jamk

KATAKRI 2020 Arviointi Ympäristöön

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Kyberturvallisuuden hallinta TTC6020-3007
17.11.2024
Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

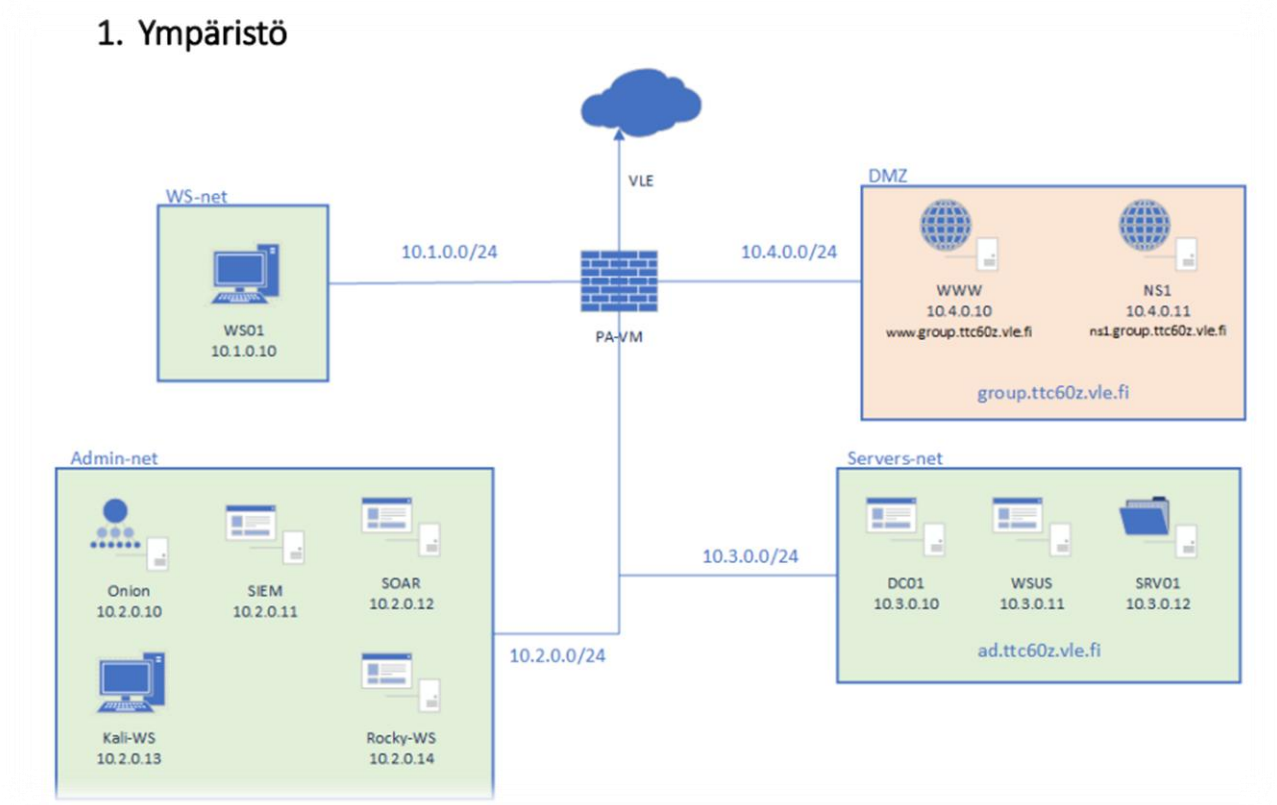
Kuviot

1 Johdanto

Kyberturvallisuuden hallinnan viimeisessä labrassa suoritetaan KATAKRI 2020 arviointi, Defend-ByVirtual yrityksessä (Kuvio 1). Labran tarkoituksena on kokeilla, miten arvioinnin vaatimukset täyttyvät ja jos eivät, mitä toimenpiteitä yrityksessä tulee tehdä.

Valitaan viisi arvioitavaa kohdetta Katakri 2020- arviointityökalun kriteereistä, jokaisesta työkalun osa-alueesta vähintään yksi. Katakrin osa-alueet ovat Turvallisuusjohtaminen (T), Fyysinen turvallisuus (F) ja Tekninen tietoturvallisuus (I).

