäisen turvatoimen pettäminen ei aiheuta vielä suurta uhkaa suojattavan tiedon luottamuksellisuudelle, eheydelle ja saatavuudelle. Laaja-alaisesti toteutettu monitasoinen suojaaminen ottaa huomioon haavoittuvuudet laitteistojen ja ohjelmistojen osalta sekä pienentää inhimillisten virheiden vaikutusta tietoturvan vaarantumiselle. Inhimilliset virheet ja ihmisten välinpitämättömyys ovat usein tietomurtojen syynä, joten tämän riskin pienentämisellä on suurin yksittäinen vaikutus tietoturvan kannalta. [(11), Fortinet]

Ennen monitasoisen suojaamisen suunnittelua ja toteutusta kannattaa tehdä oma riskiarvio todellisista riskeistä, ja näihin varautumisesta. Riskiarvion tulisi helpottaa havaitsemaan todennäköisimmät riskit ja näiden vaikutus liiketoiminnan tai muun ympäristön tietoturvaan. Jos riskien ja niiden realisoitumisen mahdollisuuksilla ei ole merkittävää vaikutusta tavalla, ja jos jäännösriskit voidaan hyväksyä, ei kannata käyttää määräänsä enempää aikaa ja rahaa suojaustoimenpiteiden toteuttamiseksi. Vastaavasti jos teknisen tietoturvan pettäminen aiheuttaa liiketoiminnan päättymisen, on syytä käyttää sen toteuttamiseen enemmän resursseja.

Varmuuskopioinnin arvo suojattavien tietojen saatavuuden kannalta on asia, johon kannattaa panostaa toimintaympäristöstä riippumatta. Toimiva ja testattu

varmuuskopiointi auttaa suojaamaan laiterikkojen sekä tahallisten että tahattomien tietojen menettämisten varalta. Yhdysvaltalaisen valokuvaaja Peter Kroghin luoma yleisesti tunnettu käsite “3-2-1”-strategiasta varmuuskopioiden ottamisen on hyvä lähtökohta mistä aloittaa. Kyseinen sääntö kuuluu, että tiedosta tulee olla kolme kopiota, kahden eri tyypin tallennusmedialla, ja joista yhden tulee olla eri fyysisessä sijainnissa. Erityyppisten tallennusmedioiden käyttö pyrkii estämään tallennusmediasta johtuvat vaikutukset ja yhden kopion säilytys muualla pyrkii poistamaan sijainnin vaikutuksen palauttamiseen [(12), Seagate]. Varmuuskopioinnista täytyy kuitenkin muistaa, ettei se suojaa tiedon luottamuksellisuuden tai eheyden suhteen. Näitä vasten täytyy varautua muilla keinoin.

Monitasoisen suojaamisen käyttöönotto tiedon luottamuksellisuuden ja eheyden varmistamiseksi on mahdollista toteuttaa osissa. Tämä mahdollistaa uusien ja kehittyvien ympäristöjen osalta suojauksen tason skaalaamisen ympäristön myötä. Alussa voidaan keskittyä kriittisimpien lisäarvoa tuovien suojausten toteuttamiseen, ja myöhemmin lisätä turvallisuuden kerroksia vähemmän kriittisten toimenpiteiden kautta.

Verkkoinfrastruktuurin turvaamista voidaan pitää yhtenä kriittisimmistä osista ympäristön turvaamiseksi. Varsinkin verkkolaitteiden osalta turvatoimien pettäminen voi mahdollistaa hyökkääjän pääsy seuraamaan, ohjaamaan ja muokkaamaan liikennettä, sekä etenemään verkossa. Yhdysvaltojen valtion virasto CISA suosittelee verkkolaitteiden turvaamiseksi [(13), CISA]:

- Verkkojen ja toimintojen erottelua ja segmentointia
- Rajoita tarpeetonta sivuttaista liikennettä verkossa
- Kovenna verkkolaitteet
- Suojaa pääsy verkon laitteisiin (MFA, AAA)
- Erota hallintaliikenne tuotantoliikenteestä
- Ylläpidä laitteiston ja ohjelmiston eheyttä

Verkon turvaamisen jälkeen loogisesti seuraava askel on turvata verkon sisällä olevat palvelut. Tässä voidaan käyttää muun muassa Katakrin kohtia järjestelmäkovennuksista (I-08), haittaohjelmasuojauksesta (I-09), jäljitettävyydestä (I-10) ja ohjelmistohaavoittuvuuksien hallinnasta (I-19) lähtökohtina, soveltaen ja suhteut-

taen omaan käyttötarpeeseensa. Varsinkin ohjelmistohaavoittuvuuksien hallintaan liittyvä ohjelmistojen säännöllinen päivittäminen on asia, joka on helposti toteutettavissa ja jolla on suuri vaikutus turvallisuuteen.

Turvallisuuteen liittyvien toimenpiteiden toteutus kannattaa yleisellä tasolla aloittaa helpommasta päästä, jotta voidaan saavuttaa liiketoimintaan tai henkilökohtaiseen käyttöön vaadittava ympäristön tietoturvan perustaso. Tietoteknisestä näkökulmasta katsottuna tässä pyritään varmistamaan, että myös kaikista itsestään selvimmät tietojen käsittelyn tukipilarit tulisi olla kunnossa, ennen kuin ruvetaan miettimään lisäturvan käyttöönottoa. Tämän toteuttamiseksi ei ole olemassa yhtä absoluuttista totuutta eikä ohjetta. Kirjallisuudesta ja internetistä saatavien lähteiden perusteella, kuten esimerkiksi Information Commisioner’s Officen verkkoartikkelin “11 practical ways to keep your IT systems safe and secure” [(14), ICO], voidaan saada käsitys perustason vaatimuksista.

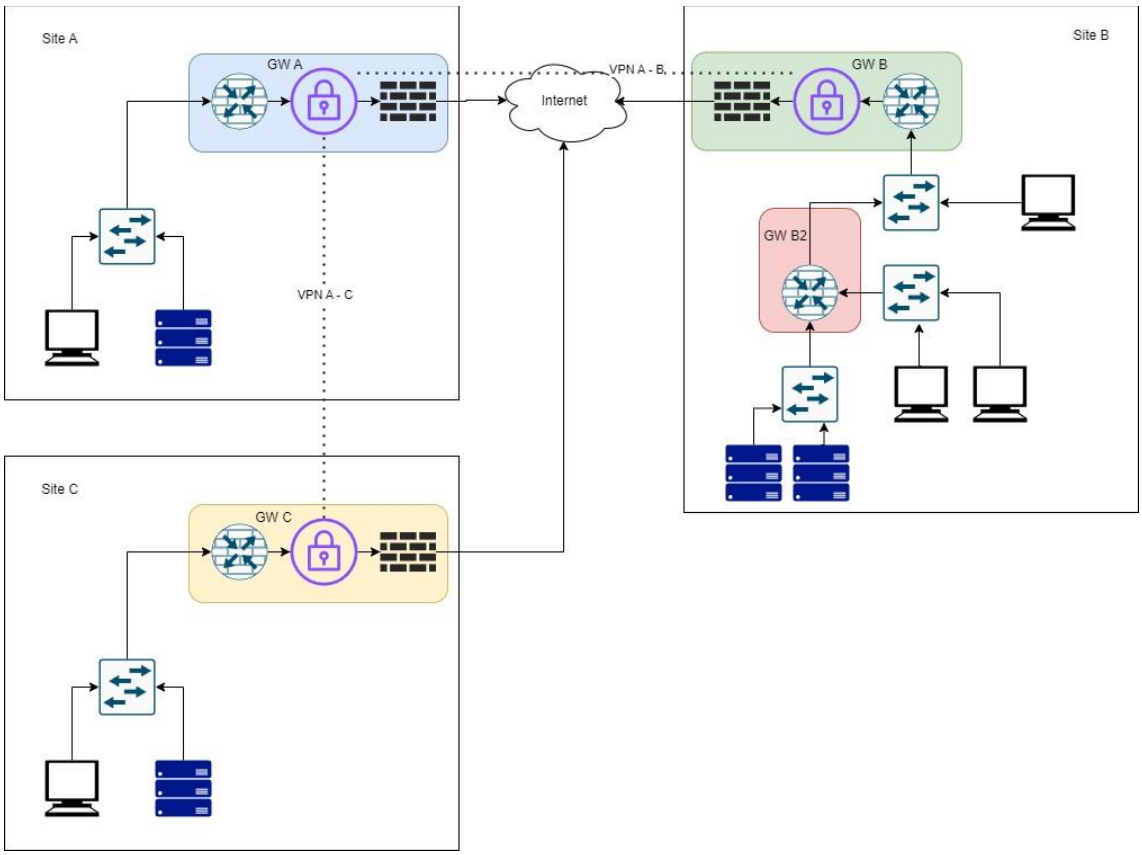
Käytännössä tietoturvan perustason rakentaminen lähtee ihmisistä. Vahvojen salasanojen käyttö, varmuuskopioiden teko, työaseman lukitseminen sen ääreltä poistumisen yhteydessä ja oikeanlainen kriittisyys tuntemattomien lähettäjien sähköpostien avaamisessa ovat esimerkkejä näistä toimenpiteistä. Tietoturvapolitiikkojen määrittely ja ihmisten sitouttaminen näiden noudattamiseksi tulisi olla tehty, ennen kuin aletaan pohtimaan korkeamman tason turvatoimien, kuten IDS- tai IPS-järjestelmien käyttöönottoa verkossa.

4 YHDYSKÄYTÄVÄRATKAISUT

Kappaleessa 4 esitellään erilaisia verkon yhdyskäytäviin liittyviä vaihtoehtoja ja toteutustapoja. Esiteltävät laitteet ja ratkaisut ovat poimintoja Katakrin vaatimuksista ja toteutusehdotuksista. Esiteltävät ratkaisut eivät jokaiseen ympäristöön ole käytännöllisiä tai yksistään riittäviä, mikä tulee ottaa huomioon yhdyskäytäväratkaisuja toteutettaessa.

4.1 Yleistä

Yhdyskäytävä yhdistää tietoverkon toiseen tietoverkkoon toimien liikenteen solmukohtana näiden välillä. Yhdyskäytävä koostuu yhdestä tai useammasta laitteesta, jotka ohjaavat ja rajoittavat liikennettä tietoverkosta toiseen. Tyypillisiä yhdyskäytävälaitteita ovat muun muassa palomuurit, reitittimet, salaimet sekä näiden väliset fyysiset tai langattomat mediat, joita pitkin verkkoliikenne kulkee.



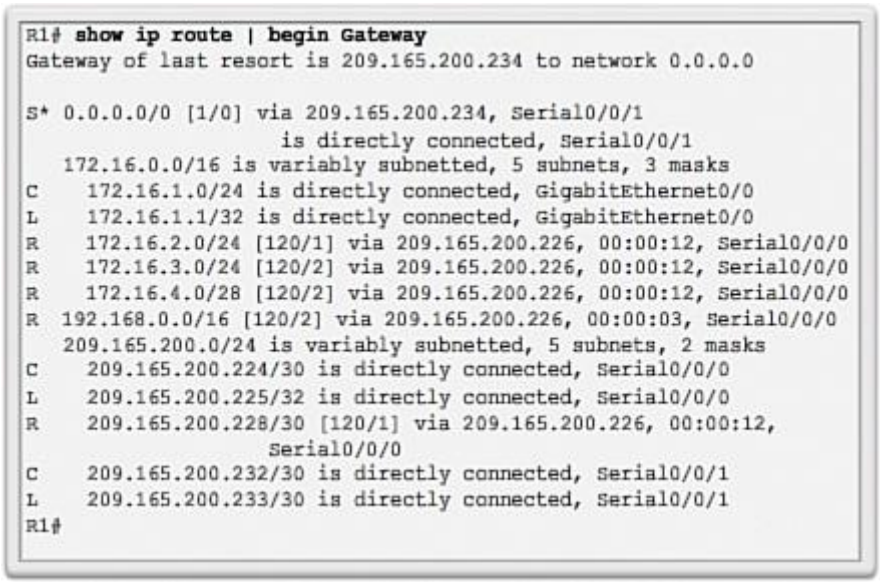
KUVA 1. Yhdyskäytäviä yrityksen toimipisteissä