Labran tavoitteena on ottaa selville, mikä Katakri 2020 on, miten sitä voidaan käyttää auditoinnissa ja tehdä muutaman Katakrin kriteerin pohjalta auditointi, jossa nähdään, miten yritys pärjää näitä vastaan. On myös hyvä muistaa auditoinnin merkitys jatkossa, koska sitä tultaisiin käyttämään DefendByVirtual-yrityksen kyberympäristön arviointiin, tasaisin väliajoin.



Kuvio 1. Laboratorio ympäristö

2 KATAKRI 2020

Katakri 2020 on suomalainen, viranomaisten ylläpitämä tietoturvallisuuden auditointityökalu. Katakri -auditointityökalun neljänteen versioon (Katakri 2020) päivityksessä on ollut mukana sekä viranomaisia että elinkeinoelämän edustajia. Päivitys oli tarpeellinen uusien, vuoden 2020 alussa tulleiden lainsäädäntöjen muutosten vuoksi. Myös digitaalinen tietojenkäsittelyn kehitys oli osasyynä päivitykseen. Katakri 2020 vahvistaa myös sen merkitystä suomalaisessa tietoturvassa ja tuo yleisesti Suomelle hyvää mainetta tietoturvaan liittyvissä asioissa. (Katakri 2020. 2020. Sivut 2 ja 5.)

Kuvio 2. Katakri 2020 dokumentista

Katakri 2020 tarkoituksena on arvioida organisaation kykyä suojata turvallisuusluokiteltua tietoa. Tieto voi olla luokiteltu kansallisesti tai kansainvälisesti. Katakrissa on Suomen lainsäädännön ja kansainvälisten toimijoiden tietoturvavelvoitteita, kuten laki julkisen hallinnon tiedonhallinnasta (906/2019) ja valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta, joihin sen vähimmäisvaatimukset perustuvat. Katakrin kriteerit eivät ole itsessään sitovia laillisesti, vaan sen avulla voidaan varautua muihin voimassa oleviin lain säädöksiin, kuten Suomen lain, EU:n ja muiden kansainvälisten toimijoiden turvallisuussääntöihin. (Katakri 2020. 2020. Sivu 5.)

2.1 Turvallisuusjohtaminen (T)

Tämä osa-alue käsittelee organisaation tietoturvallisuuden hallintajärjestelmää sekä menettelyjä, joilla varmistetaan turvallisuusluokiteltujen tietojen asianmukainen suojaus. Tavoitteena on varmistaa, että organisaatiolla on riittävät ja toimivat tietoturvallisuuden hallintakäytännöt sekä menettelyt henkilöstön turvallisuuden takaamiseksi. (Katakri 2020. Sivu 8.)

Keskeiset elementit: Tähän osa-alueeseen kuuluu johtamisen sitoutuminen tietoturvallisuuteen, riskienhallinta, turvallisuuspolitiikan dokumentointi ja henkilöstön tietoturvakoulutus. Vaatimuksilla varmistetaan, että organisaatio ymmärtää tietoturvariskit ja pystyy hallitsemaan niitä tehokkaasti. (Katakri 2020. Sivu 8.)

2.2 Fyysinen turvallisuus (F)

Tämä osa-alue keskittyy turvallisuusluokitellun tiedon käsittely- ja säilytyspaikkojen fyysiseen turvallisuuteen. Fyysiset turvallisuusvaatimukset varmistavat, että tietoa säilytetään ympäristöissä, joissa estetään asiattomien henkilöiden pääsy ja mahdolliset fyysiset uhkat. (Katakri 2020. Sivu 22-23.)

Keskeiset elementit: Osa-alue sisältää vaatimuksia esimerkiksi kulunvalvonnasta, kameravalvonnasta, lukituksesta ja paloturvallisuudesta. Näiden avulla organisaatiot voivat suojata tietoja fyysisesti niin, ettei ulkopuolisilla ole pääsyä turvallisuusluokiteltuun tietoon. (Katakri 2020. Sivu 22-23.)

2.3 Tekninen tietoturvallisuus (I).

Tekninen tietoturvallisuusosa-alue käsittelee vaatimuksia, jotka liittyvät teknisten järjestelmien turvallisuuteen. Näitä ovat erityisesti tietojenkäsittely-ympäristöihin ja tietoliikenteen suojaamiseen liittyvät vaatimukset, joilla pyritään turvaamaan tietojen luottamuksellisuus, eheys ja saatavuus. (Katakri 2020. Sivu 63-64.)

Keskeiset elementit: Tämä osa-alue kattaa tekniset suojatoimet, kuten palomuurit, salaus, pääsynhallinta, tietoverkkojen suojaus ja järjestelmien valvonta. Vaatimukset auttavat varmistamaan, että tiedot pysyvät suojattuina sekä ulkoisilta että sisäisiltä uhilta. (Katakri 2020. Sivu 63-64.)

3 Valitut kriteerit

Tässä esitellään, mitä kriteereitä on valittu (5 kriteeriä, vähintään 1 jokaisesta osa-alueesta) ja miten ne yleisellä tasolla voidaan tavoittaa Katakri 2020 mukaan. Seuraavassa kappaleessa käydään läpi, miten ne saadaan aikaiseksi DefendbyVirtual yrityksessä, ja vaaditaanko niiden toteuttamiseen erillisiä toimenpiteitä.

3.1.1 Kriteerit: Turvallisuusjohtaminen (T)

T-02 – TURVALLISUUSTYÖN TEHTÄVIEN JA VASTUIDEN MÄÄRITTÄMINEN:

T-02-kriteerin mukaan organisaatiossa tulee määritellä henkilöstön tehtävät ja vastuut tietoturvaan liittyvissä kysymyksissä. Tarkoituksena on, että jokainen toimija ymmärtää oman roolinsa tietoturvassa, ja omaa myös tarpeellisen osaamisen rooliin liittyen. Jos osaamista ei ole henkilöstöllä, johdon tulee järjestää koulutuksia, jotta osataan toimia tietoturvan periaatteiden mukaan. Kriteerin tavoite on saada tietoturva osaksi yrityksen toimintaa niin, että se ei ole vain IT:n vastuulla. Jokaisen henkilöstön jäsenen tulee ymmärtää oma osuutensa organisaation tietoturvaan liittyvissä asioissa. (Katakri 2020. Sivu 10.)

- **Vaatimus**: Organisaatio on määritellyt tietoturvallisuuden hoitamisen tehtävät ja vastuut. (Katakri 2020. s. 10.)

T-06 – TOIMINTAHÄIRIÖT JA POIKKEUSTILANTEET:

T-06-kriteerin tarkoituksena on varmistaa, että yrityksellä on toimenpiteet valmiina mahdollisten toimintahäiriöiden ja poikkeustilanteiden varalle, varsinkin turvallisuusluokiteltuja tietoja varten. Tavoitteena on fyysisten ja teknisten toimenpiteiden käyttö, jolla estetään esimerkiksi luvaton pääsy ja tietojen vuotaminen ulos organisaatiosta. Jotta häiriöiden ja poikkeustapausten vaikutus yrityksen toimintaan saadaan mahdollisimman pieneksi, määriteltyjä suojauskeinoja käytetään riskienhallinnassa ja yrityksen tietojen turvauksessa. (Katakri 2020. Sivu. 24.)

- **Vaatimus:** Organisaatiolla on määritetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta pienennettäisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen. (Katakri 2020. S. 24.)
  a) Organisaatio on huomioinut turvallisuusluokiteltujen tietojen suojaamisen hätä- tai häiriötilanteissa.
  b) Suojaustoimenpiteet ovat riittävät estämään luvattoman pääsyn turvallisuusluokiteltuihin tietoihin ja tietojen ilmitulon sekä turvaamaan niiden eheyden ja käytettävyyden.
  c) Turvallisuusluokitellut tiedot on suojattu teknisiltä ja fyysisiltä vahingoilta.