Kuvassa 1 on havainnollistettu yhdyskäytävän konseptia. Esimerkissä on kolme toimialuetta, “Site A”, “Site B” ja “Site C”. Toimialueilta ulospäin suuntautuva liikenne kulkee sinisen, vihreän ja keltaisen yhdyskäytävän kautta, jotka sisältävät reitittävän palomuurin, VPN-salaimen sekä ulkopalomuurin. Nämä yhdyskäytävät sisältävät useampia yhdyskäytävälaitteita liikenteen suojaamiseksi julkiverkkoon ja julkiverkosta sisäänpäin. Toimialue B:llä on lisäksi yhdyskäytävä GW B2, joka rajaa pääsyä palvelimien ja työasemien välillä. VPN-laitteilla on muodostettu salatut yhteydet A:n ja B:n sekä A:n ja C:n välillä, ja sisäverkon liikenne B:n ja C:n välillä kulkee A:n kautta.

Verkon yhdyskäytävää voi verrata talon ulko-oveen. Sen sisäpuolella on kotisi, jonne et halua päästää ketä tahansa ilman lupaasi. Ovia on erilaisia, ovien paksuus ja lukkojen tyyppi sekä lukumäärä kertovat oven turvallisuudesta. Vaikka talon sisällä olisi liiketunnistimet, valvontakamerat ja kassakaappi arvokkaimman omaisuuden suojaamiseksi, on tärkeää pitää talosi ovet lukossa kolmansilta osapuolilta. Parasta suojaa et saa lisäämällä ääretöntä määrää lukkoja oveesi, vaan rakentamalla aidan talosi ympäri. Turvallisuuskerrosten lisääminen hajauttaa riskiä vähentämällä yksittäisen turvatoimen pettämisen vaikutusta kokonaisuuteen. Kuvan 1 palvelimet ovat palomuurin GW B2:n takana, jolloin näihin voi verkkotasolla rajoittaa pääsyä myös sisäverkosta.

4.2 Reititin

Reititin on yleisin yhdyskäytäväratkaisu. Reititintä käytetään verkkojen reunalla ja se operoi OSI-mallin verkkokerroksella L3. Reitittimen primäärinen funktio on ohjata IP-paketteja reititystauluun tallennettujen tietojen mukaisesti kohteeseensa parhaalla mahdollisella tavalla. Reititin päivittää reititystauluunsa tietoja suoraan reitittimeen yhdistettyjen verkkojen lisäksi muista IP-verkoista reititysprotokollien sekä käsin määritettävien staattisten reittien kautta. Kuva 2 esittää IPv4-reititystaulun tarkastelua geneerisestä Cisco-reitittimestä R1.