3.1.2 Kriteerit: Fyysinen Turvallisuus (F)

F-01 – FYYSISTEN TURVATOIMIEN TAVOITE:

F-01-kriteerin tarkoituksena on suojata organisaatiota fyysisillä toimenpiteillä, joilla estetään luvattomien pääsy turvallisuusluokiteltuihin tietoihin. Tiedot tulee käsitellä ja säilyttää suojatussa paikassa ja niihin ei saa olla pääsyä kuin vain erikseen määritellyillä organisaation henkilöillä, joilla on tarve käyttää sitä. Suojatoimilla estetään tuntemattomien pääsy tietoihin, ehkäistään tiedon päätyminen luvattomille henkilöille ja voidaan havaita yritykset päästä tietoihin henkilöiden toimesta, joilla niihin ei ole oikeutta päästä. Fyysisillä suojatoimilla voidaan varmistaa, että tiedot pysyvät niissä tiloissa ja niillä henkilöillä, joilla sen kuuluu olla. (Katakri 2020. Sivu 24.)

- **Vaatimukset:** Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin (Katakri 2020. 2020. s. 24.):

  a) Varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti.

b) Mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin tiedon saantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella.
c) Ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet.
d) Estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

3.1.3 Kriteerit: Tekninen tietoturvallisuus (I)

I-02 VÄHIMPIEN OIKEUKSIEN PERIAATE - TIETOLIIKENNE-VERKON VYÖHYKKEISTÄMINEN JA SUODATUSSÄÄNNÖSTÖT KO. TURVALLISUUSLUOKAN SISÄLLÄ:

I-02-kriteerin tarkoituksena on varmistaa organisaation tietoliikenneverkon suojaus. Verkon turvallisuussäännöt ja sen vyöhykkeet tulee olla tehtynä vähimpien oikeuksien periaatetta hyödyntäen. Käyttöoikeudet on siis rajattava vain niitä oikeasti tarvitseville henkilöille, tehtävänsä mukaan. Tietoliikenneverkko tulee olla monitasoisen suojauksen periaatteilla konfiguroitu, eli suojaus tehdään tavallaan monien suojakerroksien avulla, jotta voidaan varmistua organisaation tietoturvasta ja tietovuodoilta vältytään. Suojauksella pyritään pitämään turvallisuusluokiteltujen tietojen säilytys ja käsittely turvallisena. (Katakri 2020. Sivu 69.)

- **Vaatimus:** Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti. (Katakri 2020. s. 69.)

I-06 VÄHIMPIEN OIKEUKSIEN PERIAATE - PÄÄSYOIKEUKSIEN HALLINNOINTI:

Aiempaan kriteeriin liittyen, **I-06-kriteerin** tarkoituksena on varmistaa, että yrityksen tietojärjestelmien pääsyoikeuksia hallitaan vähimpien oikeuksien periaatteella. Periaatteen mukaan käyttöoikeuksia tulee myöntää vain niitä tarvitseville henkilöille, joilla on oikeus tietojen käsittelyyn ja olennainen tarkoitus (työtehtävä) päästä kyseisiin tietoihin. Pääsyn tulee olla rajoitettuna oikeuksiin, jotka ovat enintään tarpeen käyttäjälle tai automatisoidulle prosessille, jotta liikaa oikeuksia ei jaeta turhaan. Käyttöoikeuksia tulee myös valvoa säännöllisesti ja ne on pidettävä ajantasaisina. (Katakri 2020. Sivu 75.)

- **Vaatimus:**
  1. Tietojärjestelmien käyttöoikeudet on määritelty.
  2. Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksista (vrt. T-13) on varmistuttu.
  3. Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.
  4. Käyttöoikeudet on pidettävä ajantasaisina. (katakri 2020. 2020. S. 75.)

4 Katakri 2020 arviointi DefendByVirtual organisaatiossa

Seuraavaksi käymme läpi, miten kriteereihin vastataan ja miten ne saadaan aikaiseksi DefendByVirtual yrityksessä. Jos kriteerin vaatimuksiin ei vastata, täytyy laatia korjausohje, joiden pohjalta vaatimustaso saavutetaan.

4.1 Kriteerien arviointi

4.1.1 T-02 – TURVALLISUUSTYÖN TEHTÄVIEN JA VASTUIDEN MÄÄRITTÄMINEN

- **Vaatimus**: Organisaatio on määritellyt tieto turvallisuuden hoitamisen tehtävät ja vastuut. (Katakri 2020. s. 10.)