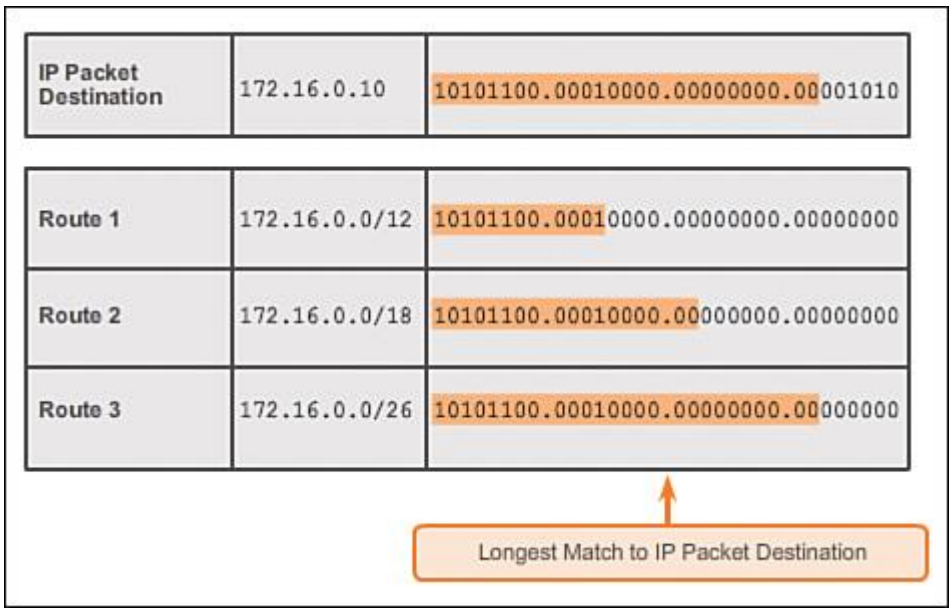
```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
                    is directly connected, Serial0/0/1
   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R  192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
   209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
                    Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

Kuva 2. Cisco-reitittimen R1 reititystaulu. [(15), Cisco]

Reititin tekee reitityspäätökset aina reititystaulunsa mukaisesti. Reititin katsoo saamansa paketin kohdeosoitetta, ja etsii sille aina tarkimman vastaavuuden reititystaulustaan. Kuvassa 2 rivin ensimmäinen sarake kertoo, miten kyseinen rivi on reititystauluun valittu. Cisco-reitittimissä S-kirjain kertoo staattisesta eli käsin konfiguroidusta reitistä. Taulun ensimmäisen rivin 0.0.0.0/0 on niin kutsuttu nollareitti tai oletusreitti, jolla määritetään paketit, joiden kohdeosoite ei ole tiedossa, kulkemaan osoitteeseen 209.165.200.234 reitittimen portin Serial0/0/1 kautta. ”L” tarkoittaa paikallista verkkoa, ”C” yhdistettyä verkkoa ja ”R” kertoo reititystiedon tulleen RIP-protokollan kautta. Hakasulkeissa olevat arvot kertovat metriikoista, esimerkiksi yhteyden nopeudesta tai pituudesta, jotka riippuvat reititysprotokollista. Metriikoita käytetään reitityksessä siinä tapauksessa, kun kohteeseen on enemmän kuin yksi reitti ja tarvitsee tehdä päätös parhaan valitsemiseksi.

Alla olevassa kuvassa 3 [(15), Cisco] on havainnollistettu tarkimman vastaavuuden löytäminen ja valinta reititystaulusta. Ensimmäisellä rivillä on IPv4-paketin kohdeosoite 172.16.0.10 ja sitä vastaava 32-bittinen binääriarvo. Kolme esimerkkireittiä eroaa verkkomaskin pituudessa, joista pisin kohdeosoitteeseen täsmäävä valitaan. Punaisella korostettu osuus binääriarvosta vastaa verkkomaskin pituutta. Mikäli esimerkin reititystaulussa olisi neljäs reitti 172.16.0.0/28 sekä viides reitti 172.16.0.0/29, olisi neljäs reitti paras osuma ja se valittaisiin. Viides reitti ei täsmää enää kohdeosoitteeseen verkkomaskin ollessa liian pitkä.



Kuva 3. Tarkimman reitin valinta. [(15), Cisco]

Kuluttajapuolella reititintä käytetään yleisnimityksenä laitteelle, joka kytketään palveluntarjoajan ja kodin sisäverkon välille. Kuluttajareitittimet voivat sisältävät mm. modeemin, palomuurin, WLAN-moduulin ja antenneja, DHCP-palvelun, Quality of Service (QoS) -liikenteen priorisointitoiminnon, yhden WAN- ja useamman LAN-puolen verkkoportin. Kuluttajareitittimien hyvä puoli on käyttöönoton helppous, mutta nämä eivät yleensä sovellu yritysten käyttöön konfiguroitavuuden ja tehojen puolesta.

Katakrissa reitittimet mainitaan muiden verkkolaitteiden kanssa laitteina, joihin vain ylläpitäjillä tulisi olla pääsy. Näiden verkossa liikennettä suodattavien ja valvovien järjestelmien tarkoituksenmukaista toimintaa tulee ylläpitää erityisen huolellisesti. Reititysprotokollien käyttö ja niiden ominaisuudet tulee huomioida tietoliikenneverkon vyöhykkeistämisen ja vähimpien oikeuksien periaatteiden noudattamisessa.

4.3 Palomuuri

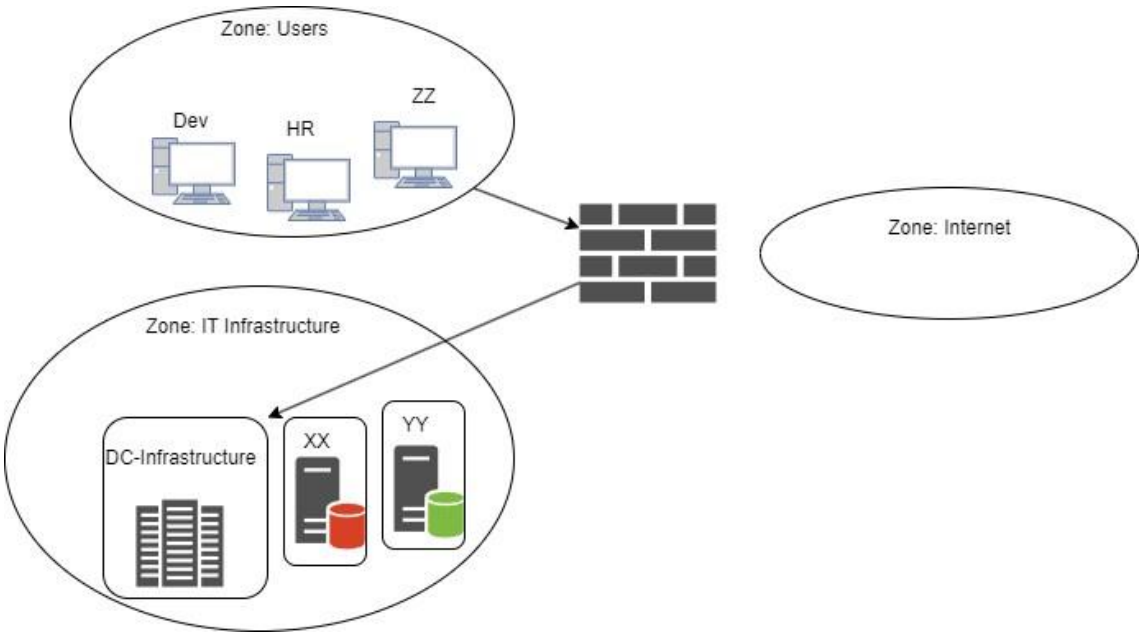
Palomuuri on oleellinen osa tietoturvallista yhdyskäytäväratkaisua niin yrityksissä kuin kotikäytössäkin. Palomuurin tehtävä sallia haluttu liikenne verkkojen välillä. Palomuuri voi olla joko fyysinen laite tai virtualisoitu toiminto. Fyysiset palomuurit

toimivat usein myös reitittiminä näiden verkkojen reunalla olevan loogisen sijainnin vuoksi. Palomuureja on myös verkon päätelaitteissa, esimerkiksi Windows-työasemissa Microsoft Defender Firewall.

Perinteisen palomuurin toiminta perustuu säännöstöihin, joissa liikennettä suodatetaan lähde- ja kohdeosoitteen sekä käytetyn protokollan ja portin mukaan. Säännöt ovat hierarkkisia, ja palomuuri tekee ratkaisun liikenteen sallimisesta tai estämisestä ensimmäisen liikenteeseen täsmäävän säännön mukaan, käydessään sääntöjä ylhäältä alas pain läpi. Yleinen tapa toteuttaa palomuurisäännöstö on luoda niin sanottu “default deny”-sääntö, joka kieltää kaiken liikenteen (deny). Tämän yläpuolelle tehdään säännöt, jotka halutaan sallia (allow).

Niin sanotuissa seuraavan generaation palomuureissa, next-generation firewall (NGFW), voidaan suodatussääntöjä luoda myös muun muassa OSI-mallin sovellustasolla. Käsitteet vaihtelevat valmistajittain, mutta yleisesti NGFW:t hyödyntävät syvällisempää pakettien tulkintaa ja analysointia esimerkiksi uhkien havaitsemiseksi liikenteen seasta.

Alue- tai Zone-pohjaisen palomuurin toiminta perustuu samankaltaisten verkkoalueiden liityntäkohtien (interfacejen) loogiseen yhdistämiseen palomuurilla. Esimerkiksi yrityksessä on toteutettu ohjelmistokehittäjien verkko “Dev”, henkilöstöosaston verkko “HR” ja “ZZ” verkko. Näillä kaikilla on yhteneväisiä tarpeita verkon suhteen, ja ne on liitetty käyttäjille luotuun alueeseen (zone) “Users”. Users-alue eroaa tarpeiltaan infrastruktuuripalveluiden verkoista. Näille on luotu alue nimeltä “IT Infrastructure”. Users ja IT Infrastructure -alueiden lisäksi on luotu kolmas alue nimellä “Internet”, joka kuvaa julkista internettiä ja sen palveluita. Tämä esimerkkitapaus on havainnollistettu kuvassa 4.



KUVA 4. Alueet (zone) palomuurilla

Esimerkin yrityksessä on tunnistettu tarve saada dns, ntp, oscp, ja smtp -palvelut käyttöön yrityksen työntekijöille. Lisäksi infrapalveluiden suuntaan halutaan sallia ping, mikä auttaa mahdollisten yhteysongelmien selvittelyssä. Kyberturvallisuusyhtiö Palo Alton palomuureissa palomuurisääntöjen konfigurointi ja hallinta on tehty helpoksi Panorama-hallintapalvelun kautta. Kuvassa 5 on tehty palomuurisääntö Panoraman kautta sallimaan edellä mainitut palvelut lähdealueelta kohteisiin.

		Source		Destination						
Name	Type	Zone	Address	Zone	Address	Application	Service	Action	Profile	Options
Network Infrastructure	universal	Users	any	IT Infrastructure	DC-Infrastructure	dns ntp ocsp ping smtp	application-default	Allow		

KUVA 5. Palomuurisääntö Panorama-hallintapalvelussa [(16), Palo Alto Networks]

Lisäksi halutaan sallia pääsy tavanomaisiin internet-palveluihin. Tämä sääntö on tehty kuvassa 6.

		Source		Destination						
Name	Type	Zone	Address	Zone	Address	Application	Service	Action	Profile	Options
Internet Access	universal	Users	any	Internet	any	Internet ssl	application-default	Allow		

KUVA 6. Palomuurisääntö internettiin Panorama-hallintapalvelussa [(16), Palo Alto Networks]

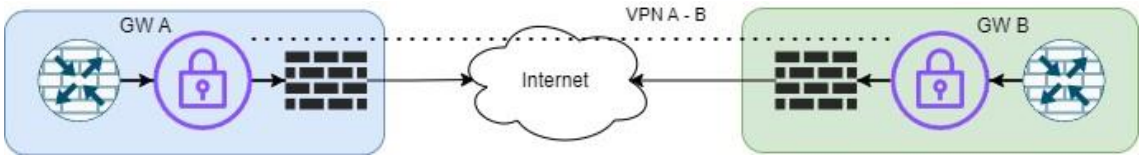
Kuvan 6 palomuurisäännössä kohdepuolen (Destination) osoitteiksi on määritetty DC-Infrastructure, joka sisältää ennalta määritellyt IP-osoitteet tai verkkoalueet. Internet-zonen suuntaan olevassa säännössä kohdeosoitetta ei ole rajoitettu, ja se sallii ulospäin yhteydet kaikkialle. “Application-default”-kohta määrittää, että vain palveluiden oletusportit ja protokolla sallitaan, esimerkiksi HTTP ja HTTPS osalta TCP 443 ja TCP 80. Application-default palvelun (servicen) käyttö mahdollistaa tunnistamaan verkkoliikenteen, joka yrittää naamioida itsensä joksikin muuksi. Esimerkiksi SQL-kysely porttiin TCP 80 nostaa lipun, sillä NGFW:n paketin OSI-mallin sovellustason tutkiminen huomaa, ettei kyseessä ole HTTP-liikenne.

Katakri kertoo palomuuriratkaisun käytön sekä liikenteen salaamisen olevan vähimmäisvaatimuksena, kun TL IV tietojenkäsittely-ympäristö kytketään muuhun, matalamman turvallisuusluokan ympäristöön. TL III ja TL II ympäristöissä edellytetään hyväksytyn yhdyskäytäväratkaisun käyttöä. Monissa näistä tapauksissa palomuuri on oleellinen osa hyväksyttyä yhdyskäytäväratkaisua.

4.4 VPN