Arviointiprosessi:

DefendByVirtual-yrityksessä tietoturvallisuuteen liittyvät vastuut on selkeästi määritelty ja osoitettu päteville asiantuntijoille. Mikke Kuula toimii yrityksen turvallisuuspäällikkönä, kun taas Leevi Kauranen ja Samir Benjenna työskentelevät tietoturva-asiantuntijoina. Heidän työtehtäviinsä sisältyvät turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus, ja vastuut on määritetty organisaation tietoturvatavoitteiden mukaisesti. Mikke Kuulan vastuulla on varmistaa, että yrityksen turvallisuuskäytännöt ovat yhteneväisiä määriteltyjen politiikkojen kanssa ja noudattavat alan standardeja. Leevi Kauranen ja Samir Benjenna vastaavat teknisistä tietoturvatehtävistä, kuten verkon valvonnasta, pääsynhallinnasta sekä salaus- ja muiden tietosuojaa vahvistavien keinojen käyttöönotosta tietojen eheyden ja luottamuksellisuuden turvaamiseksi.

4.1.2 T-06 – TOIMINTAHÄIRIÖT JA POIKKEUSTILANTEET

- **Vaatimus:** Organisaatiolla on määritetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta pienennettäisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset turvallisuusluokiteltujen tietojen käsittelyyn ja säilyttämiseen. (Katakri 2020.2020. S. 24.)
  a) Organisaatio on huomioinut turvallisuusluokiteltujen tietojen suojaamisen hätä- tai häiriötilanteissa.
  b) Suojaustoimenpiteet ovat riittävät estämään luvattoman pääsyn turvallisuusluokiteltuihin tietoihin ja tietojen ilmitulon sekä turvaamaan niiden eheyden ja käytettävyyden.
  c) Turvallisuusluokitellut tiedot on suojattu teknisiltä ja fyysisiltä vahingoilta.

Arviointiprosessi:

1. Organisaatiolla on poikkeustilanteiden hallintaprosessi, joka selventää toiminnan hätä- tai häiriötilanteissa, kuten tietomurroissa, palvelunestohyökkäyksissä ja fyysisten vahinkojen sattuessa. Hallintaprosessi sisältää toimintavaiheet aina häiriön tunnistamisesta niiden raportointiin ja ratkaisuun. Organisaation tietoturvakäytännöissä on otettu huomioon erilaiset uhkaskenaariot, jotka voivat vaarantaa turvallisuusluokiteltujen tietojen käsittelyn tai säilytyksen.

2. Laitteet on suojattu vahvoilla salauksilla fyysisen vahingon, kuten luvattoman tunkeutumisen seurauksena. Organisaatiolla on ylimääräisiä suojatoimenpiteitä. Näihin toimenpiteisiin kuuluu esimerkiksi varmuuskopiointi ja tiedonsiirto turvallisiin etäpalvelimiin, jolloin tietoja voidaan suojata fyysisistä uhkista riippumatta.

3. Ympäristön suojaamiseen esimerkiksi tietomurroilta tai palvelunestohyökkäyksiltä käytetään palomuuria ja erillisiä haittatorjunta- ja valvontatyökaluja, kuten SIEM- ja SOAR järjestelmiä. Hyökkäyksen sattuessa pyritään havaitsemaan se ajoissa ja eristämään hyökkäyksen kohteen oleva verkkoalue tai laite. Pyritään pääsemään uhkasta eroon ja analysoida, mitä on vahingoittunut tai onko tietoja päässyt vuotamaan. Sen jälkeen palautetaan järjestelmä ennalleen. Tiedotetaan tapahtumasta viranomaisille ja oleellisille sidosryhmille. Tehdään myös jälkianalyysi tapahtuneesta.

4. Organisaatio säilyttää fyysiset turvallisuusluokitellut tiedot aina suojatuissa tiloissa, joihin pääsy on rajoitettu. Verkossa säilytettävät turvallisuusluokitellut tiedot sijaitsevat erillisessä verkossa, joka on eristetty muista verkoista. Näin varmistetaan, että vain valtuutetut henkilöt voivat päästä käsiksi tietoihin.

4.1.3 F-01 – FYYSISTEN TURVATOIMIEN TAVOITE

- **Vaatimukset:** Fyysisten turvatoimien tavoitteena on estää luvaton pääsy turvallisuusluokiteltuihin tietoihin (Katakri 2020. 2020. s. 24.):

  a) Varmistamalla, että turvallisuusluokiteltuja tietoja käsitellään ja säilytetään asianmukaisesti.

b) Mahdollistamalla henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin tiedon saantitarpeen ja tarvittaessa turvallisuusselvitysten perusteella.
c) Ehkäisemällä, estämällä ja havaitsemalla luvattomat toimet.
d) Estämällä oikeudetta tapahtuva tunkeutuminen tai viivyttämällä sitä.

Arviointiprosessi:

Turvallisuusluokiteltujen tietojen käsittely ja säilytys tapahtuvat suojatuissa ja valvotuissa tiloissa, joihin pääsy on rajoitettu vain tarvittaville henkilöille. Organisaatiossa on määritelty pääsyoikeuspolitiikka, jonka mukaisesti henkilöstö on jaettu tietoturvatarpeen mukaan luokiteltuihin pääsyoikeusryhmiin. Henkilöstön luokitus ja pääsy turvallisuusluokiteltuihin tietoihin perustuvat työtehtävien vaatimuksiin ja tarvittaviin turvallisuusselvityksiin. Ainoastaan valtuutetuilla työntekijöillä on oikeus käsitellä tiettyjä turvallisuusluokiteltuja tietoja, ja nämä oikeudet tarkistetaan ja päivitetään säännöllisesti. Mikke Kuula tarkistaa valvontajärjestelmät säännöllisesti varmistaakseen niiden toimivuuden. Lisäksi tiloihin on asennettu liiketunnistimia ja hälytysjärjestelmiä, jotka aktivoituvat luvattomasta liikkeestä. Organisaation tilat on varustettu useilla turvaesteillä, jotka viivyttävät ja estävät mahdollista tunkeutujaa. Näihin kuuluvat lujitetut sisäänkäyntiovet ja pääsy esteellisiin turva-alueisiin, kuten sulkutiloihin, joihin pääsy on mahdollista vain valtuutetun henkilökortin avulla.

4.1.4 I-02 VÄHIMPIEN OIKEUKSIEN PERIAATE - TIETOLIIKENNE-VERKON VYÖHYKKEISTÄMINEN JA SUODATUSSÄÄNNÖSTÖT KO. TURVALLISUUSLUOKAN SISÄLLÄ

- **Vaatimus:** Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti. (Katakri 2020. 2020. s. 69.)

Arviointiprosessi:

1. **Tietoliikenneverkon vyöhykkeistäminen**

Organisaation verkko on jaettu erillisiin vyöhykkeisiin. Vyöhykkeistäminen rajoittaa pääsyä erityyppisiin järjestelmiin ja tietoihin vähimpien oikeuksien periaatteiden mukaisesti. Organisaatiossa esimerkiksi Admin-net, Servers-net ja DMZ ovat erillisiä vyöhykkeitä. Vyöhykkeistämisen ansiosta eri

verkkojen liikennettä voidaan hallita erikseen. Tämä rajoittaa verkon laajuisten kyberhyökkäysten leviämistä.

2. **Suodatussäännöt ja palomuuri**

Vyöhykkeiden välinen liikenne kulkee aina palomuurin läpi. Palomuurissa on tarkat suodatussäännöt, jotka valvovat tulevaa ja lähtevää liikennettä sekä sallivat liikennettä vain rajoitetusti ja luotetuista IP-osoitteista, protokollista ja porteista, mikä toteuttaa vähimpien oikeuksien periaatetta. Ympäristön liikennettä rajoitetaan palomuurisäännöillä, jolla pystytään myös hallitsemaan organisaation sisäistä liikennettä. Palomuurilla valvotaan ja rajoitetaan, että vain erikseen hyväksytty, toiminnalle välttämätön liikenne sallitaan.

3. **Monitasoinen suojaus (defence in depth)**

Organisaatiossa käytetään monitasoista suojautumista eri vyöhykkeillä. Tämä sisältää pääsynvalvonnan (esim. VPN), IDS/IPS- järjestelmät sekä liikenteen valvonnan SOAR- ja SIEM järjestelmillä. Suojaus estää, että hyökkääjät eivät pääse ollenkaan tai eivät pääse suoraan kriittisiin järjestelmiin edes päästyään johonkin verkon osaan. Organisaation järjestelmiä on kovennettu ja pienennetty hyökkäyspinta-alaa esimerkiksi poistamalla tarpeettomia toimintoja.

4.1.5 I-06 VÄHIMPIEN OIKEUKSIEN PERIAATE - PÄÄSYOIKEUKSIEN HALLINNOINTI

- **Vaatimus:**
    1. Tietojärjestelmien käyttöoikeudet on määritelty.
    2. Tietojärjestelmien käyttöoikeudet voidaan myöntää vain henkilöille, joiden käsittelyoikeuksista (vrt. T-13) on varmistuttu.
    3. Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.
    4. Käyttöoikeudet on pidettävä ajantasaisina. (Katakri 2020. 2020. S. 75.)

Arviointiprosessi:

1. **Käyttöoikeuksien määrittely**

Jokaisen työntekijän ja tietojärjestelmän käyttöoikeudet on määritelty ja dokumentoitu heidän työtehtäviensä perusteella. Käyttöoikeuksien määritteleminen organisaatiossa tapahtuu group-policy säännöillä. Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilöt, jotka vastaavat organisaation henkilöiden käyttöoikeuksista.

2. Käyttöoikeuksien myöntäminen

Käyttöoikeuksien myöntäminen tapahtuu aina organisaation johdon sekä turvallisuuspäällikön kautta. Työntekijän käyttöoikeudet riippuvat, missä arvossa ja tehtävässä työntekijä työskentelee. Työntekijälle tehdään turvallisuusselvitys hänen työuransa alussa, jolla varmistetaan, onko työntekijä sovelias käyttöoikeuksiin.

3. Automaattisten prosessien käyttöoikeudet

Group-policyjen avulla olemme poistaneet sovelluksia ja automaattisia prosesseja käyttäjiltä sekä järjestelmältä rajataksemme pinta-alaa. Myös palomuuri käyttää tiukkoja sääntöjä rajatakseen uhkia. Tämä ehkäisee luvattoman pääsyn riskejä ja minimoi tietoturvariskit, joita liian laajat käyttöoikeudet voivat aiheuttaa.

4. Käyttöoikeuksien ajantasaisuus

Pääsyoikeudet tarkistetaan vähintään kuuden kuukauden välein, ja aina organisaation sisäisissä muutostilanteissa, kuten ylennysten tai tehtävämuutosten yhteydessä. Jos työntekijä irtisanoutuu tai hänen roolinsa muuttuu, hänen käyttöoikeutensa poistetaan tai päivitetään välittömästi. Jokaisesta myönnetystä käyttöoikeudesta jää myös dokumentti organisaation tiedostoihin.

5 Pohdinta

Katakri 2020 -arvioinnin tekeminen oli mielenkiintoinen prosessi, jossa pääsimme tarkastelemaan omaa ympäristöämme kriittisesti ja pohtimaan mitä olemme muiden opintojaksojen aikana tehnyt

ja miksi. Arviointi oli myös siinä mielessä hyvä tehdä, että olemme huomanneet, että monissa kyberturvallisuusalan työpaikoissa on vaatimuksena tai hyötynä Katakri 2020 tunteminen. Saimme harjoitusta tehdessä paljon hyvää oppia tulevaisuutta varten.

Ympäristömme vastasi tarkasteltujen kriteerien vaatimuksiin hyvin, mutta laajemmalla tarkastelulla löytyisi varmasti vielä epäkohtia, joita olisi hyvä korjata. Kaiken kaikkiaan olemme kuitenkin tyytyväisiä siihen, miten ympäristömme vastaa kriteeristöä.

Lähteet

Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. 2020. Viitattu 11.11.2024. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246