VPN eli virtual private network mahdollistaa kahden laitteen tai verkon yhdistämisen toisiinsa turvallisesti julkisen verkon yli. Tyypillisiä VPN-toteutuksia on “site-to-site” VPN, jolla yhdistetään esimerkiksi yrityksen toimipisteitä keskenään, sekä “remote access” VPN, jolla yrityksen työntekijä voi muodostaa yhteyden yrityksen verkkoon sen ulkopuolelta. Site-to-site VPN muodostetaan yleisesti kahden fyysisen laitteen kautta, kun taas remote access VPN:ssa yhteys yrityksen sisäverkkoon muodostetaan etäkäyttäjän tietokoneella olevan VPN-ohjelmiston avulla.

Katakrissa VPN:sta puhutaan salausratkaisuna. Turvallisuusluokalle hyväksyttyjen salausratkaisujen avulla voidaan liittää eri toimipisteiden turvallisuusluokiteltuja käsittely-ympäristöjä yhteen. I-01-osiossa mainitaan, että TL III järjestelmä voi olla tiedonsiirtojärjestelmä kahden tai useamman fyysisen pisteen välillä, jotka ovat turvallisuustasoltaan vastaavia. Kuvassa 7 on esitetty Katakrin mukainen ratkaisu.



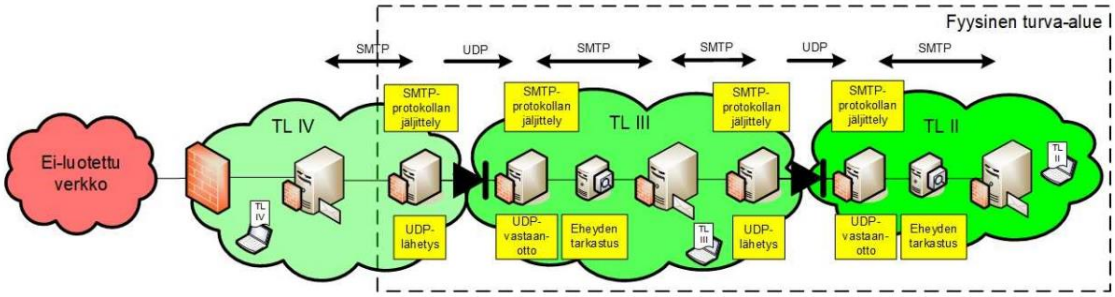
KUVA 7. Salausratkaisu tiedonsiirtojärjestelmässä

Salausratkaisun tulee olla turvallisuusluokalle hyväksytty. Hyväksyntään liittyy käytettävän laitteen lisäksi käyttöpolitiikka ja sen tarkastaminen. Turvallisuusluokalle hyväksytty salauslaite ei sellaisenaan riitä, vaan sen käyttötapaus ja määritetyt asetukset tulee hyväksyttää. Salausratkaisun tuomat hyödyt esimerkiksi kyvykkyydestä vahvaan liikenteen salaukseen eivät päde, mikäli niitä käytetään väärin.

4.5 Datadiodi

Datadiodi on yksisuuntainen yhdyskäytäväratkaisu. Sen toiminta perustuu OSI-mallin fyysisellä kerroksella tapahtuvaan tiedonsiirron yksisuuntaiseen rajoittamiseen, esimerkiksi yksisuuntaista valokuituyhteyttä käyttäen. Datadiodia voidaan käyttää esimerkiksi ohjelmistopäivitysten tuomiseen tai muuhun luontaisesti yksisuuntaiseen liikenteeseen matalamman turvatason verkosta korkeamman turvatason verkkoon. Datadiodin tärkein tehtävä on rajoittaa tiedon siirtosuuntaa ja estää tiedon valuminen korkeammasta turvatasosta matalampaan.

Datadiodeilla voidaan toteuttaa yhden tai useamman turvallisuusluokan ylittävä yhdyskäytäväratkaisu. Kuvassa 8 on kyberturvallisuuskeskuksen julkaisemasta yhdyskäytäväratkaisuohjeesta viitteellinen esimerkkitoteutus sähköpostiliikenteen tuomisesta TL II -ympäristöön. [(17), NCSA]



KUVA 8. Sähköpostin vienti korkeamman turvallisuusluokan ympäristöön [(17), NCSA]

Datadiodi vaatii luonteensa vuoksi lähetin- ja vastaanottopään datadiodin molemmin puolin. Nämä voidaan toteuttaa esimerkiksi palvelimina, jotka lähettävät ja vastaanottavat yhteydetöntä UDP-liikennettä. Turvallisuusluokitelluissa ympäristöissä datadiodin hyväksyminen osana ratkaisua edellyttää tyypillisesti myös siirrettävän datan eheyden tarkastusta sekä haittaohjelmaskannauksen.

Muissa kuin turvallisuusluokitelluissa ympäristöissä on vaikea nähdä tilannetta, jossa datadiodin käyttö osana yhdyskäytävää olisi perusteltua. Datadiodin käyttöönotto lähettimineen ja vastaanottimineen on työlästä, eikä internettiin kytketyissä ympäristöissä ole usein hyötyä tuoda päivityspaketteja sisään erillisiä yhdyskäytäviä pitkin.

5 POHDINTA

Työn tavoitteena oli tutustuttaa lukija turvallisuusluokiteltujen ympäristöjen vaatimuksiin Katakrin kautta. Tämä näkökulma valittiin lähestymistavaksi, koska Katakriin on koottu lakisääteiset turvallisuuden vähimmäisvaatimukset selkeästi jäsennellyssä muodossa toteutusesimerkkeineen. Aluksi työn aiheen rajaamista miettiessä oli ajatus pitää pääpaino turvallisuusluokitelluissa ympäristöissä. Työn kappalejaon kautta tehdyn hahmottelun myötä koin kuitenkin tärkeäksi tuoda aihealuetta myös lähemmäksi lukijaa. Tätä näkökulmaa varten aihealueita käsitellään työssä turvallisuusluokiteltujen ympäristöjen lisäksi yleisellä tasolla.

Työssä vaikeinta oli tehdä päätöksiä siitä, kuinka syvällisellä tasolla Katakrin vaatimuksia esitellään lukijalle. Liian syvällisellä tasolla kohtien läpikäymisessä ei olisi mitään järkeä, sillä silloin lukijan olisi parempi tutustua suoraan Katakriin. Toisaalta asioiden liian vähäinen läpikäyminen saattaisi herättää kysymyksiä Katakrista ja sen hyödyllisyydestä tietoturvallisuuden auditointikriteeristönä. Päätin lopulta keskittyä Katakrin I-osioon sen teknisyyden takia, esitellen kuitenkin myös T- ja F-osiot pintapuoleisesti. Näin lukija pystyisi työn kautta tutustumaan Katakrin osa-alueisiin helposti, ja saisi käsityksen mistä vaatimuksia turvallisuusluokitelluissa ympäristöissä on ja mistä ne tulevat. Tietenkin suosittelen lukijaa tutustumaan myös suoraan Katakri 2020 -julkaisuun, löydät sen sähköisesti lähdeluettelosta ensimmäisenä.

Katakrin osioista yleiselle tasolle asioiden poimimisessa oli vaikeinta päättää konkretian taso, eli kuinka tarkasti nostetuista asioita kerrotaan. Pyrin pitämään nämä nostot yleisellä tasolla, ja esimerkkien kautta tuomaan konkretiaa sekä herättämään ajatuksia, tavoitteena saada lukija pohtimaan oman ympäristönsä kautta näitä näkökulmia. Yleisen tason toteutusesimerkit olettavan tietoturvan vähimmäisvaatimusten jo täyttyvän kuvitellussa esimerkkiympäristössä.

Yhdyskäytäväratkaisuista kirjoittaessa valinta kohdistui Katakrissa mainittuihin ja viitattuihin toteutuksiin. Tämä oli mielestäni hyvä jatkumo Katakrin läpikäymiselle työssä, sillä näitä ei Katakrissa kovin tarkasti esitellä. Datadiodi mainitaan Katakrissa ainoastaan yksisuuntaisen liikenteen sallivan yhdyskäytäväratkaisun esimerkkinä sen enempää asiaa selittämättä. Vaikka Katakria ei luotu tarjoamaan valmiita ratkaisuja, on mielestäni tärkeä esitellä teoksessa mainitut laitteet edes yleisellä tasolla, jotta näiden käytön ja tarpeen voi paremmin ymmärtää. Yhdyskäytäväratkaisuissa on tästä syystä esitelty laitteiden toiminta, sekä perinteisemmät käyttötapaukset Katakrin kannalta, sekä yleisellä tasolla.

Lähteet on työssä esitetty siinä järjestyksessä, jossa ne tulevat työn aikana esille. Tämän tarkoituksena on helpottaa lukijaa tutustumaan aihepiireihin tarkemmin, mikäli työssä näiden esittelyn perusteella herää suurempi kiinnostus aiheisiin.

LÄHTEET

[1] Katakri 2020. Ulkoministeriön julkaisu. Saatavilla sähköisesti osoitteessa https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf

[2] Laki julkisen hallinnon tiedonhallinnasta 2019/906. Annettu Naantalissa 9.8.2019. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/laki/alkup/2019/20190906#Pidm45843170436160

[3] Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 28.11.2019/1101. Viitattu 26.5.2023. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/laki/ajantasa/2019/20191101

[4] Turvallisuusluokkien leimamallit. Valtiovarainministeriön julkaisuja. Saatavilla sähköisesti osoitteessa http://urn.fi/URN:ISBN:978-952-367-292-5

[5] Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä 2021:5. Valtiovarainministeriön julkaisuja. Saatavilla sähköisesti osoitteessa http://urn.fi/URN:ISBN:978-952-367-500-1

[6] Turvallisuusselvityslaki 19.9.2014/726. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/laki/ajantasa/2014/20140726

[7] CIS Benchmarks. Center for Internet Security julkaisema. Saatavilla sähköisesti osoitteesta https://learn.cisecurity.org/benchmarks

[8] Group Policy Management Console. Microsoftin dokumentaatiota. Saatavilla sähköisesti osoitteesta https://learn.microsoft.com/en-us/previous-versions/windows/desktop/gpmc/group-policy-management-console-portal

[9] Traficomin NCSA-toiminnon hyväksymät salausratkaisut. Saatavilla sähköisesti osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut

[10] Kiintolevyjen elinkaaren hallinta: ylikirjoitus ja uusiokäyttö. Kyberturvallisuuskeskus. Saatavilla sähköisesti osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf

[11] Defence in Depth. Tietoturvayhtiö Fortinetin artikkeli. Saatavilla sähköisesti: https://www.fortinet.com/resources/cyberglossary/defense-in-depth

[12] What is a 3-2-1 Backup Strategy. Tallennusmediayhtiö Seagaten blogista. Saatavilla sähköisesti: https://www.seagate.com/gb/en/blog/what-is-a-3-2-1-backup-strategy/

[13] Securing Network Infrastructure Devices. Cybersecurity & Infrastructure Security Agencyn blogista. Saatavilla sähköisesti: https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices

[14] 11 practical ways to keep your IT systems safe and secure. The Information Commissioner's Officen julkaisu. Saatavilla sähköisesti: https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/11-practical-ways-to-keep-your-it-systems-safe-and-secure/

[15] Cisco Networking Academy's Introduction to Routing Dynamically. Julkaisija Cisco Press, 2014. Saatavilla säköisesti osoitteessa https://www.ciscopress.com/articles/article.asp?p=2180210

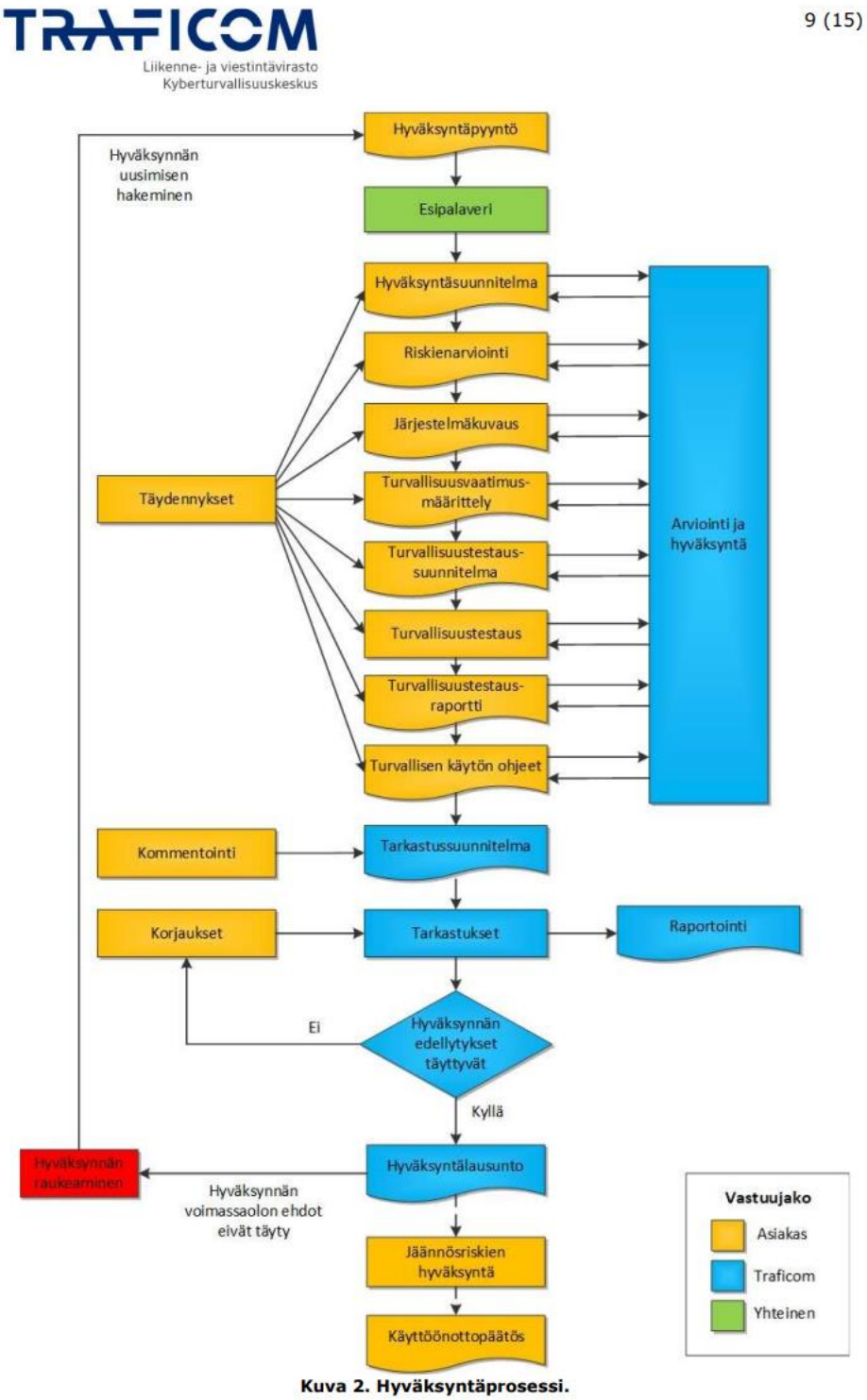
[16] Set Up a Basic Security Policy. Palo Alto Networksin dokumentaatio. Saatavilla sähköisesti: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/getting-started/set-up-a-basic-security-policy

[17] Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. Kyberturvallisuuskeskuksen julkaisu. Saatavilla sähköisesti osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf

LIITTEET

Liite 1. Liikenne- ja viestintäviraston hyväksyntäprosessi tietojärjestelmälle

Sähköisesti: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-tietojarjestelmien-arviointi-ja-hyvaksyntaprosesseista.pdf



Kuva 2. Hyväksyntäprosessi.

Liite 2. Kansallisen turvallisuusluokitellun tiedon käsittely ja säilytys Katakrista

Sähköisesti ulkoministeriön sivuilta: https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

F-04 – TIEDON KÄSITTELY JA SÄILYTYS TURVALLISUUSALUEILLA JA NIIDEN ULKOPUOLELLA

KANSALLISEN TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY JA SÄILYTYS

Turvallisuusluokka	Käsittely			Säilytys		
	Turvallisuusalueiden ulkopuolella	**Hallinnollinen alue**	**Turva-alue**	**Turvallisuusalueiden ulkopuolella**	**Hallinnollinen alue**	**Turva-alue**
TL II SALAINEN	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Ei** Päätelaitteessa: **Ei**	Paperiasiakirjat: **Ei** Päätelaitteessa: **Ei**	Paperiasiakirjat: **Kyllä**, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa
TL III LUOTTAMUKSELLINEN	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Ei** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Ei** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Kyllä**, soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa
TL IV KÄYTTÖ RAJOITETTU	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: **Kyllä**, tilapäisesti, ja lisäehtojen täyttyessä** Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa ja lisäehtojen täyttyessä*	Paperiasiakirjat: **Kyllä**, soveltuvassa lukitussa toimistokalusteessa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa	Paperiasiakirjat: **Kyllä**, soveltuvassa lukitussa toimistokalusteessa Päätelaitteessa: **Kyllä**, vaatimukset täyttävässä laitteessa

Lisäehdot:

* **Turvallisuusluokan III tai IV tietojen säilyttäminen vaatimukset täyttävässä päätelaitteessa hallinnollisella alueella tai turvallisuusalueiden ulkopuolella** on mahdollista, jos laitetta säilytetään:
  a) valvotussa tilassa (ks. F-05.5) tai
  b) soveltuvassa lukitussa toimistokalusteessa turvapussissa tai vastaavalla tavalla.

** **Turvallisuusluokan IV tiedon säilytys turvallisuusalueiden ulkopuolella** on mahdollista, jos tiedon käsittelijä:
  - on sitoutunut noudattamaan annetuissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä.