Antopäivä:	Voimaantulopäivä:	Voimassa:
[pp.kk.vvvv]	[pp.kk.vvvv]	toistaiseksi

Lainsäädäntö, johon suositus perustuu:
Laki kyberturvallisuuden riskienhallinnasta (XXXX/2024) 9 ja 18 §
Laki julkisen hallinnon tiedonhallinasta annetun lain muuttamisesta (XXXX/2024) 18 c §

Muutostiedot:

Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä

Sisällys

I. Suosituksen tausta ja tarkoitus

Suositus viranomaisille

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on laatinut tämän suosituksen valvoville viranomaisille NIS2-direktiivin mukaisten kyberturvallisuuden riskienhallinnan toimenpiteiden valvomiseksi. Suositus perustuu kyberturvallisuuden riskienhallinnasta annettuun lakiin (XXXX/2024) ja julkisen hallinnon tiedonhallinnasta annettuun lakiin (906/2019, jäljempänä tiedonhallintalaki) tehtyihin muutoksiin (XXXX/2024).

Suosituksen tarkoitus on tarjota viranomaisten käyttöön tietoa siitä, millaisia toimenpiteitä laissa säädettyihin vaatimuksiin voi kuulua. Suosituksessa kuvataan myös erilaisia keinoja, joita valvova viranomainen voi harkintansa ja tapauskohtaisen arvionsa mukaan käyttää ohjaus- ja valvontatehtävissään. Viranomainen voi myös käyttää apunaan oman organisaation ulkoisia tietoturvallisuuden arviointilaitoksia tai muita tietoturvallisuusammattilaisia. Ulkoisen avun käyttäminen voisi olla tarpeen esimerkiksi tilanteessa, jossa tarkastus edellyttäisi teknistä erityisosaamista tai laajoja teknologisia kyvykkyyksiä, mitä valvovalla viranomaisella ei itsellään ole. Tällaisia ovat esimerkiksi tilanteet, joissa valvovilla viranomaisilla ei ole tarvittavia työkaluja tai osaamista skannausten tekemiselle tai konfiguraatiokatselmointeihin.

Liikenne- ja viestintävirasto toteaa selvyyden vuoksi, että suositus ei sido viranomaisia eikä toimijoita, vaan oikeudellisesti sitovat velvoitteet säädetään laeissa,

mahdollisissa komission täytäntöönpanosäädöksissä ja mahdollisissa viranomaisen määräyksissä. Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää tästä suosituksesta poikkeavia, tiukempia vaatimuksia. Kukin valvova viranomainen on toimivaltainen ratkaisemaan, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla. Sääntelyn soveltamisalaan kuuluvan toimijan tulee puolestaan huolehtia siitä, että organisaation toiminta vastaa säädettyjä velvoitteita. Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

Annetut suositukset voivat tukea myös kyberturvallisuuden riskienhallinnasta annettavan lain 3 §:n mukaisten toimijoiden kyberturvallisuuden riskienhallinnan suunnittelua. Erityisesti luvussa 11 esitettyjä perustason tietoturvakäytäntöjä koskevat suositukset on laadittu siten, että myös sellaiset toimijat, jotka eivät kuulu NIS-sääntelyn soveltamisalaan voisivat suosituksia seuraamalla arvioida organisaationsa kyberturvallisuuden kypsyystasoa ja parantaa kyberturvallisuuden tilaa.

Liikenne- ja viestintävirasto toteaa, että suosituksessa mainittujen standardien tai yleisten viitekehysten täyttäminen tai Liikenne- ja viestintäviraston laatiman Kybermittarin käyttäminen ei takaa sitä, että toimija täyttäisi säädetyt velvoitteet kokonaisuudessaan.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on laatinut tämän suosituksen kyberturvallisuuden riskienhallinnan toimenpiteitä valvoville viranomaisille osana keskitetyn yhteyspisteen viranomaisyhteistyötä ja koordinointitehtävää.

Säädöspohja

Suosituksen taustalla on niin kutsuttu NIS2-direktiivi tai kyberturvallisuusdirektiivi, eli Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta.

NIS2-direktiivin 21 artiklassa säädetään kyberturvallisuusriskien hallintatoimenpiteistä. Artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin. Näiden toimenpiteiden on artiklan 2 kohdan mukaan perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö poikkeamilta. Artiklan 2 kohdan alakohdissa on lueteltu seikkoja, jotka mainitussa toimintamallissa vähintään tulee huomioida.

[Seuraavat kappaleet perustuvat hallituksen esityksen luonnokseen.]

NIS2-direktiivi on pantu kansallisesti täytäntöön uudella lailla kyberturvallisuuden riskienhallinnasta sekä tiedonhallintalakiin tehdyillä muutoksilla. Nämä kansallisen lainsäädännön muutokset tulevat voimaan 18.10.2024.

Kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan kuuluvat lain 3 §:ssä määritellyt eri toimialojen toimijat. Lain 9 §:ssä säädetään kyberturvallisuuden riskienhallinnan toimenpiteistä. Pykälän 1 momentin mukaan toimijoiden olisi toteutettava kyberturvallisuuden riskienhallinnan toimintamallin mukaiset oikeasuhteiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuudelle kohdistuvien riskien hallitsemiseksi ja haitallisten

vaikutusten estämiseksi tai minimoimiseksi. Pykälän 2 momentissa säädetään siitä, että kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä olisi huomioitava ja ylläpidettävä ajantasaisena vähintään momentin kohdissa 1–12 luetellut seikat. Tässä suosituksessa käsitellään näihin 12 kohtaan soveltuvia käytäntöjä omina lukuinaan.

Julkishallinnon toimijoiden osalta kyberturvallisuuden riskienhallinnan toimenpiteisiin liittyvät vaatimukset on pantu täytäntöön tiedonhallintalaissa. Lain 3 §:ssä säädetään tarkemmin, mitä julkishallinnon toimijoita vaatimukset koskevat. Tiedonhallintalaissa kyberturvallisuuden riskienhallinnan toimenpiteiden vaatimukset ovat uuden 4 a luvun 18 c §:ssä. Vaatimukset ovat saman sisältöisiä kuin laissa kyberturvallisuuden riskienhallinnasta.

Kyberturvallisuuden riskienhallinnasta annetun lain 18 §:n mukaan Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii NIS2-direktiivin 8 artiklan 3 kohdassa tarkoitettuna keskitettynä yhteyspisteenä. Pykälän 2 momentin mukaan keskitetyn yhteyspisteen tehtävänä on myös edistää valvovien viranomaisten välistä yhteistyötä ja koordinaatiota tämän lain mukaisten tehtävien toteuttamisessa. Säännöksen perusteluiden mukaan keskitetty yhteyspiste voisi edistää valvovien viranomaisten välistä yhteistyötä ja tiedonvaihtoa sekä antaa suosituksia valvoville viranomaisille tämän lain mukaisten vaatimusten ja valvonnan yhteensovittamiseksi.

Edellä mainitussa kansallisessa täytäntöönpanevassa sääntelyssä ei säädetä NIS2-direktiiviä tiukempia vaatimuksia, vaan direktiivi on pantu täytäntöön minimiharmonisoinnin periaatteen mukaisesti.

Suosituksen valmistelu ja ylläpito

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on tätä suositusta laatiessaan tarkastellut rinnakkain kansallista luonnosta hallituksen esitykseksi, NIS2-direktiiviä, direktiivin puitteissa käynnissä olevaa jäsenvaltioiden ja ENISAn yhteistä valmistelutyötä sekä lukuisia tietoturvallisuuden kriteeristöjä ja arviointityökaluja, kuten ISO/IEC 27001, IEC 62443, NIST CSF, Julkri ja Kybermittari. Näiden ja viraston eri tietoturvallisuustehtävissä kertyneen kokemuksen avulla on pyritty määrittämään kyberturvallisuuden kannalta yleiset käytännöt, jotka soveltuvat laissa esitettyihin kyberturvallisuuden riskienhallinnan toimenpiteisiin ja niiden valvomiseen.

Suosituksen valmistelun aikana on käyty keskusteluja nykyisten, jo NIS-direktiivin mukaista toimintaa valvovien ja uusien valvovien viranomaisten kanssa. Keskustelujen tarkoituksena on ollut muun muassa kartoittaa eri viranomaisten valvontaan kuuluvan toimijakentän laajuutta sekä viranomaisen valmiuksia uuden sääntelyn mukaiseen valvontaan. Keskusteluissa käytiin läpi erityisesti kysymyksiä valvonnassa tarvittavista osaamisesta ja resursseista sekä ulkoisen avun hankkimisesta. Viranomaiset toivoivat apua erityisesti teknisen kyberturvallisuuden valvontaan niin valvonnan suorittamiseen kuin valvontatulosten arviointiin. Näihin kysymyksiin on pyritty vastaamaan tässä suosituksessa, jota on täydennetty valmistelun aikana em. viranomaisten kanssa käytyjen keskustelujen pohjalta.

Suositusluonnoksesta pyydettiin lausuntoja Lausuntopalvelussa X.X.2024–X.X.2024. Lausuntopyyntö kohdistettiin erityisesti kyberturvallisuuden riskienhallinnasta annettavan lain mukaisille valvoville viranomaisille, mutta lausuminen oli mahdollista kaikille halukkaille.

[Lausuntopalautetta täydennetään lausuntokierroksen jälkeen.]

Suositus on voimassa xx.xx.2024 alkaen toistaiseksi. Suositusta päivitetään tarvittaessa sidosryhmiltä saadun palautteen ja käytännön kokemusten myötä.

Vaikutusten arviointi

Tietoyhteiskunta- ja turvallisuusvaikutukset

Kyberturvallisuuden riskienhallintaa koskevan uuden sääntelyn ja sitä kautta myös tämän suosituksen tavoitteena on viestintäverkko- ja tietojärjestelmäriippuvaisen yhteiskunnan turvallisuuden ja toimintavarmuuden parantaminen. Suosituksen valmistelun aikana käydyn ja suosituksen hyödyntämisessä käytävällä keskustelulla on mahdollista konkretisoida kyberturvallisuuden arviointia ja edistämistä eri toimialoilla.

Yhtenä osana uutta sääntelyä ovat perustason tietoturvakäytännöt (NIS2-direktiivissä kyberhygieniakäytännöt). Suosituksen alaluvussa 11 on esitetty suositukset perustason tietoturvakäytännöiksi, joita voivat hyödyntää kaikki yhteiskunnan toimijat riippumatta siitä, kuuluuko toimija säädettyjen velvoitteiden piiriin. Erityisesti tältä osin suosituksella on tarkoitus parantaa yhteiskunnan kyberturvallisuutta.

Viranomaisvaikutukset

Suosituksen tavoitteena on johdon- ja yhdenmukaistaa kansalliseen sääntelyyn liittyvää ohjausta, neuvontaa ja valvontaa yhteiskunnan tasolla. Suositus tarjoaa viranomaisille työkaluja, joita ne voivat käyttää toimijoiden kannalta ennakoivan materiaalin laatimisessa sekä neuvonnassa, ohjauksessa ja vaatimusten soveltamisessa, kuten myös mahdollisten kyberturvallisuuden riskienhallinnan toimenpiteitä koskevien määräysten laatimisessa. Suosituksen on tarkoitus toimia viranomaisille tukena, jotta niiden ei tarvitsisi luoda kaikkia menetelmiä ja käytäntöjä alusta alkaen. Valvovien viranomaisten osaaminen ja resurssit vaihtelevat, muun muassa siksi, että osalle viranomaisista kansallisen sääntelyn mukaiset tehtävät ovat uusia. Toimialojen eroista johtuen suosituksessa ei kuitenkaan voida käsitellä toimialakohtaisia erityispiirteitä.

Suosituksella tullee olemaan positiivisia vaikutuksia valvovien viranomaisten toimintaan ja se antaa osaltaan selkänojan eri valvovien viranomaisten yhteistyölle. Mikäli suositus omaksutaan laajasti, yhdenmukaistuvat eri valvovien viranomaisten valvontakäytänteet. Tämä myös edesauttaa viranomaistoiminnan läpinäkyvyyttä ja valvontatoiminnan ennakoitavuutta toimijoiden keskuudessa.

Suosituksen valmistelussa on pyritty teknologianeutraaliuteen ja yleispäteviin ratkaisuihin. Tulevaisuuden teknologioita on kuitenkin vaikea ennustaa, mikä voi aiheuttaa päivittämistarvetta suosituksen osalta. Suosituksen ajantasaisena pitäminen voi teknologian kehitysnopeuden vuoksi osoittautua haastavaksi.

Suositeltavien asioiden laajuudesta ja teknisestä luonteesta johtuen kevyemmällä informaatio-ohjauksella, kuten yksittäisiin tilanteisiin kohdistuvalla viranomaisneuvonnalla, ajoittain järjestettävillä koulutustilaisuuksilla tai viranomaisen Internet-sivuilla julkaistuilla usein kysytyt kysymykset -palstoilla ei arvioida olevan yhtä kattavaa vaikuttavuutta kuin suosituksella. Suosituksen avulla on mahdollista keventää toimijakohtaisen ohjauksen tarvetta.

Vaikutukset toimijoihin

Suositus edesauttaa sitä, että tulevaisuudessa kyberturvallisuusriskit arvioidaan kattavasti osana toimijan riskienhallintaa ja että toimintaympäristön muutokset ja vaikutus toimintaan tunnistetaan paremmin. Lisäksi suositus mahdollistaa riskienhallinnan toimenpiteiden oikeasuhteisen arvioinnin riskiin nähden ja tukee riskienhallinnan toteuttamisessa. Suosituksen mukaisia toimia toteuttamalla toimijat kykenevät palautumaan paremmin kyberhäiriötilanteista ja pystyvät näin ollen tuottamaan turvallisempia ja luotettavampia palveluita koko yhteiskunnalle.

Suosituksessa huomioidaan riskienhallinnan näkökulmasta myös hankinnat ja toimitusketjut. Suosituksen mukaisten toimien toteuttaminen mahdollistaa toimijalle paremman tilannekuvan muodostamisen siihen mahdollisesti kohdistuvista riskeistä. Erityisesti hankintojen osalta suosituksessa pyritään tarjoamaan työkaluja näihin liittyvien kyberriskien tunnistamiseen ja hallintaan.

Hyvästä riskienhallinnasta voi olla toimijalle monia etuja. Mikäli suosituksen avulla opitaan tekemään kyberturvallisuuden riskienhallintaa, voi se keventää toimijoiden taakkaa mahdollisessa toimialalla vaaditussa tai vapaaehtoisesti hankittavassa sertifioinnissa. Pitkällä aikavälillä jatkuvasti ylläpidetty ja hyvä riskienhallintajärjestelmä tukee toimijoiden liiketoimintaa ja auttaa tunnistamaan liiketoiminnan kehittämisen mahdollisuuksia. Suosituksen seuraaminen voi estää kyberriskin toteutumisen, jolloin häiriön selvittelyyn ja siitä toipumiseen ei kulu taloudellisia resursseja. Toimija voi suosituksen avulla myös oppia arvioimaan jäännösriskin merkityksen ja varautumaan siihen. Lisäksi toimija voi suosituksen avulla määritellä paremmin jäännösriskin ottamiseen liittyvän vastuunjaon.

Määritelmät

Tässä esitetyt määritelmät perustuvat suurelta osin kyberturvallisuuden riskienhallinnasta annetun lain ja sitä koskevassa hallituksen esityksessä esitettyihin määritelmiin sekä TEPA-termipankin[1] määritelmiin. Osa määritelmistä on laadittu itse. Kunkin määritelmän kohdalla esitetään lähdeviite.

Toimijalla (entity) tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa kyberturvallisuuden riskienhallinnasta annetun lain liitteessä I tai II tarkoitettua toimintaa tai on liitteessä I tai II tarkoitettua toimijatyyppiä ja täyttää tai ylittää keskisuuren toimijan määritelmän. (L kyberturvallisuuden riskienhallinnasta 3 §)

Viestintäverkolla ja tietojärjestelmällä (network and information system) tarkoitetaan

a) teledirektiivin[2] 2 artiklan 1 alakohdassa määriteltyä sähköistä viestintäverkkoa;

b) laitetta taikka yhteen kytkettyjen tai toisiinsa yhteydessä olevien laitteiden ryhmää, joista yksi tai useampi suorittaa ohjelman avulla digitaalisten tietojen automaattista käsittelyä; tai

c) digitaalisia tietoja, joita a ja b alakohdassa tarkoitetuissa järjestelmissä säilytetään, käsitellään, haetaan tai siirretään näiden järjestelmien toimintaa, käyttöä, suojausta tai ylläpitoa varten. (L kyberturvallisuuden riskienhallinnasta 2 §:n 1 mom. 27 k)

Poikkeamalla (incident) tarkoitetaan tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. (L kyberturvallisuuden riskienhallinnasta 2 §:n 1 mom. 15 k)

Merkittävällä poikkeamalla (significant incident) tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai

[1] Sanastokeskuksen erikoisalojen sanastojen ja sanakirjojen kokoelma https://termipankki.fi/tepa/fi/

[2] Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972 Eurooppalaisesta sähköisen viestinnän säännöstöstä

asianomaiselle toimijalle taloudellisia tappioita taikka jos poikkeama on vaikuttanut tai voisi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Riskienhallinnan toimintaperiaatteilla (risk management policy) tarkoitetaan organisaation ylimmän tason suunnittelua, jolla tunnistetaan, arvioidaan ja käsitellään järjestelmällisesti organisaatioon tai sen toimintaan kohdistuvia riskejä, asetetaan päämäärät ja seurataan niiden toteutumista. Vastaavista toimintaperiaatteista voidaan käyttää termiä riskienhallintapolitiikka. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Riskienhallinnan toimintamallilla (risk management procedure/process) tarkoitetaan riskienhallinnan prosessia, jolla tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä säännöllisesti. Osana riskienhallinnan toimintamallia käsiteltyjen riskien hallintatoimenpiteiden vaikuttavuutta arvioidaan sopivin mittarein. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Riskienhallinnan toimenpiteillä (risk management measures) tarkoitetaan toimijan toteuttamia toimenpiteitä viestintäverkkojen ja tietojärjestelmien turvallisuudelle kohdistuvien riskien hallitsemiseksi, ehkäisemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Turvallisuutta koskevilla toimintaperiaatteilla (information security policy) tarkoitetaan toimijan näkemystä viestintäverkkojen ja tietojärjestelmien tietoturvan päämääristä, periaatteista ja toteutuksesta koko elinkaaren ajan. ISO/IEC 27001 -standardin yhteydessä vastaavista toimintaperiaatteista käytetään termiä tietoturvapolitiikka. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Turvallisuutta koskevilla menettelyillä (information security procedures/processes) tarkoitetaan erilaisia prosesseja ja teknisiä menettelytapoja, joilla toteutetaan viestintäverkkojen ja tietojärjestelmien turvallisuuteen liittyviä toimintaperiaatteita. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Turvallisuutta koskevilla käytännöillä (information security practices) tarkoitetaan tietoturvallisuuteen ja kyberturvallisuuteen liittyviä toimintatapoja, joilla käytännössä toteutetaan turvallisuutta koskevat menettelyt. (L kyberturvallisuuden riskienhallinnasta, hallituksen esityksen perustelut)

Todentamisella tai todennuksella (verification) tarkoitetaan menettelyä, jolla pyritään varmistumaan kohteen todenmukaisuudesta, oikeellisuudesta tai alkuperästä. Todentamista on eri tasoista, se voi olla vahvaa tai heikkoa, ja se voidaan tehdä halutulla varmuustasolla. (TEPA-termipankki)[3].

Tässä suosituksessa todentamista tai todennusta (authentication) voidaan käyttää myös osana pääsynhallintaa, jolloin termin määritelmä on tuotu erikseen esiin.

II. Suosituksen lukuohje

Seuraavissa luvuissa on kussakin keskitytty yhteen kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentissa lueteltuun kyberturvallisuuden riskienhallinnan toimenpiteeseen. Toimenpiteet on esitetty samassa järjestyksessä kuin laissa.

[3] Sanastokeskuksen erikoisalojen sanastojen ja sanakirjojen kokoelma https://termipankki.fi/tepa/fi/

Toimenpiteiden ja niiden valvonnan toteuttamisessa muunlaiset kuin tämän suosituksen mukaiset etenemisjärjestykset voivat olla perusteltuja. Lisäksi valvontatoimissa voi olla perusteltua keskittyä erityisesti niihin valvonnallisiin toimenpiteisiin, jotka ovat valvottavan toimialan tai toimijan kohdalla tärkeimpiä.

Kukin esitetyistä kyberturvallisuuden riskienhallinnan toimenpiteistä jakautuu edelleen täsmällisemmiksi suosituksiksi, jotka esitetään luettelon muodossa. Suositusluettelon jälkeen selostetaan taulukoissa yksityiskohtaisemmat perustelut kullekin suositukselle.

Toteutusesimerkit

- Toteutusesimerkeissä kuvataan, millä tavoin taulukossa kuvattu suositus tai sen osia voidaan toteuttaa ja millaisia toteutuksia valvova viranomainen saattaa kohdata valvonnan yhteydessä.
- Toteutusesimerkit eivät ole tyhjentäviä, vaan niiden tarkoituksena on antaa esimerkkejä erityisesti sellaisiin tilanteisiin, joissa aikaisempaa kokemusta suosituksessa kuvattujen asioiden toteutuksesta ei ole. Toteutusten laajuuden tulisi kuitenkin olla sopivassa suhteessa toimintaan liittyvään riskiin ja muuhun toiminnan vaatimuksiin.
- Tarvittavat toimenpiteet voivat vaihdella merkittävästi toimijan koon, toimialan ja toimijaan kohdistuvien uhkien perusteella. Toteutusesimerkeissä on kuitenkin pyritty ottamaan huomioon erilaisia toimijoita ja näiden erilaisia tarpeita mahdollisuuksien mukaan.

Todennus

Todennuksessa kuvataan esimerkkejä siitä, miten valvova viranomainen voi todentaa toimijan kyberturvallisuuden riskienhallinnan toimenpiteiden toteutumista. Todennusesimerkit on jaettu kolmeen eri kategoriaan keinojen teknisen vaativuuden perusteella. Eri kategorioiden mukainen valvonta antaa eritasoista varmuutta toimijan kyberturvallisuuden tilasta tarkastushetkellä. Eri kategorioiden toimenpiteitä voidaan valikoida käytettäväksi myös käytettävissä olevien resurssien mukaan.

1. Kategoriassa 1 kuvataan pääasiassa dokumentaatioon tai itsearvioon perustuvaa valvontaa. Dokumentaatioon tai itsearviointiin perustuva tarkastelu antaa harvoin syvällistä kuvaa todellisesta kyberturvallisuuden tilasta. Siksi on suositeltavaa valita tarkasteltavaksi ainakin joitain asioita kategorioista 2 tai 3. Kategorian 1 toteutusesimerkkejä käyttämällä valvova viranomainen voi kuitenkin saada suhteellisen kevyesti laajan käsityksen toimialan kokonaistilasta kohdentamalla saman tyyppisen valvonnan tai itsearvioinnin suureen joukkoon toimijoita.
2. Kategoriassa 2 kuvataan syvemmälle menevää, toimijan toimenpiteiden nykytilan katselmointia. Kategoria keskittyy kuitenkin teknisesti kevyihin menetelmiin, kuten haastatteluihin, konfiguraatiokatselmointeihin tai muuhun vastaavaan näyttöön. Kategorian 2 tarkastelussa voidaan tyypillisesti hyödyntää toimijan toimittamaa teknisempää näyttöä.
3. Kategoriassa 3 kuvataan teknisesti monipuolisempia menetelmiä, jotka vaativat yleensä valmistelua ja erilaisia valmiuksia, kuten erilaisten ohjelmien ja työkalujen käyttöä sekä kykyä tulkita teknistä dataa. Tällaisia voivat olla esimerkiksi erilaiset skannaukset, joita voi viranomaisen lisäksi suorittaa myös toimija itse tai kolmas osapuoli.

Valvonnassa on suositeltavaa käyttää eri kategorioiden menetelmiä myös esimerkiksi toimialariskeihin tai toimialan luonteesta johtuviin haavoittuvuuksiin

perustuen. Viestintäverkot ja tietojärjestelmät voivat olla hyvin eri laajuisia ja teknologialtaan eriäviä ja niihin liittyy paljon kyberturvallisuuteen vaikuttavia yksityiskohtia. On myös tyypillistä, että itsearviointi ja dokumenttien katselmointi eivät anna realistista kuvaa viestintäverkon ja tietojärjestelmän kyberturvallisuuden tilasta. Itsearviointi riippuu luonnollisesti myös itsearvioinnin tekijän kokemustaustasta ja käytettävissä olevasta ajasta. Muilla todentamiskeinoilla voidaan täydentää itsearvioinneilla saatavaa kuvaa järjestelmän tilanteesta.

Valvova viranomainen harkitsee, mitä keinoja se kulloinkin katsoo tarpeelliseksi käyttää valvontatoiminnassaan. Sen lisäksi, että viranomainen saa selvitystä ja näyttöä toimijalta, viranomainen voi tehdä itse tarkastuksia ja muuta havainnointia tai käyttää apunaan ulkoisia arviointitahoja kuten tietoturvallisuuden arviointilaitoksia tai muita päteviä tietoturvallisuuden ammattilaisia. Joissain tilanteissa valvonta voi edellyttää myös yhteistyötä toisen valvovan viranomaisen kanssa Suomessa tai toisessa jäsenvaltiossa.

Perustelut

Perusteluissa esitetään joitain käytännön perusteluita sille, miksi otsikon mukainen toimenpide on nostettu lainsäädäntöön ja sisällytetty suositukseen, sekä mihin sillä pyritään.

Perustelut tarjoavat työkaluja keskusteluun valvovan viranomaisen ja toimijan välillä vaatimusten perusteista. Perustelut auttavat valvovaa viranomaista tulkitsemaan, suojaavatko toimijan toteuttamat toimenpiteet esimerkiksi perusteluissa mainittuja uhkanäkökulmia vastaan.

Joissakin kohdin perustelut on jätetty kirjoittamatta. Tällöin on katsottu, että erillisten perusteluiden esittäminen ei tuo lisäarvoa taulukossa jo esitettyjen toteutusesimerkkien tai valvontakeinojen lisäksi.

Viitteet

Viitteissä annetaan esimerkkejä laajasti tunnetuista standardeista, viitekehyksistä ja ohjeistuksista, jotka liittyvät kyseiseen suositukseen. Näistä valvova viranomainen voi hakea lisää tietoa tai kuvauksia yleisesti käytetyistä toteutuksista.

Listaus on esimerkinomainen ja siihen on pyritty nostamaan sellaisia standardien ja viitekehysten täsmällisiä kohtia, jotka erityisesti palvelevat kunkin suosituksen tavoitteita. Toimialalla voi olla käytössä muitakin relevantteja standardeja ja viitekehyksiä.

Työkalut

Työkaluissa mainitaan arviointivälineitä ja mittareita sekä työkaluja ja ohjelmistoja, joita valvova viranomainen voi hyödyntää valvontatoimissaan. Myös toimija voi käyttää työkaluja oman kypsyystasonsa mittaamiseksi ja toiminnan kehittämiseksi.

1 Kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan f alakohtaan sekä osin a alakohtaan. Näiden alakohtien kansallisesta täytäntöönpanosta säädetään

kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 1 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 1 kohdassa.

1. **Kyberturvallisuuden riskienhallinnan toimintamalli**: Toimijalla tulisi olla käytössään kyberturvallisuuden riskienhallinnan toimintamalli, jolla tunnistetaan, analysoidaan, arvioidaan ja käsitellään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä säännöllisesti. Riskienhallinnan tulisi olla luonteeltaan jatkuva osa organisaation toimintaa. Se edellyttää, että toimintaperiaatteiden ja toimenpiteiden vaikuttavuuden arviointi on yksi noudatettavista hallintatoimenpiteistä. Kyberturvallisuuden riskienhallinnan toimintamallin olisi suositeltavaa perustua ajantasaisiin toimialalla omaksuttuihin parhaisiin käytänteisiin ja standardeihin. (Ks. kohta 1.1 ja 1.1.1).

2. **Kaikki vaaratekijät huomioiva lähestymistapa**: Riskienhallinnassa tulisi noudattaa kaikki vaaratekijät huomioivaa lähestymistapaa ja varmistaa, että yrityksen hallintotapa ja riskienhallintaprosessit ottavat huomioon kyberturvallisuusriskit. (Ks. kohta 1.2).

3. **Tarpeiden ja toimintojen tunnistaminen**: Riskienhallinnan lähtökohtana tulisi olla tunnistaa luottamuksellisuuteen, eheyteen, saatavuuteen ja aitouteen liittyvät tarpeet sekä sen kohteena toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt. Tätä tunnistamista tarkennetaan omaisuudenhallintaa koskevassa kohdassa 5. (Ks. kohta 1.3).

4. **Uhkien tunnistaminen**: Lisäksi tulisi tunnistaa toimijaan kohdistuvat yleisesti kyberturvallisuuteen liittyvät ja toimialalle ominaiset uhkat ja arvioida näiden todennäköisyydet sekä vaikutukset. Tämä on edellytys riskienhallintatoimenpiteiden oikeasuhtaisuuden arvioinnille. (Ks. kohta 1.4 ja 1.4.1).

5. **Riskien käsittely**: Riskienhallinnan tavoitteena on riskien käsittely niin, että niiden todennäköisyys tai vaikutus on minimoitu, poistettu tai ulkoistettu eli huolehdittu riskien käsittelystä sopimussuhteissa. Riskien käsittelyn lopputuloksena muodostuneet jäännösriskit on hyväksytty perustellusti. (Ks. kohta 1.5).

6. **Riskienhallinnan vaikuttavuuden arviointi ja mittaristo**: Riskienhallinnan vaikuttavuutta olisi arvioitava säännöllisesti sopivin mittarein niin, että valittujen toimenpiteiden toimivuutta voitaisiin mitata ja tarvittaessa parantaa. Arvioinnin voisi tehdä itsearviointina tai hyödyntää riippumattomia tietoturvapalveluntarjoajia. (Ks. kohta 1.6 ja 1.6.1).

1.1 Kyberturvallisuuden riskienhallinnan toimintamalli

Toteutusesimerkit
• Toimijalla on käytössä kyberturvallisuuden riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Kyberturvallisuuden riskienhallinnan toimintamalli on keskeinen osa toimijan riskienhallinnan kokonaisuutta. Riskienhallinnan toimintamalli on yleensä osa organisaation johtamisjärjestelmää ja tukee organisaation liiketoimintastrategiaa. Ylin johto on hyväksynyt riskienhallinnan toimintamallin sekä tietoturvan ja riskienhallinnan kannalta tärkeät roolit, vastuut ja valtuudet ks. kohta 6.1 Henkilöstöturvallisuuden menettelyt.

- Toimija on dokumentoinut riskienhallinnan toimintamallin ja se on saatavilla. Dokumentaatiosta käy ilmi toimintaperiaatteet, kuten riskienhallintaprosessi, johdon sitoutuminen, riskienhallinnan kannalta tärkeät roolit ja vastuut, toimintamallin arviointi ja kehittäminen sekä riskienhallinnan toimenpiteiden vaikuttavuuden arviointi ja mittaaminen.
- Riskienhallinnan toimintaperiaatteet ja toimenpiteet ovat toimijan tarpeisiin sopivat, niitä on kehitetty jatkuvasti ja toimintaympäristön muuttuessa. Osana hallintatoimenpiteitä tulisi arvioida myös niiden vaikuttavuutta, jotta varmistetaan että valitut riskienhallinnan toimenpiteet ovat ajantasaisia. Ks. kohta 1.6 Vaikuttavuuden arviointi.
- Riskienhallinnan toimintamallin on suositeltavaa perustua yleisesti tunnettujen standardien mukaisiin riskienhallintamenetelmiin ja työkaluihin tai toimialalla omaksuttuihin parhaisiin käytänteisiin.
- Riskienhallinnan toimintamalliin on suositeltavaa sisällyttää myös toimialakohtaiset toimintaperiaatteet ja säännöt, standardit ja toimialakohtainen sääntely.
- Toimija on tehnyt riskienhallintaa säännöllisesti ja erityisesti silloin kun toiminnassa tai toimintaympäristössä tapahtuu muutoksia tai merkittäviä poikkeamia.
- Toimija on sisällyttänyt riskienhallintaprosessiin riskienhallintaan tarvittavat vaiheet, kuten riskien tunnistamisen, analysoinnin ja vaikutusten arvioinnin sekä menettelyt niiden käsittelyyn mukaan lukien johdon katselmukseen, korjaaviin toimenpiteisiin sekä jatkuvaan parantamiseen. Ks. kohta 1.5 Riskien käsittely.

Todennus

1. Valvova viranomainen todentaa, että toimijalta löytyy dokumentoitu kyberturvallisuuden riskienhallinnan toimintamalli ja ohjeet, ja että ne ovat henkilöstön saatavilla. Toimintamallista käy ilmi riskienhallintaprosessin eri vaiheet kuten riskien tunnistaminen, analysointi, arviointi ja käsittely. Toimintamallista käy ilmi, miten kyberturvallisuuden riskienhallintaa toteutetaan osana organisaation toimintaa ja miten riskienhallinnassa huomioidaan viestintäverkkojen ja tietojärjestelmien sekä niiden fyysisen ympäristön riskit, sekä miten toimija on sisällyttänyt riskien hallintatoimenpiteisiin toimintaperiaatteiden ja toimenpiteiden vaikuttavuuden arvioinnin. Toimintamallista käy ilmi myös, miten johdon vastuu toteutuu riskienhallinnan toimintamallissa sekä mahdolliset riskienhallintaan liittyvät roolit ja valtuutus (ks. 6.1). Riskienhallinnan toimintamallista käy ilmi riskienhallinnan säännöllisyys ja jatkuvuus, jota voi arvioida myös katselmoimalla toimintamallin muutoshistoriaa. Mikäli toimintamalli perustuu johonkin standardiin tai viitekehykseen, ilmenee se selkeästi dokumentaatiosta. Dokumentaatiosta käy ilmi, mitä standardia tai viitekehystä on käytetty ja miten sitä on sovellettu (miltä osin käytössä ja miltä osin ei).
2. Valvova viranomainen todentaa haastattelemalla toimijan henkilöstöä, miten kyberturvallisuuden riskienhallinnan toimintamallia ylläpidetään ja kehitetään. Haastatteluista käy ilmi, että riskienhallintaa tehdään viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysisen ympäristön riskeihin. Riskienhallinnan toimintamallin toteutuminen käytännön tasolla todennetaan haastattelemalla henkilöstöä riskienhallinnan toimintamallista ja kyberturvallisuusriskien ilmoituskäytännöistä organisaatiossa. Henkilöstö osaa soveltuvilta osin tehdä riskienhallintaa osana päivittäistä työtä. Henkilöstö osaa ilmoittaa havaitsemistaan riskeistä ja poikkeamista (ks. 9).

Perustelut
Toimijan toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvia riskejä tulisi tunnistaa, arvioida ja hallita säännöllisesti ja kiinteänä osana organisaation riskienhallintaa. Riskienhallinnan toimintamallia tulisi arvioida säännöllisesti ja aina kun toimintaympäristössä tapahtuu muutoksia. Toimintaansa nähden oikeinmitoitetulla riskienhallinnalla estetään ja minimoidaan poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin.
Viitteet
COSO Enterprise Risk Management Framework IEC 62443-2-1:2013 (4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13, 4.3.2.6.3, 4.3.2.6.5, 4.3.2.6.6, 4.3.3.2.6, 4.3.4.2) IEC 62443-2-4:2019 (SP 02.01, SP 03.01) ISO/IEC 27001:2022 (6.1, 6.2, 8.2, 8.3) ISO/IEC 27005:2022 ISO 31000:2018 NIST CSF 1.1 (ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6, ID.GV-4, ID.RM-1, ID.RM-2, ID.RM-3) NIST CSF 2.0 (ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-03, GV.RM-01, GV.RM-02, GV.RM-03) NIS CG Reference document (3.3.1 Risk management framework) Valtionneuvoston riskienhallinnan käsikirja valtiohallinnon toimijoille
Työkalut
Julkri (HAL-06) Kybermittari (CRITICAL-2, RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, THIRD-PARTIES-2, ARCHITECTURE-1)

1.1.1 Riskienhallinnan toimintamalli - laajennettu ohjeistus

Toteutusesimerkki
Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa. • Kohdan 1.1 lisäksi toimija on luonut ja ylläpitänyt itselleen sopivaa riskien käsittelykriteeristöä. Käsittelykriteeristössä on määritelty toimijalle soveltuvat menettelyt eri riskitasojen määrittelyyn ja niiden käsittelyyn. • Riskien käsittelykriteeristö voi sisältää käytännöt riskien käsittelytapojen valintaan, joita voivat olla esimerkiksi riskin ottaminen, vaikutusten minimointi, poistaminen ja ulkoistaminen.

- Riskien käsittelykriteeristöstä tulisi käydä ilmi toimijan riskinsietokyky ja käytännöt jäännösriskin hyväksymiseen.

Todennus

1. Valvova viranomainen todentaa, että toimija on määritellyt ja riittävällä tasolla dokumentoinut riskien käsittelykriteeristön.
2. Valvova viranomainen varmistaa riskien käsittelykriteeristön toteutumista arvioidaan katselmoimalla riskienkäsittelyä ja jäännösriskien kirjaamista. Lisäksi kriteeristöjen soveltamista voi todentaa haastattelemalla henkilöstöä niiden soveltamisesta.

Perustelut

Osana riskienhallinnan toimintamallia määritellyt kriteeristöt auttavat organisaatiota tuottamaan keskenään vertailukelpoisia riskiarviointeja.

Viitteet

ISO/IEC 27001:2022 (6.1.2)

ISO 31000:2018 (6.3.2, 6.3.4)

NIST CSF 1.1 (ID.RM-2, ID.RM-3)

NIST CSF 2.0 (GV.RM-02, GV.RM-03)

NIS CG Reference document (3.3.1 Risk management framework)

Työkalut

Julkri (HAL-06)

Kybermittari (RISK-3, RISK-4)

1.2 Kaikki vaaratekijät huomioiva lähestymistapa

Toteutusesimerkki

- Osana toimijan hallintotapaa ja riskienhallinnan toimintamallia toimija on arvioinut viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvia riskejä kaikki vaaratekijät huomioivalla lähestymistavalla.
- Toimija on arvioinut sisäpiiriuhkan, ulkoisen uhkan tai fyysisen uhkan vaikutusta tiedon tai palvelujen luottamuksellisuuteen, eheyteen, aitouteen ja saatavuuteen ja ottaa ne huomioon omassa riskienhallinnan toimintamallissaan. Muita tällaisia uhkia voivat olla esimerkiksi tietoliikennekatkos, sähkökatkos, varkaus, ilkivalta, tulipalo, ankarat sääolosuhteet, luonnonmullistukset ja katastrofit.
- Toimija on huomioinut riskiarviointiin muiden osapuolten aiheuttamat riskit. Ks. kohdat 3.2 Hankinnan kohteen turvallisuus ja 4.2 Toimitusketjujen riskienhallinta.
- Riskiarviointiin sisältyvät myös henkilöstöön ja pääsynhallintaan liittyvät riskit. Ks. kohdat 6 Henkilöstöturvallisuus ja kyberturvallisuuskoulutus ja 7 Pääsynhallinnan ja todentamisen menettelyt.

- Toimenpiteitä fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi tarkennetaan kohdassa 12 Toimenpiteet fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Todennus

1. Valvova viranomainen katselmoi, että toimija on ottanut kyberturvallisuuden riskienhallinnan toimintamallissaan ja riskiarvioissaan huomioon kaikki olennaiset vaaratekijät. Toimintamallista käy ilmi, että yrityksen hallintotavassa ja riskienhallintaprosesseissa otetaan huomioon kyberturvallisuusriskit. Toimijan riskiarvioinnista käy ilmi, että viestintäverkkoihin ja tietojärjestelmiin kohdistuvat riskit ovat kattavia ja pitävät sisällään mm. fyysisiä, teknisiä ja henkilöön perustuvia riskejä.

Perustelut

Kaikki vaaratekijät huomioivalla lähestymistavalla on tarkoitus huomioida kaikki kohtuudella ennakoitavissa olevat viestintäverkkoihin ja tietojärjestelmiin kohdistuvat uhkatekijät. Mitä merkittävämpi viestintäverkko tai tietojärjestelmä on toimijalle, sitä kattavammin siihen kohdistuvia uhkia tulisi arvioida. Tällä lähestymistavalla voi edistää toimijan varautumista erityyppisiin uhkiin ja varmistaa, että esimerkiksi tiettyihin kategorioihin liittyviä uhkia ei jäisi liikaa huomioimatta.

Viitteet

IEC/TR 62443-3-1:2013 (4.2.3.7)

ISO/IEC 27001:2022 (6.1.1)

ISO 31000:2018 (6.3.3)

NIST CSF 1.1 (ID.RA-5)

NIST CSF 2.0 (ID.RA-05)

NIS CG Reference document (2.2 All Hazard approach)

Työkalut

Julkri (FYY-01)

Kybermittari (CRITICAL-2, RISK-1, PROGRAM-1, PROGRAM-2)

1.3 Tarpeiden ja toimintojen tunnistaminen

Toteutusesimerkki

- Toimija on tunnistanut toimintojen kannalta keskeiset palvelut, järjestelmät, prosessit ja henkilöt ja sisällyttänyt niiden tietoturvatarpeet osana riskienhallintaan. Tätä kohtaa tarkennetaan kohdassa 5 Omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen.
- Toimija on tunnistanut, dokumentoinut ja tehnyt riskiarvion viestintäverkoille ja tietojärjestelmille mukaan lukien yksittäisille laitteille, palveluille tai

tietojärjestelmille, joiden häiriö keskeyttäisi koko toiminnan (single point of failure, SPOF).

- Riskin vaikutuksen arvioinnin tukena on mahdollista käyttää riskien käsittely-kriteeristöä (ks. 1.1.1).
- Toimija on tunnistanut toimintaympäristönsä ja siihen perustuvat tietojen ja palvelujen luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät tietoturvatarpeet. Ks. kohta 2.3 Turvallisuusmenettelyiden valinta.
- Toimijalla on suositeltavaa olla kuvaukset ulkoisesta ja sisäisestä toimintaympäristöstä, joista käy ilmi olennaisista sidosryhmistä sekä toimijasta itsestään tulevat vaatimukset riskienhallinnalle.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on tunnistanut toiminnalleen kriittisimmän omaisuuden (keskeiset palvelut, järjestelmät, prosessit ja henkilöt) ja sisällyttänyt riskienhallinnan toimintamalliinsa niiden erityispiirteet ja -tarpeet tiedon ja palvelun luottamuksellisuudelle, eheydelle ja saatavuudelle. Tunnistetut kriittiset toiminnot ja omaisuus sekä niiden tietoturvatarpeet tulisi käydä ilmi riskienhallinnan toimintamallista ja omaisuuden hallinnasta.

Perustelut

Kriittisten tarpeiden ja toimintojen ja niihin kohdistuneiden riskin vaikutusten tunnistaminen auttaa oikeasuhtaisten tietoturvatoimenpiteiden valinnassa ja jäännösriskin hyväksynnässä.

Viitteet

IEC 62443-2-1:2013 (4.2.3.4, 4.2.3.6)

ISO/IEC 27001:2022 (6.2, A5.9, A5.12)

ISO/IEC 27002:2022 (5.9)

ISO/IEC 27005:2022 (6.1, 6.2)

ISO 31000:2018 (6.3.2)

NIST CSF 1.1 (ID.RA-1)

NIST CSF 2.0 (ID.RA-01)

NIS CG Reference document (3.4.1 Asset classification)

Työkalut

Julkri (HAL-04)

Kybermittari (CRITICAL-1, CRITICAL-2, ASSET-1, ASSET-2, RESPONSE-4, THIRD-PARTIES-1)

1.4 Uhkien tunnistaminen

Toteutusesimerkki

- Osana kyberturvallisuuden riskienhallintaa toimija on seurannut kohdassa 1.3. tunnistettujen viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvia uhkia, mukaan lukien kyberuhkatietoja ja haavoittuvuuksia, ja arvioinut näiden todennäköisyyttä ja vaikutusta osana riskiarviointia. Toimija sisällyttää uhka-analyysiinsä sisäisiä ja ulkoisia uhkia, tuottamuksellisia tekoja ja vahinkoja.
- Toimija on arvioinut uhkan todennäköisyyden ja toteutumisen vaikutuksia. Todennäköisyyden arvioinnissa on huomioitu esimerkiksi se, miten usein kyseinen uhka yleensä tapahtuu, onko uhka toteutunut organisaatiossa aikaisemmin ja onko vastaavaa uhkaa toteutunut toimialalla. Todennäköisyyden arviointiin on hyvä sisällyttää myös uhkapotentiaali, kuten hyökkääjän tahtotila, motiivi, kyvykkyys ja automatisoitujen haittaohjelmien saatavuus.
- Vaikutuksia arvioidakseen toimija on voinut järjestää simulointeja ja skenaarioharjoituksia toimintaansa kohdistuvia uhkia vasten arvioidakseen omaa valmiuttaan ja riskienhallinnan kyvykkyyttä erilaisissa kuvitteellisissa tilanteissa.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on esittää dokumentaatiota tunnistetuista viestintäverkkoihin ja tietojärjestelmiin kohdistuvista uhkista ja ne on huomioitu osana kyberturvallisuuden riskienhallintaa. Toimijan uhka-analyysistä käy ilmi toimijan arvio uhkien vaikutuksista ja todennäköisyyksistä.

Perustelut

Uhkien tunnistaminen ja systemaattinen uhka-analyysi tarjoavat keinon tunnistaa järjestelmään kohdistuvat yleisimmät uhkat ja haavoittuvuudet, jotka muodostavat riskin viestintäverkon tai tietojärjestelmän luotettavuudelle, eheydelle ja saatavuudelle. Uhka-analyysillä kerrytetään ymmärrystä uhkan vaikutuksista ja mahdollisten haavoittuvuuksien hyödyntämisen todennäköisyydestä.

Viitteet

ISO/IEC 27001:2022 (A5.7)

ISO/IEC 27002:2022 (5.7)

NIST CSF 1.1 (ID.RA-2, ID.RA-3)

NIST CSF 2.0 (ID.RA-02, ID.RA-03)

Työkalut

Kybermittari (THREAT-1, THREAT-2)

Kyberturvallisuuskeskuksen tilannekuvatuotteet, kuten Kyberturvallisuuskeskuksen viikkokatsaus ja kybersää

Kyberharjoitukset ja simuloinnit

1.4.1 Uhka-analyysi - laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Kohdan 1.4 lisäksi uhka-analyysiä varten toimija on kerännyt uhkatietoa ja haavoittuvuustietoa useasta eri lähteestä ja analysoinut uhkien todennäköisyyttä ja vaikutusta omassa toiminnassaan.
- Toimija on seurannut uhkaympäristön ja kyberturvallisuuteen liittyvien toimintojen viimeisintä kehitystä (state of the art) sekä kehittänyt ja ylläpitänyt omien viestintäverkkojensa ja tietojärjestelmiensä kyberturvallisuutta riskiarvion mukaisesti.
- Oman uhkaympäristön kartoittamiseksi voi tarvittaessa tehdä uhkamallinnuksen käyttäen sopivaksi havaitsemiaan uhkamallinnusmenetelmiä, kuten STRIDE ja DREAD.

Todennus

1. Valvova viranomainen katselmoi toimijan tekemiä uhka-analyysejä. Niistä tulisi käydä ilmi se, että analyysi on perustunut systemaattiseen menetelmään ja se on jatkuvaa, säännöllistä ja johdonmukaista. Uhka-analyysi on sisältänyt uhkatiedon keräämistä ja analysointia sekä oman uhkaympäristön kartoitusta ja analysointia. Toimijan on voinut käyttää yleisesti tunnettua uhkamallinnusmenetelmää, kuten STRIDE tai DREAD, järjestelmään kohdistuvien uhkien tunnistamisessa.
2. Valvova viranomainen todentaa uhka-analyysin systemaattisuuden haastattelemalla henkilöstöä uhka-analyysin käytännöistä. Haastatteluilla todennetaan, että uhkatiedon keräämisen laajuus, analyysien tiheys, omasta uhkaympäristöstä tunnistetut potentiaaliset uhkat sekä uhka-analyysien pohjalta sovitut toimenpiteet ovat riittävät toimijan tarpeet huomioiden.

Perustelut

Uhka-analyysin avulla pyritään tunnistamaan ja dokumentoimaan viestintäverkkojen ja tietojärjestelmien kriittiset tiedot, rajapinnat, ulkoiset riippuvuudet ja tietovirrat. Säännöllisesti tehdyllä uhka-analyysillä voidaan havaita uhkaympäristön muuttuminen ja tunnistaa järjestelmään kohdistuvat uudet uhkat. Toisaalta uhka-analyysillä voidaan myös sulkea pois sellaiset uhkat, joiden mahdollinen vaikutus toimintaympäristöön on pieni.

Viitteet

ISO/IEC 27001:2022 (A5.7)

ISO/IEC 27002:2022 (5.7)

NIST CSF 1.1 (ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6)

NIST CSF 2.0 (ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06)

Työkalut

Kybermittari (CRITICAL-3, THREAT-1, THREAT-2)

Uhkamallinnusmenetelmät: STRIDE[4], DREAD[5]

1.5 Riskien käsittely

Toteutusesimerkki
• Toimija on käsitellyt tunnistetut riskit ja kunkin riskin merkityksen arvioinnin perusteella. Riskin käsittelyyn on voitu sisällyttää eri reagointitapoja, kuten esimerkiksi riskin pitäminen/hyväksyminen, vaikutusten minimointi, poistaminen ja ulkoistaminen. Toimija voi hyödyntää riskienkäsittelyn tukena riskien käsittelykriteeristöä (ks. 1.1.1). • Toimija on määritellyt riskille omistajan, joka on vastuussa päätettyjen riskienhallinnan toimenpiteiden täytäntöönpanosta. Riskin omistaja voisi tarvittaessa määritellä, milloin toimenpide tulisi toteuttaa, seurata hallintatoimenpiteiden toteutumista ja toimenpiteiden vaikuttavuutta. • Toimija on tunnistanut ja priorisoinut asianmukaiset kyberturvallisuuden riskienhallinnan toimenpiteet ottaen huomioon riskiarvioinnin tulokset ja hallintatoimenpiteiden tehokkuuden arvioinnin tulokset. Toimija on voinut tilanteen mukaan arvioida myös riskinhallinnan toimenpiteen vaikutusta ja sen aiheuttamaa muutosta toimintaan sekä tarvittaessa suorittaa tarkentavan riskiarvion. • Toimija on dokumentoinut myös riskienhallinnan toimenpiteet ja perustellut jäännösriskien hyväksymisen syyt selkeästi. • Toimijan ylin johto on tarvittaessa hyväksynyt riskiarvioinnin ja -käsittelyn tulokset ja jäännösriskit. • Riskiarviointia ja riskienhallinnan toimenpiteitä on suositeltavaa katselmoida ja tarkistaa säännöllisesti sekä merkittävien muutosten tai merkittävien poikkeamien tapahduttua. • Riskienhallinnan toimenpiteet on otettu osaksi toimintaa ja koulutettu henkilöstölle. Tätä tarkennetaan kohdissa 2.2 Henkilöstön sitouttaminen ja 6 Henkilöstöturvallisuus ja kyberturvallisuuskoulutus.
Todennus
1. Valvova viranomainen todentaa kyberturvallisuusriskien käsittelyn katselmoimalla riskiarviointia. Toimijalla on esittää tuloksia kyberturvallisuusriskien arvioinnista ja käsittelystä. Dokumenteista käy ilmi riskinarvioinnin tulokset, riskien käsittely ja sovitut hallintatoimenpiteet sekä mahdolliset roolit ja vastuut. Riskienhallinnan tavoitteena on ollut riskien käsittely niin, että niiden todennäköisyys tai vaikutus on esimerkiksi minimoitu, poistettu tai ulkoistettu. Dokumenteista käy ilmi myös jäännösriskit, jäännösriskin käsittely ja hyväksymiseen liittyvät perustelut. Jotta riskien käsittelyn säännöllisyydestä saadaan näyttöä, on valvovan viranomaisen syytä todentaa riskien käsittelyyn liittyvää tapahtumatietoa. Valvova viranomainen voi todentaa toimijan riskienhallinnan historiaa esimerkiksi seuraamalla riskien määrää ja niiden vaikuttavuutta tietyn ajanjakson ylitse. Mikäli erityisesti keskeisiin riskeihin (key risk) on kohdistettu niitä hallitsevia (mitigoivia) toimenpiteitä, voi riskien määrä tai niiden vaikuttavuus laskea

[4] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
[5] https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers

ajan kuluessa. Mikäli riskit tai niiden vaikuttavuus eivät ole muuttuneet pitkänkään ajan kuluessa, olisi hyvä tarkastella riskienhallinnan toimintamallin toimivuutta ja sitä käytetäänkö oikeita kriteerejä riskien mittaamisessa.
Perustelut
Riskejä käsiteltäessä arvioidaan riskienhallinnan toimenpiteiden vaikuttavuutta ja jäännösriskin suhdetta: onko jäännösriskin taso siedettävä vai tulisiko siihen kohdistaa vielä lieventäviä toimenpiteitä. Riskien käsittelyn tavoitteena on toteuttaa sellainen riskienhallinnan toimenpiteiden yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Toimijan riskinkantokyky ja -halu määrittää hyväksyttävän jäännösriskin tason.
Viitteet
ISO/IEC 27001:2022 (8.1, 8.2, 8.3, 9.3) ISO/IEC 27005:2022 (8) ISO 31000:2018 (6.5) NIST CSF 1.1 (ID.RA-4, ID.RA-5, ID.RA-6, ID.RM-2, ID.RM-3) NIST CSF 2.0 (ID.RA-04, ID.RA-05, ID.RA-06, GV.RM-2, GV.RM-3) NIS CG Reference document (3.3.1 Risk management framework)
Työkalut
Julkri (HAL-06) Kybermittari (CRITICAL-2, RISK-3, RISK-4, WORKFORCE-4)

1.6 Riskienhallinnan vaikuttavuuden arviointi ja mittaristo

Toteutusesimerkki
• Osana riskienhallintaa toimija on arvioinut käsiteltyjen riskien toimenpiteiden vaikuttavuutta sopivin mittarein ja kehittänyt mittaristoa toimijan liiketoiminnan ja toimintaympäristön muuttuessa ja kehittyessä. • Mittaristo voi pohjautua liiketoimintastrategiasta pohjautuvaan toimintaperiaatteeseen ja organisaatiossa käytössä oleviin toimenpiteisiin ja menettelyihin. • Viestintäverkkojen ja tietojärjestelmien riskienhallinnan toimenpiteiden vaikuttavuuden arvioinnissa on huomioitu myös alakohtaiset toimintaperiaatteet ja säännöt, standardit ja toimialakohtainen sääntely. • Mittariston avulla toimija on arvioinut, ovatko listatut riskit edelleen merkityksellisiä, onko riskin vaikutus tai todennäköisyys edelleen samalla tasolla ja ovatko kohdistetut toimenpiteet ajantasaisia. Toimenpiteiden vaikuttavuutta arvioitaessa on huomioitu toimijaan kohdistuvat uhkat ja niiden ennakoitavissa olevat vaikutukset, kuten tyypillisimmät uhkatekijöiden aiheuttamat seuraukset ja näiden tyypilliset vaikutukset.

- Riskienhallinnan vaikuttavuutta on arvioitu säännöllisesti ja merkittävien poikkeamien tai muutosten yhteydessä.
- Riskienhallinnan vaikuttavuuden arvioinnin ja mittaamisen tuloksena toimija on muokannut riskienhallinnan toimenpiteitä vastaamaan muuttunutta tilannetta.
- Toimijan toteuttamaa viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallintaa ja sen toteuttamista on katselmoitu ja arvioitu riippumattomasti. Toimija on luonut prosessit riippumattomiin katselmointeihin ja johdon tulisi suunnitella ja toteuttaa niitä säännöllisesti.
- Katselmointia suorittavat henkilöt ovat toimijan toiminnasta riippumattomia ja heillä on asianmukainen osaaminen ja kokemus arvioinnin suorittamiseen. Katselmointi on voitu suorittaa itsearviointina tai tietoturvapalveluntarjoajan toimesta.
- Arvioinnin tulokset on raportoitu johdolle. Korjaavat toimenpiteet on toteutettu ja jäännösriskit on hyväksytty toimijan riskikriteeristön mukaisesti.

Todennus

1. Valvova viranomainen katselmoi toimijan määrittelemän mittariston. Mittariston tulisi soveltua riskienhallinnan toimenpiteiden vaikuttavuuden arviointiin niin, että valittujen toimenpiteiden toimivuutta voidaan mitata ja tarvittaessa parantaa. Suunnitelmista tulisi käydä ilmi toimijan prosessit ja suunnitelmat katselmointeihin. Toimijalla on esittää raportteja katselmoinneista ja arvioinneista.
2. Valvova viranomainen haastattelee toimijan työntekijöitä ja arvioi mittariston käyttöä ja toimivuutta käytännössä. Mittariston tulisi tarvittaessa toimia johdon työkaluna kyberturvallisuuden riskienhallinnan tilanteesta. Valvova viranomainen haastattelee toimijaa riskienkäsittelystä. Haastatteluista tulisi käydä ilmi riskienhallinnan toimenpiteiden käynnistyminen mittariston perusteella. Toimijaa voi pyytää esittämään myös riskienkäsittelydokumenttia, josta tulisi käydä ilmi toimenpiteiden historia.

Perustelut

Riskienhallinnan toimenpiteillä olisi pystyttävä luomaan lisäarvoa, jonka vuoksi niitä on arvioitava säännöllisesti. Jatkuvasti muuttuva uhkaympäristö ja teknologia aiheuttavat suurimmat haasteet valittujen toimenpiteiden ajantasaisena pysymiseen. Tämän vuoksi riskienhallintaa ja vaikuttavuuden arviointia tulisi tehdä riskin koko elinkaaren ajan. Riippumattomat arvioijat varmistavat organisaation riskienhallinnan vaikuttavuuden ja ajantasaisuuden.

Viitteet

IEC 62443-2-1:2013 (4.4.2.3, 4.4.3)

IEC/TR 62443-3-1:2013

IEC 62443-3-3:2019 (SR 3.9)

ISO/IEC 27001:2022 (6.2, 9.1, 9.2, 9.3, 10.1, A.5.31, A.5.35, A.5.36, A.8.34)

ISO/IEC 27005:2022 (9.2)

ISO 31000:2018 (6.6)

NIST.CSF 1.1 (ID.RM-1)

NIST CSF 2.0 (ID.IM-01) NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures) NIS CG Reference document (3.3.4 Independent review of information and network security)
Työkalut
Kybermittari (CRITICAL-2, RISK-4, RISK-5, Yleisiä hallintatoimia-f)

1.6.1 Riskienhallinnan vaikuttavuuden arviointi ja mittaristo - laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Kohdan 1.6 lisäksi toimija on sisällyttänyt riskienhallinnan vaikuttavuuden menettelyihin tietoturva-arvioinnit ja tietoverkkojen ja tietojärjestelmien tietoturvatestaukset
- Riskienhallinnan toimenpiteiden vaikuttavuuden mittaamiseksi toimija on määrittänyt seuraavanlaisia asioita:
  - seurattavat ja mitattavat riskienhallintatoimenpiteet
  - prosessit ja menetelmät valvontaan
  - milloin seuranta ja mittaus tulisi suorittaa
  - kuka valvoo ja mittaa
  - milloin seurannan ja mittauksen tulokset olisi analysoitava ja arvioitava sekä
  - kuka analysoi ja arvioi nämä tulokset.
- Toimija on arvioinut riskienhallinnan toimintamallin toteutumista organisaatiossa.
- Vaikuttavuutta voidaan arvioida myös seuraamalla NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteiden toteutumista.

Todennus

1. Valvova viranomainen katselmoi toimijan laatiman mittariston kyberturvallisuuden riskienhallinnan toimenpiteiden vaikuttavuuden arviointiin. Mittaristosta käy ilmi organisaation toteuttama riskienhallintasuunnitelma sekä mahdolliset vastuuhenkilöt. Mittaristosta voi käydä ilmi myös kyberturvallisuuden riskienhallinnan toimenpiteiden toteutuminen, vaikuttavuus ja ajantasaisuus.

Perustelut

Mittaristolla varmistetaan kelvolliset ja vertailtavissa olevat riskienhallinnan tulokset. Mittaristo voi myös auttaa toimijaa seuraamaan NIS2-direktiivissä asetettujen kyberturvallisuuden riskienhallinnan toimenpiteiden toteutumista organisaatiossa.

Viitteet
IEC 62443-2-1:2013 (4.4.2.3, 4.4.4)
IEC/TR 62443-3-1:2013
ISO/IEC 27001:2022 (9.1, 9.2)
ISO/IEC 27002:2022 (5.31, 5.35, 5.36)
NIST CSF 1.1 (PR.IP-8)
NIST CSF 2.0 (ID.IM-03)
NIS CG Reference document (3.3.2 Policies and procedures to assess the effectiveness of security measures)
NIS CG Reference document (3.3.3 Compliance monitoring)
Työkalut
Kybermittari (CRITICAL-2, RISK-4, RISK-5, Yleisiä hallintatoimia-f)

2 Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan a alakohtaan. Alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 2 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 2 kohdassa.

1. **Turvallisuutta koskevat toimintaperiaatteet ja menettelyt**: Nämä voivat koskea hallinnollista, henkilöstö-, laitteisto-, ohjelmisto-, viestintäverkko- ja tietoaineistoturvallisuutta sekä operoinnin ja fyysisen ympäristön turvallisuutta. Nämä ovat oikeasuhtaisia toimijan tarpeisiin nähden ja ajantasaisesti ylläpidettyjä. ISO 27001 -standardin yhteydessä vastaavista toimintaperiaatteista käytetään termiä tietoturvapolitiikka. Toimijalla tulisi olla kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet ja menettelyt. Mikäli tällaisia on, tulisi niiden olla oikeasuhtaisia toimijan tarpeisiin nähden ja ajantasaisesti ylläpidettyjä. (Ks. kohta 2.1 ja 2.1.1).

2. **Henkilöstön sitouttaminen**: Toimijan henkilöstö tulisi tuntea käytössä olevat turvallisuusmenettelyt ja sitoutuu niiden noudattamiseen. (Ks. kohta 2.2).

3. **Turvallisuusmenettelyiden valinta**: Sopivien menettelyiden valinnassa voitaisiin huomioida esimerkiksi liiketoiminnalliset tarpeet ja tunnistetut kyberturvallisuusriskit. (Ks. kohta 2.3).

2.1 Turvallisuutta koskevat toimintaperiaatteet ja menettelyt

Toteutusesimerkki
• Toimija on laatinut kirjalliset viestintäverkkojen ja tietojärjestelmien turvallisuutta koskeva toimintaperiaatteet ja menettelyt. Standardien yhteydessä näistä käytetään joskus termiä tietoturvapolitiikka. Toimijan ylin johto on hyväksynyt turvallisuutta koskevat toimintaperiaatteet ja menettelyt ja ne on

jalkautettu henkilöstölle ja mahdollisesti myös kolmansille osapuolille, kuten alihankkijoille, toimittajille ja palveluntarjoajille (Ks. 2.2).

- Toimija on voinut käyttää turvallisuutta koskevien toimintaperiaatteiden ja menetelmien laatimisen tukena yleisesti hyväksyttyjä standardeja, kyberturvallisuuden viitekehyksiä tai alan parhaita käytänteitä tietoturvapolitiikasta.
- Turvallisuutta koskevat toimintaperiaatteet ja menettelyt koskevat hallinnollista, henkilöstö-, laitteisto-, ohjelmisto-, viestintäverkko- ja tietoaineistoturvallisuutta sekä operoinnin ja fyysisen ympäristön turvallisuutta.
- Toimija on sisällyttänyt viestintäverkkojen ja tietojärjestelmien turvallisuutta koskeviin toimintaperiaatteisiin soveltuvilta osin NIS2-direktiivin kyberturvallisuuteen liittyviä toimenpiteitä, kuten pääsynhallinta, omaisuudenhallinta, päätelaitteiden turvallinen konfigurointi, verkkoturvallisuus, varmuuskopiointi, salaus, häiriötilanteiden hallinta, haavoittuvuuksien hallinta ja fyysinen turvallisuus.
- Osana turvallisuutta koskevia toimintaperiaatteita ja menettelyjä toimija on esitellyt turvallisuuteen liittyvät roolit, vastuut ja valtuudet (ks. 6.1).
- Toimija on huomioinut turvallisuutta koskevien toimintaperiaatteiden ja menettelyiden valinnassa liiketoiminnalliset tarpeet ja tunnistetut kyberturvallisuusriskit. Toimintaperiaatteet ja menettelyt soveltuvat toimijan käyttöön ja ovat oikeasuhtaisia toimintaan kohdistuvaan riskiin nähden.
- Turvallisuutta koskevista toimintaperiaatteista ja menettelyistä käy ilmi viestintäverkkojen ja tietojärjestelmien turvallisuuden tavoitteet, toimijan sitoumus täyttää sovellettavat tietoturvaan liittyvät vaatimukset sekä sitoumus toimintaperiaatteiden ja menettelyiden jatkuvaan parantamiseen. Toimijan mittaristo tukee myös turvallisuutta koskevien toimintaperiaatteiden jatkuvaa parantamista (ks. 1.6).
- Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevien toimintaperiaatteita ja menettelyjä on pidetty ajantasaisena säännöllisillä katselmoinneilla. Säännöllisiä katselmointeja on pidetty ennalta sovituin ajankohdin (esimerkiksi kerran vuodessa) ja kun merkittäviä muutoksia tai merkittäviä poikkeamia on tapahtunut.
- Toimintaperiaatteiden ja menettelyiden soveltuvuutta käytäntöön on arvioitu katselmoinneissa ja ne on sovitettu vastaamaan toimijan tarpeita. Toimija on voinut huomioida myös toimintaympäristön ja uhkaympäristön muutoksen ja tietoturvatoimintojen kehityksen.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on esittää dokumentit viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevista toimintaperiaatteista ja menettelyistä. Turvallisuutta koskevat toimintaperiaatteet ja menettelyt ovat riittävän kattavat ja niihin on sisällytetty toimijan tarpeisiin sopivat osa-alueet. Dokumenteista käy ilmi selkeästi toimijan tietoturvan päämäärät, periaatteet ja toteutus.

   Toimintaperiaatteiden ja menettelyiden oikeasuhtaisuuden todentamiseksi dokumenteista tulisi käydä ilmi toimintaperiaatteiden linkittyminen liiketoimintaan ja toimijan toteuttamaan kyberturvallisuuden riskienhallintaan.

   Toimintaperiaatteet ja menettelyt ovat ajantasaisia ja niitä on ylläpidetty. Tämä voidaan todentaa tarkistamalla dokumenttien päivityshistoriaa. Päivityksiä tulisi tehdä säännöllisesti tai merkittävien muutosten tai poikkeamien tapahduttua. Toimijalla on esittää suunnitelmat ja dokumentaatiota toimintaperiaatteiden ja menettelyiden katselmoinneista.
2. Valvova viranomainen arvioi toimijan turvallisuutta koskevia toimintaperiaatteita ja menettelyiden oikeasuhtaisuutta ja ajantasaisuutta haastattelemalla

toimijan henkilöstöä siitä, miten tietoisia he ovat laadituista toimintaperiaatteista ja menettelyistä sekä miten niitä toteutetaan ja noudatetaan käytännössä.

Perustelut

Turvallisuutta koskevat toimintaperiaatteet ja menettelyt luovat perustan organisaation tietoturvakulttuurille ja viestintäverkkojen ja tietojärjestelmien turvallisuuden hallintaan ja turvallisuuden toteuttamiseen, mukaan lukien ihmiset, prosessit ja teknologiat/tekniikat. Ajantasaiset ja oikeasuhtaiset toimintaperiaatteet ja menettelyt tukevat arjen työtä ja mahdollistavat organisaation turvallisuustavoitteiden toteutumisen.

Viitteet

IEC 62443-2-1:2013 (4.3.2.2.1, 4.3.2.2.2, 4.3.2.6)

IEC 62443-2-4:2019 (SP 01)

ISO 27001:2022 (5.2, A.5.1, A.5.36)

ISO 27002:2022 (5.1, 5.36)

NIST SP 800-53 Rev. 5

NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.BE-3)

NIST CSF 2.0 (GV.OC-01, GV.OC-03, GV.PO-01, GV.PO-02)

NIS CG Reference document (3.2.1 Network and information security policy)

Työkalut

Julkri (HAL-01)

Kybermittari (PROGRAM-1, PROGRAM-2, Yleiset hallintatoimet, CRITICAL-2)

2.1.1 Turvallisuutta koskevat toimintaperiaatteet ja menettelyt - laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Kohdan 2.1 lisäksi osana turvallisuutta koskevia toimintaperiaatteita ja menettelyjä toimija on voinut laatia tarkemmat menettelyt ja ohjeet eri osa-alueisiin, kuten pääsynhallinta, omaisuudenhallinta, päätelaitteiden turvallinen konfigurointi, verkkoturvallisuus, varmuuskopiointi, salaus, häiriötilanteiden hallinta, haavoittuvuuksien hallinta ja fyysinen turvallisuus.
- Tarve tarkempaan menettelyyn ja ohjeeseen voi tulla esimerkiksi osa-alueen koosta tai päivitystarpeen tiheydestä. Esimerkiksi osana omaisuudenhallintaa toimijalla voi olla tarvetta ohjeistaa kriittisen omaisuuden osalta laitteiden, ohjelmistojen ja tietojen turvallisesta siirtämisestä toimijan ulkopuolisiin tiloihin.

Todennus
1. Valvova viranomainen katselmoi toimijan laatimat turvallisuutta koskevat tarkentavat ohjeet.
Perustelut
Viitteet
ISO/IEC 27002:2022 (5.1, 5.37) NIST CSF 1.1 (ID.GV-4) NIST CSF 2.0 (GV.OC-4)
Työkalut
Kybermittari (PROGRAM-1, Yleiset hallintatoimet, CRITICAL-2)

2.2 Henkilöstön sitouttaminen

Toteutusesimerkki
• Toimijan johto on huolehtinut, että koko henkilöstö ja mahdolliset kolmannet osapuolet noudattavat viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevia toimintaperiaatteita ja menettelyjä (ks. 2.1) sekä muita eri osa-alueista laadittuja tarkempia menettelyjä ja ohjeita (Ks. 2.1.1). • Toimija on viestinyt turvallisuutta koskevista toimintaperiaatteista ja menettelyistä säännöllisesti henkilöstölle ja kolmansille osapuolille. • Turvallisuutta koskevat toimintaperiaatteet ja menettelyt on sisällytetty osaksi toimijan järjestämiä koulutuksia. Koulutuksesta löytyy lisätietoa kohdassa 6.5 Henkilöstökoulutus ja 11.1 Perustason tietoturvakäytännöt. • Toimijalla on toimintamallit mahdollisten turvallisuutta koskevien toimintaperiaatteiden ja menettelyiden vastaisen toiminnan varalta. Tätä kohtaa tarkennetaan kohdassa 6.1 Henkilöstön turvallisuus.
Todennus
1. Valvova viranomainen katselmoi käytännöt turvallisuuteen liittyvistä toimintaperiaatteiden ja menettelyiden viestimisestä tai kouluttamisesta henkilöstölle. Tämä voi olla esimerkiksi toimijan esittelemä verkkosivu, koulutusmateriaali tai muu vastaava, joka on koko henkilöstön saatavilla. Valvova viranomainen voi myös tarkistaa toimijan laatiman toimintamallin henkilöstön sitouttamiseksi kyberturvallisuuden toimintamallien noudattamiseen. Tämä voi olla esimerkiksi turvallisuutta koskevien toimintaperiaatteiden koulutuksen seuranta. 2. Valvova viranomainen todentaa haastattelulla, että henkilöstö tuntee turvallisuutta koskevat toimintaperiaatteet ja menettelyt. Haastatteluista ilmenee

henkilöstön toiminta yhteisten toimintaperiaatteiden ja menettelyiden mukaisesti. Henkilöstöllä on tieto siitä, mistä kirjalliset materiaalit löytyvät.

Perustelut

Turvallisuutta koskevien toimintaperiaatteiden ja menettelyiden omaksuminen on osaavan henkilökunnan varassa. Koulutuksen avulla jokainen henkilöstön jäsen ymmärtää oman tehtävänsä merkityksen osana organisaation kokonaisturvallisuutta.

Viitteet

ISO/IEC 27001:2022 (5.2, A5.4, A6.3)

ISO/IEC 27002:2022 (5.4, 6.3)

NIST CSF 1.1 (ID.GV-2, ID.AM-6, DE.DP-1, PR.AT-5)

NIST CSF 2.0 (GV.RR-02, PR.AT-02)

NIS CG Reference document (3.2.2 Roles, responsibilities and authorities)

Työkalut

Julkri (HAL-02, HAL-03, HAL-12, HAL-13)

Kybermittari (CRITICAL-2, WORKFORCE-2 WORKFORCE-3, Yleiset hallintatoimet)

2.3 Turvallisuusmenettelyiden valinta

Toteutusesimerkki

- Toimija on ottanut huomioon viestintäverkkojen ja tietojärjestelmien turvallisuuteen liittyvien menettelyiden valinnassa toimijan liiketoiminnan tarpeet ja tunnistetut kyberturvallisuusriskit (ks. 2.1). Liiketoiminnan tarpeisiin on sisältynyt esimerkiksi keskeisten sidosryhmien vaatimukset, toimialaan kohdistuva sääntely ja toimijan standardit ja sertifikaatit.
- Turvallisuusmenettelyt on valittu tunnistettujen turvallisuustarpeiden pohjalta. Valitakseen oikeasuhtaiset turvallisuusmenettelyt toimija on luetteloinut omaisuutensa, tehnyt sille riskiarvion ja luokitellut omaisuuden tietoturvatarpeen (esim. luottamuksellisuus, eheys, aitous ja saatavuus) mukaisesti. Tarvittaessa toimija on voinut sisällyttää niihin myös aitouden, kiistämättömyyden ja todentamisen. Omaisuusluetteloa ja omaisuuden luokittelua tarkennetaan kohdassa 5.2.
- Toimija on päivittänyt ja kehittänyt turvallisuusmenettelyjä säännöllisesti ja merkittävien muutosten yhteydessä, kuten toimintaympäristön tai uhkaympäristön muuttuessa tai poikkeamien tapahduttua.

Todennus

1. Valvova viranomainen katselmoi dokumentoidut turvallisuutta koskevat toimintaperiaatteet ja menettelyt. Dokumentteihin on kirjattu muun muassa toimijan liiketoiminnasta ja alaan kohdistuvasta sääntelystä muodostuvat vaatimukset. Turvallisuutta koskevien menettelyiden valinnasta käy ilmi

liiketoiminnalliset tarpeet, kuten toimijan liiketoimintastrategia, osana johtamisjärjestelmää olevat standardit ja sertifioinnit, toimialaan kohdistuva sääntely ja keskeisten sidosryhmien tarpeet. Menettelyiden valinnasta käy ilmi myös tunnistetut kyberturvallisuusriskit ja niissä on selkeä linkitys riskiarviointiin, riskienhallinnan toimenpiteiden valintaan, niiden vaikuttavuuden arviointiin ja mittaristoon sekä omaisuudenhallintaan ja sen luettelointiin ja luokitteluun.
Perustelut
Viitteet
ISO/IEC 27001:2022 (A5.12, A5.36) ISO/IEC 27002:2022 (5.12, 5.36) NIST CSF 1.1 (ID.GV-1, ID.GV-3, ID.GV-4) NIST CSF 2.0 (GV.OC-1, GV.PO-1) NIS CG Reference document (3.2.1 Network and information security policy)
Työkalut
Julkri (HAL-05) Kybermittari (ASSET-1, ASSET-2, PROGRAM-1, PROGRAM-2, ARCHITECTURE-1)

3 Viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan e alakohtaan. Alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 3 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 3 kohdassa.

1. **Viestintäverkkojen ja tietojärjestelmien suojaus elinkaaren ajan**: Toimijan tulisi pyrkiä ylläpitämään viestintäverkkojen ja tietojärjestelmien riittävää turvallisuuden tasoa koko niiden elinkaaren ajan. (Ks. kohta 3.1).

2. **Hankinnan kohteen turvallisuus**: Hankittavien järjestelmien olisi oltava toiminnan tarpeiden perusteella riittävän turvallisia muun muassa eheyden, saatavuuden ja luottamuksellisuuden suhteen. Järjestelmien hankinnassa voitaisiin kiinnittää huomiota esimerkiksi niiden kykyyn suojautua tavallisimpia hyökkäyksiä vastaan. (Ks. kohta 3.2).

3. **Järjestelmäkovennukset**: Järjestelmien turvallinen konfiguraatio eli asetukset voitaisiin määritellä, dokumentoida ja ylläpitää koko elinkaaren ajan, ja erityistä huomiota voitaisiin kiinnittää tähän erityisesti päivitysten aikana. (Ks. kohta 3.3 ja 3.3.1).

4. **Muutosten- ja päivitysten hallinta**: Konfiguraatio- ja ohjelmistopäivitysten osalta voitaisiin esimerkiksi pyrkiä siihen, että ne olisivat dokumentoituja, muutoshallintaprosessien mukaisesti suunniteltuja, kattavia sekä kohteen ominaispiirteiden ja päivitysten kriittisyyden kannalta oikea-aikaisia. Luvattomien tai haitallisten muutosten tekeminen voitaisiin esimerkiksi estää. (Ks. kohta 3.4 ja 3.4.1).

5. **Turvallisuuden testaus**: Turvallisuuden kannalta kriittisimmät kohteet voitaisiin tunnistaa erikseen ja näiden turvallisuudesta voitaisiin huolehtia esimerkiksi tarkastelemalla säännöllisesti prosesseja tai teknisillä testauksilla. (Ks. kohta 3.5).

6. **Haavoittuvuuksien käsittely ja julkistaminen**: Löydettyjä haavoittuvuuksia varten olisi oltava olemassa raportointikanava sekä menettelytavat ja käytännöt ilmoitusten käsittelyä varten. (Ks. kohta 3.6).

7. **Kehittämisen turvallisuus**: On varmistuttava siitä, että tuotteet on kehitetty käyttäen tunnettuja hyviä käytäntöjä niin, että prosessi kattaa koko kehityksen elinkaaren. Tämä kohdistuu vain toimijoihin, jotka tuottavat sovelluksia, palveluita, laitteita tai tämän kaltaisia tuotteita. (Ks. kohta 3.7).

8. **Toimitettavien palveluiden turvallisuus**: Jos toimija tuottaa viestintäverkko- tai tietojärjestelmäpalveluita, olisi toimijan huolehdittava tuotteidensa turvallisuudesta. Toimija voisi esimerkiksi varmistaa, että näiden viestintäverkkojen ja tietojärjestelmien turvallinen konfiguraatio on mahdollista ja niille tuotetaan turvallisuuspäivityksiä. (Ks. kohta 3.7.1).

9. **Viestintäverkkojen rakenteellinen turvallisuus**: Viestintäverkkojen osalta olisi huolehdittava verkon turvallisesta rakenteesta. Esimerkiksi toiminnoille kriittiset kohteet tulisi tunnistaa ja tarvittaessa suojata ajantasaisin teknisin keinoin, kuten esimerkiksi vyöhykkeistämällä. (Ks. kohta 3.8).

10. **Haittaliikennesuojaukset**: Mahdollinen haitallinen liikenne tulisi kyetä havaitsemaan ja estämään. (Ks. kohta 3.9).

3.1 Viestintäverkkojen ja tietojärjestelmien suojaus elinkaaren ajan

Toteutusesimerkki
Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.3. • Toimijalla on menettelyt viestintäverkkojen ja tietojärjestelmien suojaamiseksi koko elinkaaren ajan. Elinkaariajattelussa on otettava huomioon sekä suunnittelu, käyttöönotto, operointi että käytöstä poisto. Omaisuuden elinkaarta tarkennetaan kohdassa 5.3 Omaisuusluettelon käyttö.
Todennus
1. Valvova viranomainen todentaa dokumentaatiota katselmoimalla, että toimija suojaa viestintäverkkojaan ja tietojärjestelmiään. Dokumentaatiosta käy ilmi se, miten näitä suojataan koko elinkaaren ajan. Elinkaaren osalta on huomioitu suunnittelu, käyttöönotto, operointi ja käytöstä poisto. Se, että suojaukset on käyttöönotettu, voidaan todentaa esimerkiksi hyödyntäen omaisuuskatalogia ja siihen kohdistuvia muutoksia sekä muulla toimijan toimittamalla näytöllä kuten kuvaruutukaappauksilla sekä haastatteluin. Tarkasteltavia suojauksia ovat muun muassa kohdat 3.3 Järjestelmäkovennukset, 3.4

Muutosten- ja päivitysten hallinta, 3.8 Viestintäverkkojen rakenteellinen turvallisuus sekä 11 Perustason tietoturvakäytännöt soveltuvin osin.

2. Toimijan toimittamia konfiguraatioita ja tilatietoa (esimerkiksi DNS, DHCP-lokitiedot ja kirjanpito, ARP-taulut (vain IPv4), muut laitekannat, verkkolaitteiden konfiguraationhallinta tai versiointi) tarkastelemalla ja vertaamalla niitä dokumentaatioon valvova viranomainen voi todentaa, että menettelyjä on toteutettu. Tiedoista tulisi käydä ilmi, ettei ympäristössä ole esimerkiksi käytöstä poistettuja laitteita tai laitteita, joiden käyttöönoton prosessia ei ole viety läpi ilman perusteltua syytä. On syytä kiinnittää erityistä huomiota laitteisiin, jotka eivät välttämättä näy suoraan viestintäverkon ja tietojärjestelmän tiedoissa. Tällaisia saattavat olla tyypillisesti esimerkiksi ulkoisissa pilvipalveluissa olevat virtuaalikoneet sekä palvelut, kuten rajapinnat, joita saattaa joutua tarkastamaan kyseisen palvelun käyttöliittymästä. Jos toimija käyttää pilvipalveluita tai muita virtuaalisia alustoja, olisi tarkastelu ulotettava myös näihin.
3. Valvova viranomainen voi laajentaa edellistä tarkastelua aktiivisin skannauksin tai tietoliikennenauhoituksilla.

Perustelut

Turvallisuuden rapautuminen ajan kuluessa voi aiheuttaa haavoittuvuuksia, joita ei tunnisteta. On tavanomaista, että laitteita, virtuaalikoneita ja sovelluksia jää poistamatta käyttötarpeen loputtua. Yleensä ylläpitämättömät kohteet aiheuttavat usein vakavia haavoittuvuuksia.

Viitteet

ISO/IEC 27003:2018

NIST CSF 1.1 (PR.AC-5, PR.DS-3)

NIST CSF 2.0 (PR.IR-01)

Työkalut

Julkri (HAL-05.1, TEK-17.2)

Kybermittari (ASSET-1, ASSET-3, ASSET-4)

3.2 Hankinnan kohteen turvallisuus

Toteutusesimerkki

- Toimijan on varmistuttava siitä, että kolmannelta osapuolelta hankittavat palvelut, järjestelmät, tuotteet ja resurssit ovat toiminnan tarpeiden perusteella riittävän turvallisia muun muassa eheyden, saatavuuden ja luottamuksellisuuden suhteen ja niiden olisi kyettävä suojautumaan tavallisimmilta hyökkäyksiltä.
- Toimijan on varmistuttava, että tuota tai palvelu on turvallisesti konfiguroitavissa ja kohteelle on tietoturvapäivityksiä koko suunnitellun elinkaaren ajan, silloin kun konfiguroitavuus ja päivitettävyys on kohteelle olennaista.
- Jos hankinnan kohde on esimerkiksi palvelu tai resurssi, on huolehdittava kohteen turvallisuudesta, laadusta ja saatavuudesta koko elinkaaren ajan.

Erityisesti on varauduttava mahdollisiin muutoksiin palveluntoimittajan osalta niin, että palvelu tai resurssi voidaan tarvittaessa siirtää tai palauttaa omaan hallintaan. Tarvittaessa on varauduttava myös omistussuhteiden muutoksiin.

- Hankinnan turvallisuudesta voi yrittää varmistua esimerkiksi sopimuksellisin keinoin, tutkimalla tuotteen ominaisuuksia, edellyttämällä esimerkiksi sertifiointeja, varmistumalla toimittajan luotettavuudesta ja varautumalla riskeihin. Turvallisuusvaatimukset on määritelty jo hankinnan alkuvaiheessa ja vaatimukset on toimitettu toimittajille ja liitetty osaksi sopimusta.
- Toimija on varmistanut, että hankitusta kohteesta on olemassa dokumentaatio, joka kattaa sen sisällön sekä turvallisen konfiguraation ja käytön.
- Hankitun kohteen turvallisuudesta on varmistuttu koko elinkaaren ajan. Tämä voi sisältää esimerkiksi päivityksiä sopimukseen, päivityksiä ylläpitoon ja säännöllisiä turvallisuustarkastuksia.
- Hankinnan kohteesta voidaan varmistua hankintaprosessin lisäksi hyväksyntätesteillä (factory acceptance test, site acceptance test).
- Toimija on huomioinut turvallisuusnäkökulmat myös hankintaprosessin aikana. Tiedon turvallisesta käsittelystä on lisää kohdassa 11.8.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on käytännöt, joilla varmistetaan hankintojen kohteiden turvallisuus (ks. edeltä toteutusesimerkit). Hankinnan kohteiden turvallisuus tulisi varmistaa erityisesti sellaisista kohteista, joissa olevat tietoturvaheikkoudet voivat aiheuttaa riskejä toimijan toiminnalle. Hankinnan kohteen turvallisuudesta varmistuminen vaatii yleensä käytännössä kattavaa hankintaprosessia, jossa otetaan huomioon turvallisuusasiat. Toimija on varmistunut siitä, että hankittavien kohteinen turvallinen konfiguraatio on mahdollista ja että kohteille tuotetaan turvallisuuspäivityksiä riittävän pitkään. Lisäksi hankinnan kohteiden olisi kyettävä suojautumaan vähintään tavallisimpia hyökkäyksiä vastaan.

   Hankintojen kohteiden turvallisuutta voi lähestyä esimerkiksi hankintaprosessin kautta. Hankittava kohde voi olla esimerkiksi laite, palvelu tai resurssi. Tyypillinen tapa varmistua turvallisuudesta voi olla esimerkiksi hankintojen yhteydessä erilaiset testaus- ja tutkintamenetelmät, kohteen elinkaaren hallintaan liittyvät toimenpiteet sekä varautumiset erilaisia uhkia ja uhkaympäristön muutosta vastaan turvallisuussopimuksin. Tulisi siis varmistua siitä, että toimijan hankintaprosessi tukee turvallisuustarpeita, hankintaprosessia noudatetaan ja huomioidaan riskiarvioinnissa. Hankintaprosessin toteutumista voi todentaa esimerkiksi tutustumalla hankintadokumentteihin, haastatteluin sekä tutkimalla hankittujen kohteiden nykytilaa. Hankinnoissa tulisi kiinnittää erityishuomiota toimijan erikoistarpeisiin. Näitä voivat olla esimerkiksi maantieteelliset vaatimukset, resursseihin ja palvelulupauksiin liittyvät tarpeet, palveluiden siirtomahdollisuus, tuotteiden ja palveluiden turvallisuusominaisuudet sekä palveluiden päivitys ja elinkaari.

Perustelut

Epäonnistuneisiin hankintoihin voi liittyä taloudellisen riskin lisäksi kyberturvallisuusriskejä. Esimerkiksi turvaton tuote tai palvelu voi vaarantaa muun tietojärjestelmän ja viestintäverkon. Jos hankintaa ei ole tehty riittävillä järjestelyillä, kasvaa monien uhkien todennäköisyys, kuten laitevalmistajariippuvuus (vendor lock-in), omistussuhteiden muutoksesta aiheutuvat uhkat, osaamisen menetys ja hankinnan kohteen menetys.

Viitteet
IEC 62443-2-1:2013 (4.3.4.3.1, 4.3.4.3.4); IEC 62443-2-4:2019 IEC 62443-3-3:2019 (SR 3.4, 3.5), ISO/IEC 27001:2022 (A5.21, A5.23) ISO/IEC 27002:2022 (5.21, 5.23) NIST CSF 1.1 (ID.SC-1, ID.SC-3, ID.SC-4) NIST CSF 2.0 (GV.SC-01, GV.SC-05, GV.SC-07) NIS CG Reference document (3.9.6 Security in acquisition of ICT services, ICT systems or ICT products)
Työkalut
Julkri (HAL-16, HAL-16.1) KYBERMITTARI (THIRD-PARTIES-1, THIRD-PARTIES-2, ARCHITECTURE-4) Tiedonhallintalautakunnan antama suositus tietoturvallisuudesta hankinnoista, kohderyhmä tiedonhallintayksiköt ja viranomaiset: https://urn.fi/URN:ISBN:978-952-367-645-9

3.3 Järjestelmäkovennukset

Toteutusesimerkki
Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.10. • Toimija on määritellyt prosessit ja työkalut, jotta laitteille, sovelluksille, palveluille ja viestintäverkoille luodaan turvallinen konfiguraatio ja tätä ylläpidetään koko elinkaaren ajan. • Osana riskiarviointia on määritelty vähintään ne kohteet, joiden toiminnallisuus on keskeistä turvallisuuden, toimintakyvyn, huoltovarmuuden tai muiden riskienhallintasyiden vuoksi. • Näille kohteille on luotu konfiguraatio, joka edistää kohteen tietoturvallisuutta. Turvallinen konfiguraatio tarkoittaa esimerkiksi selkeästi riskialttiiden ominaisuuksien poistamista, ylimääräisten palveluiden, komponenttien ja porttien sammuttamista tai poistamista, oletusarvojen kuten oletussalasanojen vaihtamista ja turvallisuustoimintojen ottamista käyttöön. • Jos kohteelle ei voi tuottaa turvallista konfiguraatiota ja kohde muodostaa kohonneen turvallisuusriskin viestintäverkolle tai tietojärjestelmälle, se on suojattu muilla riskienhallinnan keinoilla. • Konfiguraatioon liittyviä turvallisuusparametrejä, kuten salasanoja, on säilytetty turvattuna ja ne ovat saatavilla ja helposti vaihdettavissa.
Todennus
1. Valvova viranomainen todentaa, että toimija määrittelee, dokumentoi ja ylläpitää järjestelmien turvallisen konfiguraation. Turvallisen konfiguroinnin

todentamiseen voi hyödyntää olemassa olevaa dokumentaatiota ja konfiguraatiotiedostoja. Näistä käy ilmi se, että toimija johdonmukaisesti poistaa ylimääräiset asetukset, vaihtaa turvattomat oletusasetukset sekä ottaa käyttöön mahdollisia turvallisuusominaisuuksia. Lisäksi valvova viranomainen katselmoi toimijan konfigurointikäytännöt muutosten, kuten päivitysten, yhteydessä. Tyypillisiä kovennettavia asioita ovat esimerkiksi oletussalasanojen vaihtaminen, ylimääräisten palveluiden ja ominaisuuksien poistaminen käytöstä (esimerkiksi ylimääräiset hallintayhteydet), ylimääräisten laitteiden ja komponenttien poistaminen käytöstä, liikennöintiprotokollien vaihtaminen turvallisiksi (esimerkiksi salaamaton salatuksi), turvallisuusasetusten ottaminen käyttöön (esimerkiksi palomuuri, haittaohjelmatarkastus, automaattiset päivitykset).

2. Valvova viranomainen katselmoi kovennuskäytäntöjä tutustuen eri laitteiden, ohjelmistojen ja palveluiden konfiguraatioihin toimijan avustuksella. Konfiguraatioista voi pyytää myös kuvaruutukaappauksia ja hyödyntää haastatteluja. Jos kohteita on paljon, kannattaa käyttää kattavaa otantaa, mikä sisältää myös erityyppisiä kohteista. Tähän kannattaa valita toiminnan ja turvallisuuden kannalta keskeisimmät kohteet.

Perustelut

Viitteet

IEC 62443-2-4:2019 (SP 06.02)

IEC 62443-3-3:2019 (SR 7.6)

ISO/IEC 27001:2022 (A8.9)

ISO/IEC 27002:2022 (8.9)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (ID.RA-07, PR.PS-01)

NIS CG Reference document (3.9.1 Configuration management)

Työkalut

Julkri (TEK-10)

Kybermittari: ASSET-1, ASSET-3, ARCHITECTURE-3

3.3.1 Järjestelmäkovennukset viestintäverkkoon ja tietojärjestelmään toteutetaan järjestelmällisesti ja kattavasti - laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Turvallinen konfiguraatio noudattaa esimerkiksi tunnettuja konfiguraatio- tai kovennusreferenssejä. Konfiguraatiot on määritelty kattavasti tietojärjestelmän eri kohteille.
- Turvalliset konfiguraatiot on viety järjestelmiin hallitusti. Tämä voi tarkoittaa esimerkiksi keskitettyä konfiguraationhallintajärjestelmää.

Todennus

1. Valvova viranomainen todentaa, että toimija on valinnut tarvittaessa kovennusreferenssejä laitteidensa ja palveluidensa kovennuksiin. Lisäksi toimija on dokumentoinut mahdolliset poikkeamat näistä. Kovennusreferenssejä tarjoavat esimerkiksi CIS, DISA ja ohjelmistojen toimittajat. Usein referenssitoteutuksista tulee poiketa käytössä olevien ominaisuuksien vuoksi. Referenssivalinnat ja tehdyt poikkeamat voivat olla kirjallisia määrityksiä, jotka voi katselmoida. Kovennusten toteutumisen voi katselmoida esimerkiksi tutkimalla laitteiden, sovellusten ja palveluiden konfiguraatioita. Jos käytössä on keskitetty konfiguraationhallintajärjestelmä, kohteisiin vietävät konfiguraatiot voi tarkastaa siitä. Konfiguraationhallintajärjestelmän lokeista voi tarkastaa konfiguraatiojärjestelmän toimivuutta ja kattavuutta.

Perustelut

Kovennukset ovat yksi tehokkaimmista tavoista yksittäisen sovelluksen tai laitteen osalta pienentää hyökkäyspinta-alaa. Jo yksinkertaisilla kovennuksilla voi saada näkyviä tuloksia aikaiseksi, mutta todellisuudessa erityisesti laajemmissa tuotteissa on valtavat määrät ominaisuuksia, joiden poistamisesta tai konfiguraatiomuutoksesta voi olla hyötyä. Tätä varten valmiiden kovennus- ja konfiguraatio-ohjeiden hyödyntäminen voi olla tarkoituksenmukaista.

Viitteet

IEC 62443-2-4:2019 (SP 06.02)

IEC 62443-3-3:2019 (SR 7.6)

ISO/IEC 27001:2022 (A8.9)

ISO/IEC 27002:2022 (8.9)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (ID.RA-07, PR.PS-01)

NIS CG Reference document (3.9.1 Configuration management)

Työkalut

CIS benchmark

DISA STIG

Julkri (TEK-10)

Kybermittari (ASSET-3, ARCHITECTURE-3)

3.4 Muutosten ja päivitysten hallinta

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.9.

- Toimija on dokumentoinut muutoksenhallintamenettelyn ja siihen liittyvän prosessin. Muutoksenhallintaprosessi voi sisältää esimerkiksi kuvauksen muutoksen hyväksynnästä, muutoksen nopeudesta oikea-aikaisuuden varmistamiseksi sekä kuvauksen korvaavista toimenpiteistä, jos muutos ei ole toteutettavissa.
- Viestintäverkkoon ja tietojärjestelmään kohdistuvat muutokset, korjaukset ja ylläpito on toteutettu muutoksenhallintamenettelyn mukaisesti. Muutoksenhallintamenettely perustuu toimijan toimintaperiaatteisiin.
- Muutoshallintamenettelyyn on kuvattu hätämuutosten tekemiseen liittyvät toimintatavat ja velvoitteet, joissa käy ilmi esimerkiksi dokumentointivaatimukset sekä turvallisuuden varmistamisen toimenpiteet.
- Etäylläpidon kautta tehtyihin muutoksiin on käytetty hyväksyttyjä menettelyjä, jotka estävät luvattomat muutokset.

Todennus

1. Valvova viranomainen todentaa toimijan dokumentaation muutoshallinnan osalta. Toimijalla on kirjallinen kuvaus siitä, miten esimerkiksi konfiguraatio- ja sovelluspäivityksiä sekä muutoksia viedään järjestelmän eri osiin kattavasti ja oikea-aikaisesti päivityksen kriittisyyden ja järjestelmän ominaisuuksien perusteella. Menettelyissä tulisi olla kuvattuna muutoshallintaprosessi, jossa kuvataan esimerkiksi miten mahdolliset muutokset hyväksytään, miten ne pystytään myöhemmin jäljittämään ja miten nopeasti muutos on vietävä kohdejärjestelmiin. Myös mahdolliset korvaavat toimenpiteet on kuvattava, jos muutos ei ole toteutettavissa. Muutoshallinta voi olla toteutettu kevyellä tavalla riskienhallintaan perustuen, riippuen myös toimijan viestintäverkon ja tietojärjestelmän koosta. Tarvittaessa muutoshallinnasta on myös kuvaus, miten muutosten toimivuudesta ja turvallisuudesta varmistutaan, etenkin jos järjestelmän saatavuus- ja luottamuksellisuusvaatimukset ovat erityisen korkeita. Muutoshallinnan on syytä kuvata myös toimintatavat, joita seurataan hätämuutosten yhteydessä.
2. Valvova viranomainen todentaa muutoshallinnan toteutumista hyödyntämällä esimerkiksi muutoksiin liittyviä tapahtumia, tikettejä ja lokikirjauksia. Lisäksi voidaan hyödyntää haastatteluita. Muutoshallintamenettelyiden toteutumista voi todentaa myös vertaamalla konfiguraatio- ja versiotietoa sekä muutoslokia ajossa olevaan konfiguraatioon ja versioon eri kohteissa.

Perustelut

Muutosten ja päivitysten hallinnalla voidaan estää monien haavoittuvuuksien hyväksikäyttö. Nopea reagointi päivitystarpeisiin erityisesti viestintäverkkojen ja tietojärjestelmien ulkokehällä on tärkeä puolustuskeino. Päivitykset itsessään eivät kuitenkaan aina tuota täydellistä lopputulosta. Esimerkiksi viestintäverkossa ja tietojärjestelmässä saattaa olla jokin toinen tuote, jossa samainen haavoittuvuus on ilman ajantasaista päivitystä (patch). Näissä tapauksissa tuotteiden tuntemus sekä tämän perusteella kohdistetut korvaavat toimenpiteet, kuten erilaiset rajoitukset ja valvonta voivat auttaa. Myös tuotteen hankinta ja toimitusketjujen hallinta voivat olla tärkeitä. Joskus haavoittuvuus esimerkiksi käytetyssä kirjastossa ei syystä tai toisesta ole toimittajan tiedossa, jolloin toimittaja ei reagoi

korjaustarpeeseen. Tällaiset tilanteet olisi hyvä huomioida etenkin turvallisuus-kriittisten tuotteiden kohdalla. Organisaatio voi esimerkiksi pitää kirjaa kriittisten tuotteidensa riippuvuuksista (software bill of materials, SBOM) ja reagoida tarvittaessa havaitsemiinsa puutteisiin lopputuotteita päivittämällä.

Viitteet

IEC 62443-2-1:2013 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5),

IEC 62443-3-3:2019 (SR 3.4)

ISO/IEC 27001:2022 (6.3, 8.1, A7.13, A8.32)

ISO/IEC 27002:2022 (7.13, 8.32)

NIST CSF 1.1 (PR.AC-3)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)

NIS CG Reference document (3.9.2 Change management and maintenance)

Työkalut

Julkri (TEK-17)

Kybermittari (ASSET-3, ASSET-4, ARCHITECTURE-5)

3.4.1 Muutosten ja päivitysten hallinta on järjestelmällistä- laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Toimijalla on menettelyt viestintäverkkoihin ja tietojärjestelmiin tuotaviin muutoksiin. Menettelyt huomioivat elinkaaren vaiheet aina suunnittelusta poistoon asti.
- Menettelyt kattavat suunnitellut ja suunnittelemattomat muutokset sekä kehityksen, jos mahdollista.
- Toimijalla on kanavat, joilla seurataan sen viestintäverkkoon ja tietojärjestelmään kohdistuvia haavoittuvuuksia. Kanavana voi olla esimerkiksi kansallinen CSIRT-toiminto (CERT-FI) ja palvelu- tai laitetoimittajien ilmoituskanavat.
- Toimijan viestintäverkon ja tietojärjestelmän kyberturvallisuudelle kriittiset tietoturvapäivitykset on asennettu viipymättä. Jos tämä ei ole mahdollista, korvaavat toimenpiteet on otettu viivytyksettä käyttöön.
- Hätämuutokset on kirjattu niin, että niistä käy ilmi syy normaalin menettelyn ohittamiseen. Jos hätämuutoksen yhteydessä normaalitilanteessa vaadittava testaaminen on ohitettu, testaaminen on suoritettu jälkikäteen niiltä osin kuin mahdollista.
- Muutokset on testattu ja tarkastettu ennen niiden tuomista tuotantojärjestelmiin silloin kun tämä on mahdollista.
- Tarvittaessa muutokselle on tehty turvallisuusvaikutusanalyysi, joka voidaan toteuttaa myös erillisessä testijärjestelmässä.

- Muutosten tuonti järjestelmiin on organisoitua. Muutokset voidaan tuoda esimerkiksi RFC-prosessilla (request for change), missä vastuut ja menettelyt on määritelty.
- Muutoshallintamenettelyt voivat sisältää esimerkiksi seuraavia vaiheita: riskianalyysi, luokittelu ja priorisointi sekä niille tehtävien testien määrittely, muutosten peruutus (roll-back), muutosten dokumentointi ja hyväksyntä.
- Muutokset, ylläpito ja korjaukset on suoritettu ja kirjattu määritellyillä työkaluilla.

Todennus

1. Valvova viranomainen katselmoi toimijan muutoshallintaa kuvaavasta dokumentaatiosta, että muutosten ja päivitysten hallinta on kokonaisuutena hallittua, systemaattista ja organisoitua. Toimijalla on määriteltynä kanavat, joita seurataan tarpeellisten tietoturvapäivitysten ja muutostarpeiden havaitsemiseksi ja toimintatavat, joilla nämä päivitykset ja muutokset analysoidaan ja viedään tarvittaessa viivytyksettä tarvittaviin kohteisiin. Erityisesti kyberturvallisuuteen vaikuttavat muutokset testataan tarvittaessa esimerkiksi testijärjestelmässä tai muulla tavoin toimivuuden ja kyberturvallisuuden osalta ennen niiden viemistä kohteeseen. Valvova viranomainen katselmoi, että muutosten hyväksymiseen, suorittamiseen ja kirjaamiseen on olemassa systemaattinen tapa. Muutoshallinnan dokumentaatiosta käy ilmi myös se, miten mahdolliset etähallinnan kautta tehtävät muutokset ja päivitykset hallitaan, erityisesti kolmansien osapuolien tekemien muutosten osalta.
2. Muutoshallinnan toteutumisen katselmointiin valvova viranomainen voi käyttää kohdassa 3.4 todennusten 2. kohdassa kuvattuja menetelmiä laajennettuna niin, että muutoshallinta on dokumentaatiossa kuvatun mukaista. Eri toimenpiteille on oltava olemassa myös vastuuhenkilöt, jotka tuntevat ja noudattavat prosessia.

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.3.4.3.2, 4.3.4.3.3, 4.3.4.3.5, 4.3.4.3.7)

IEC 62443-2-4:2019 (SP 11)

IEC 62443-3-3:2019 (SR 3.4)

ISO/IEC 27001:2022 (6.3, 8.1, A7.13, A8.32)

ISO/IEC 27002:2022 (7.13, 8.31, 8.32, 8.32)

NIST CSF 1.1 (PR.AC-3, ID.AM-1)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01, ID.IM-01, ID.IM-02)

NIS CG Reference document (3.9.2 Change management and maintenance)

NIS CG Reference document (3.9.5 Security patch management)

Työkalut

Julkri (TEK-17)

Kybermittari (ASSET-4, THREAT-1, THREAT-2)

3.5 Turvallisuuden testaus

Toteutusesimerkki

- Toimijalla on olemassa menettelyt ja toimintatavat tietoturvallisuutensa testaamiseen, siinä laajuudessa kuin tälle on toimintaan, tarpeisiin ja riskiperusteisuuteen perustuva tarve, ks. 1.6 Riskienhallinnan vaikuttavuuden arviointi ja mittaristo. Tämä kattaa tarpeen mukaan sekä teknisen että esimerkiksi prosessien ja menettelytapojen testauksen. Testit voivat kohdistua yksittäisiin järjestelmiin tai koko organisaatioon.
- Turvallisuuden testaus on organisoitua, sille on määritelty vastuuhenkilöt ja se on säännöllistä. Testausta suoritetaan esimerkiksi tietyin väliajoin, uusien järjestelmien käyttöönoton yhteydessä, merkittävien muutosten yhteydessä sekä poikkeamien jälkeen.
- Turvallisuustestauksen sisältö on määriteltyä. Määritykset voivat sisältää esimerkiksi testausmetodien kuvauksen, testattavat kohteet ja oheiskomponentit. Testauksesta tuotetaan kattava dokumentaatio, josta käy ilmi esimerkiksi käytetyt menetelmät, aikaleima ja näyttö (evidenssi).
- Testauksen aikana tehdyt löydökset on käsitelty. Tapauskohtaisesti tämä voi tarkoittaa esimerkiksi prosessin muutosta, haavoittuvuuden vaikutuksen hallintaa, uudelleenarviointia tai jäännösriskin hyväksyntää.

Todennus

1. Valvova viranomainen katselmoi toimijan käytännöt oman turvallisuutensa testaamiseen siten kuin testaustoiminta on toimijan toiminnan, tarpeiden ja riskiarvion perusteella tarpeellista. Joillekin toimijoille kohdan 1.6 toteuttaminen voi olla riittävää, etenkin jos viestintäverkon ja tietojärjestelmien rooli toiminnassa on hyvin pieni ja riskitasoltaan maltillinen. Testaustoimenpiteet voivat olla esimerkiksi säännöllisiä tapahtumia, joissa tehdään määriteltyjä toimenpiteitä. Tällaisia ovat esimerkiksi tiettyihin prosesseihin kohdistuvat tai tekniseen ympäristöön tehtävät testit. Teknisten testien osalta voi katselmoida esimerkiksi tehtyjä testiraportteja.
2. Lisäksi valvova viranomainen voi todentaa testauksen vaikuttavuuden katselmoimalla menetelmät, joilla testauksessa löydetyt poikkeamat käsitellään.

Perustelut

Toimijan suorittamat turvallisuustestaukset auttavat tunnistamaan mahdollisia heikkouksia viestintäverkoissa, tietojärjestelmissä ja prosesseissa. Säännölliset testaukset saattavat estää hyökkääjää hyödyntämästä heikkouksia, jos toimija löytää ja korjaa ne ensin. On tyypillistä, että joskus esimerkiksi prosessissa sattuu virhe ja järjestelmään jää esimerkiksi päivittymättömiä palveluita tai avoimia portteja. Tällöin turvallisuustestaus saattaa tuottaa prosessia korjaavan vaikutuksen.

Viitteet

IEC 62443-2-1:2013 (4.3.4.3.1)

IEC 62443-2-4:2019 (SP 02.02, RE 3) IEC 62443-3-3:2019 (SR 3.5, 3.6, 3.7), ISO/IEC 27001:2022 (A8.29, A8.33, A8.34) ISO/IEC 27002:2022 (8.29, 8.33, 8.34) NIST CSF 1.1 (DE.CM-8, DE.DP-3, RS.MI-3) NIST CSF 2.0 (ID.IM-02, ID.RA-01, ID.RA-06) NIS CG Reference document (3.9.4 Security testing)
Työkalut
Julkri (TEK-03.3, TEK-17) Kybermittari (THREAT-1, THIRD-PARTIES-2)

3.6 Haavoittuvuuksien käsittely ja julkistaminen

Toteutusesimerkki
Tämä kohdistuu vain sellaisten toimijoiden valvontaan, jotka tuottavat sovelluksia, palveluita, laitteita tai tämän kaltaisia tuotteita. • Toimija on ilmoittanut havaitsemansa haavoittuvuudet CVD-menettelytapojen (coordinated vulnerability disclosure) mukaisesti. • Toimijalla on haavoittuvuuksien ilmoittamiseen ja käsittelyyn liittyvät menettelytavat ja käytännöt.
Todennus
1. Valvova viranomainen katselmoi toimijan dokumentaation siitä, miten tuotteista löydetyistä haavoittuvuuksista voi ilmoittaa toimijalle ja miten haavoittuvuudet käsitellään. Lisäksi dokumentaatiosta käy ilmi, miten löydetyt haavoittuvuudet ilmoitetaan tarvittaessa edelleen esimerkiksi kansalliselle CSIRT:lle. Tästä käy ilmi esimerkiksi viestintäkanava, kommunikointitavat sekä vastuuhenkilö.
Perustelut
Viitteet
IEC 62443-2-4:2019 (SP 02.02 RE(2), SP 03.03) ISO/IEC 27001:2022 (A8.8) ISO/IEC 27002:2022 (8.8) ISO/IEC 27003:2018 NIST CSF 1.1 (ID.RA-1, ID.RA-5, PR.IP-12, RS.AN-5, RS.MI-3)

NIST CSF 2.0 (ID.RA-01, ID.RA-05, ID.RA-06, ID.RA-08, PR.PS-02) NIS CG Reference document (3.9.3 Vulnerability handling and disclosure)
Työkalut
Kybermittari (THREAT-2, THIRD-PARTIES-2) Traficomin uutinen: Haavoittuvuudet, miten niistä ilmoitetaan oikein[6]

3.7 Kehittämisen turvallisuus

Toteutusesimerkki
Tämä kohdistuu vain sellaisten toimijoiden valvontaan, jotka tuottavat sovelluksia, palveluita, laitteita tai tämän kaltaisia tuotteita. • Toimija on tuottanut sovellukset ja järjestelmät turvallisten kehityskäytäntöjen mukaisesti, käyttäen esimerkiksi SDLC:n (security/software development life cycle) tai SSDLC:n (secure software development life cycle) määrittelemiä käytäntöjä. Käytännöt koskevat kaikkia kehityskaaren (määrittely, suunnittelu, kehitys, toteutus, testaus, käyttöönotto ja ylläpito) vaiheita. • Kyberturvallisuusvaatimukset on analysoitu määrittelyn ja suunnittelun vaiheissa. • Turvallisen tuotekehityksen toimenpiteet on määritelty. Tämä pitää sisällään esimerkiksi turvalliset arkkitehtuurivalinnat (esimerkiksi zero-trust), turvalliset ohjelmointikäytännöt, turvallisten toimitusketjujen käytön, turvallisten komponenttien valinnat. • Toimija on määritellyt kehitysympäristöä koskevat turvallisuusvaatimukset. • Turvallisuustestausprosessit on määritelty ja otettu käyttöön. Turvallisuustestauksessa voidaan hyödyntää esimerkiksi automaattista työnkulkua (DevSecOps), joka pitää sisällään erilaisia turvallisuustestejä, kuten staattista ja dynaamista turvallisuustestausta (static application security testing SAST, dynamic application security testing DAST), katselmointikäytäntöjä (review), turvallisuusskannauksia ja tunkeutumistestausta (penetration testing). • Testauksessa käytetyn datan turvallisuusvaatimukset on otettu huomioon toiminnassa. Mahdollinen luottamuksellinen data on suojattu vähintään vastaavasti kuin tuotantojärjestelmissä tai se on sanitoitu, anonymisoitu tai pseudonymisoitu.
Todennus
1. Valvova viranomainen katselmoi toimijan dokumentaation siitä, miten toimija toteuttaa turvallista tuotekehitystä. Turvallisen tuotekehityksen toimenpiteet riippuvat paljon tuotteen ominaisuuksista ja todennus suhteutetaan näihin ominaisuuksiin. Usein tuotekehityksessä hyödynnetään yleisesti tunnettuja hyviä toimintatapoja, kuten SDLC tai SSDLC. Dokumentaatiosta käy ilmi, miten toimija varmistuu toimittamiensa tuotteiden tietoturvasta esimerkiksi määrittely-, suunnittelu-, kehitys-, toteutus- ja testausvaiheissa.

[6] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein

2. Valvova viranomainen todentaa kehityskäytäntöjä esimerkiksi katselmoimalla toimijan kehitysinfrastruktuuria. Kehitysinfrastruktuuri sisältää yleensä eri alustoja esimerkiksi kehitykselle, testaukselle, laadunvarmistukselle ja esituotannolle. Lisäksi kehityksen aikana tuotteeseen kohdistetaan tavallisesti turvallisuustestauksia. Mahdolliset lähdekoodit ja konfiguraatiot on luotu turvallisesti esimerkiksi niin, että ulkoisten kirjastojen tuonti tehdään määritettyjen toimintatapojen mukaisesti, lähdekoodin luonnissa on käytetty toimintatapoja, joilla muutoksia voivat tehdä vain tunnistetut ja luvitetut käyttäjät. Jos kehitys kattaa myös laitteistoa, on syytä katselmoida tähän liittyvät toimitusketjut ja testata myös laitteiston turvallisuutta.

Perustelut

Tuotteen testaus on tapa varmistaa, että tuote on mahdollisimman turvallinen. Näin heikkoja toteutuksia ei toimiteta eteenpäin ja toimitettavat tuotteet ovat yhteensopivia kyberturvallisuuden riskienhallinnasta annetun lain kanssa. Testaus on myös tapa löytää haavoittuvuuksia ennen hyökkääjää. Lisäksi kattava testaus ja testaustulosten käsittely voi antaa realistista kuvaa turvallisuuden tilasta ja tuoda mahdolliset heikkoudet näkyväksi, jolloin niihin voi varautua kompensoivilla toimenpiteillä.

Viitteet

IEC 62443-2-1:2013 (4.3.4.3)

IEC 62443-4-1:2018

ISO/IEC 27001:2022 (A8.25, A8.31)

ISO/IEC 27002:2022 (8.25, 8.31)

ISO/IEC 27003:2018

NIST CSF 1.1 (PR.IP-2)

NIST CSF 2.0 (ID.AM-08)

OWASP Application Security Verification Standard

OWASP Top Ten

NIS CG Reference document (3.9.7 Secure development life cycle)

Työkalut

Julkri (TEK-14)

Kybermittari (ARCHITECTURE-4, THIRD-PARTIES-2)

3.7.1 Toimitettavien palveluiden turvallisuus - laajennettu ohjeistus

Toteutusesimerkki

Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa.

- Jos toimija tuottaa viestintäverkko- ja tietojärjestelmäpalveluita tai -järjestelmiä, on tarvittaessa varmistettu, että nämä palvelut ovat tietoturvaltaan kohdan 3.2 Hankinnan kohteen turvallisuus mukaisia. Ks. myös kohta 4.2 Toimitusketjujen riskienhallinta.
- Toimijalla on olemassa kanava, johon tuottamistaan palveluista ja järjestelmistä löydetyistä haavoittuvuuksista voidaan ilmoittaa. Ks. kohta 3.6 Haavoittuvuuksien käsittely ja julkistaminen.
- Toimija on ylläpitänyt palveluistaan ja järjestelmistään komponenttilistaa (esimerkiksi SBOM, software bill of materials; HWBOM, hardware bill of materials), jotta riippuvaisuudet ja näihin kohdistuvat haavoittuvuudet voidaan tunnistaa.

Todennus

1. Valvova viranomainen katselmoi toimittajan kuvaukset siitä, miten toimijan tuottamien palveluiden turvallisuudesta on varmistuttu niin, että ne täyttävät erityisesti kohdissa 3.2 kuvatut tarpeet ja huomioiden lisäksi kohdan 4.2. Kuvauksen sisältö riippuu suuresti palveluiden ja järjestelmien luonteesta ja vaatimukset kuvauksista on suhteutettava tätä vasten. Toimijalla on helposti löydettävissä oleva kanava, johon mahdolliset tietoturvaongelmat raportoidaan sekä menettelyt, joilla näitä raportteja käsitellään ja viedään tarvittaessa lopputuotteeseen (ks. 3.6). Toimijalla pitää olla palveluihin ja järjestelmiin liittyen riittävä dokumentaatio, josta selviää muun muassa riippuvuudet esimerkiksi ulkopuolisista toimittajista tai palveluntarjoajista osana 4.2 ja 3.2 toteutusta. Tämä voi olla toteutettuna niin, että toimija ylläpitää palveluiden ja järjestelmien sisältötietoa (SBOM, HWBOM)
2. Valvova viranomainen täydentää katselmointia esimerkiksi haastatteluin sekä testaamalla toimijan avustuksella haavoittuvuuksien raportointikanavaa. Lisäksi valvova viranomainen voi hyödyntää mahdollisia palveluihin ja järjestelmiin kohdistuvia skannauksia tai testausta ja näistä tuotettua materiaalia.

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.3.4.3)

ISO/IEC 27001:2022 (A8.25, A8.31)

ISO/IEC 27002:2022 (8.25, 8.31)

ISO/IEC 27003:2018

NIST CSF 1.1 (PR.IP-2)

NIST CSF 2.0 (ID.AM-08)

NIS CG Reference document (3.9.7 Secure development life cycle)

Työkalut

Julkri (TEK-14)

Kybermittari (THIRD-PARTIES-2, THREAT-1)

3.8 Viestintäverkkojen rakenteellinen turvallisuus

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtia 11.3 ja 11.4.

- Toimijan viestintäverkko on suojattu luvattomalta pääsyltä. Liikennöinti on sallittu vain tarpeellisiin osoitteisiin ja portteihin tarvittavilla protokollilla.
- Myös palveluntarjoajien etäyhteydet on suojattu. Etäylläpidossa on käytetty erityistä huolellisuutta ja etäylläpitoyhteyksien käyttö on määritelty tarkkarajaisesti.
- Lisäksi toimija voi tarvittaessa rajoittaa palveluntarjoajan pääsyn tarve- ja aikaperusteisesti.
- Viestintäverkossa on käytetty vain toimijan hallitsemia laitteita ja muiden laitteiden liittäminen viestintäverkkoon on ensisijaisesti kielletty.
- Järjestelmien keskinäiset viestintäkanavat voi tarvittaessa suojata menetelmillä, jotka perustuvat esimerkiksi loogiseen tai fyysiseen erotteluun tai salaukseen.
- Toimija on vyöhykkeistänyt (segmentoinut) viestintäverkkonsa niin, että erilaiset palvelut ja järjestelmät erotellaan omiin alueisiinsa. Tämä voi perustua esimerkiksi palveluiden tai järjestelmien kriittisyyteen, haavoittuvuuteen, luottamuksellisuuteen, käyttötarpeeseen tai -tapaan. Hallintaan ja ylläpitoon käytetyt järjestelmät ja vastaavat on mahdollisuuksien mukaan eriytetty omiin vyöhykkeisiin. Vyöhykkeistämisessä on huomioitu erityisesti teollisuusautomaatiolaitteet (OT, operational technology ja ICS, industrial control systems) ja näiden erottelu IT-järjestelmistä.
- Vyöhykkeiden välistä liikennettä on rajoitettu niin, että vain tarpeellinen liikenne on sallittua.
- Toimija on eriyttänyt järjestelmänsä ja viestintäverkkonsa toimittajien ja palveluntarjoajien järjestelmistä ja viestintäverkoista.

Todennus

1. Valvova viranomainen hyödyntää viestintäverkkojen rakenteellisen turvallisuuden katselmoinnissa dokumentaatiota esimerkiksi verkkokuvia, tietojärjestelmäkuvauksia, toimintatapoja ja muita ohjeita. Esimerkiksi verkkokuvista käy ilmi se, miten erilaiset ei-luotetuista viestintäverkoista tulevat yhteydet on rajoitettu esimerkiksi kulkeviksi yksittäisten pisteiden kautta. Näitä pisteitä ovat yleensä esimerkiksi palomuurit, salauslaitteet ja etäyhteyspisteet. Lisäksi toimija on voinut jakaa tietojärjestelmiään ja viestintäverkkojaan erillisiin osiin esimerkiksi eri roolien, tietoturvallisuustarpeiden, käyttötarpeiden tai kriittisyyden mukaan.
2. Valvova viranomainen todentaa verkon rakennetta haastatteluin ja konfiguraatiokatselmoinnein. Reunalaitteissa sekä eri sisäverkon osien välillä on sallittuna vain välttämätön liikenne. Tämä voidaan todentaa esimerkiksi palomuuri- tai reitityssäännöistä, tarvittaessa toimijan kanssa yhteistyössä. Joissain tapauksissa suodatusta voidaan tehdä myös laite- tai sovellustasolla itse kohteessa (esimerkiksi palvelu tai päätelaite). Palomuuri ja etäyhteyspisteet ovat kieltäneet oletusarvoisesti kaiken sellaisen liikenteen, jota ei tarvita. Vastaavaa toiminnallisuutta voidaan saavuttaa myös muilla tavoilla, kuten staattisella reitityksellä ja salauksella. Vyöhykkeistäminen voidaan todentaa usein edellä mainituin tavoin tai tutkimalla verkon aktiivilaitteiden konfiguraatiota. Yksi tavallisimmin käytetty tapa on jakaa eri vyöhykkeet eri virtuaalilähiverkkoihin (virtual local area network VLAN), mutta muitakin tekniikoita voi

olla käytössä. Näiden konfiguraatioiden katselmointeihin voi olla erityisen hyvä hyödyntää toimijan henkilökuntaa.

3. Verkon rakenteellista suojausta voidaan todentaa myös eri skannaussovelluksilla sekä hyödyntäen toimijan tekemiä tietoliikennenauhoituksia. Toimija voi olla tehnyt skannauksia itse tai käytössä on ollut kolmas osapuoli, joiden tuloksia valvova viranomainen katselmoi.

   Skannaustyökaluja voidaan hyödyntää esimerkiksi kartoittamalla viestintäverkon eri osien näkyvyyttä verkon muista osista. Tässä kannattaa huolehtia siitä, että skannauksia suoritetaan ristiin verkon eri osien välillä. Lisäksi erityistä huolellisuutta kannattaa käyttää skannauksissa, joissa tarkastellaan näkyvyyttä ei-luotetuista viestintäverkoista toimijan viestintäverkkoihin. Skannausten lisäksi voidaan hyödyntää erilaisten tietoliikennepakettien generointia. Eri lähteistä voidaan tehdä yhteydenottoyrityksiä testattavan kohteen palveluihin käyttäen esimerkiksi selainta ja muita ohjelmia. Verkon turvallisuuden tarkastamisessa voi hyödyntää myös tietoliikennenauhoituksia, joista voi katselmoida eri laitteiden välistä viestittelyä ja tarkastaa, etteivät ei-sallitut laitteet viestittele keskenään.

Perustelut

Viestintäverkon suojaaminen estää suuren osan turvattomista verkoista tulevasta haittaliikenteestä. Tietojärjestelmän ja viestintäverkon vyöhykkeistäminen on keskeinen keino, jolla hyökkääjän etenemistä viestintäverkossa ja tietojärjestelmässä voidaan hidastaa sen jälkeen, kun tämä on saanut jalansijaa hyökkäyksen kohteesta.

Viitteet

IEC 62443-2-1:2013 (4.2.3.5, 4.3.3.4),

IEC 62443-2-4:2019 (SP 02.03)

IEC 62443-3-3:2019 (SR 1.11, 1.12, 1.13, 2.5, 2.6, 2.7, 3.1, 3.8, 5.1, 5.2, 5.4, 7.7)

ISO/IEC 27001:2022 (A8.16, A8.20, A8.22)

ISO/IEC 27002:2022 (8.16, 8.20, 8.22)

ISO/IEC 27003:2018

NIST CSF 1.1 (PR.AC-3, PR.AC-5)

NIST CSF 2.0 (PR.AA-03, PR.AA-05, PR.IR-01)

NIS CG Reference document (3.9.8 Network security)

NIS CG Reference document (3.9.9 Network segmentation)

Työkalut

Julkri (TEK-01)

Kybermittari (ARCHITECTURE-2)

Skannaukseen: nmap, Nessus, OpenVAS, Rapid7

Tietoliikennenauhoitukseen: Wireshark, tcpdump, netflow, sFlow

Yhteydenottoyritykseen: ping, hping3, nc, ssh, Pythonin scapy-kirjasto

3.9 Haittaliikennesuojaukset

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.5.

- Toimijalla on tapa havaita haittaliikennettä ja estää luvattomat sovellukset ja näiden suorittaminen, jos tämä on mahdollista.
- Haittaliikennettä havainnoivat sovellukset on päivitetty riittävän usein, jotta ne kykenevät tunnistamaan uudet haittaohjelmat. Tämä voi tarkoittaa esimerkiksi kerran päivässä tai muutoin säännöllisesti tehtävää tunnisteiden tai heuristiikkatiedon päivitystä.
- Lisäksi luvattomien ulkoisten medioiden liittäminen järjestelmiin on estetty.
- Haittaohjelmien havainnointia ja estämistä voi tehdä myös esimerkiksi sähköposti- ja web-liikenteestä.
- Haittaohjelmien havainnoinnin ja luvattomien sovellusten suoritusten eston tulisi koskea kaikkia laitteita, mukaan lukien mobiililaitteita. Jollei tätä pystytä toteuttamaan, on käytettävä muita korvaavia ratkaisuja.

Todennus

1. Valvova viranomainen todentaa, että toimija havaitsee ja estää kattavasti haitallista liikennettä. Haittaohjelmien tai hyökkääjän tuottamaa haittaliikennettä on estetty erityisesti sellaisissa liityntäpisteissä, jossa toimijan viestintäverkko ja tietojärjestelmä yhdistyy ei-luotettuihin verkkoihin tai toiminnaltaan keskeisimpiin verkon osiin. Oleellisia kohteita ovat tyypillisesti esimerkiksi palomuurit, etäkäyttöpisteet (esimerkiksi VPN-yhdyskäytävä), langattoman verkon infrastruktuuri, viestintäjärjestelmät kuten e-mail ja SMS sekä usein myös ulkopuolelle tarjotut palvelut, kuten web-palvelut ja rajapinnat. Haitallisen liikenteen etenemistä on ehkäisty myös estämällä luvattomien ja haitallisten sovellusten ajamista ja asentamista. Tämän voi tehdä esimerkiksi haittaohjelmia tunnistavilla ja estävillä sovelluksilla, tuntemattomien ulkoisten laitteiden estävillä sovelluksilla sekä luvattomien ohjelmistojen ajon ja asennuksen estävillä sovelluksilla ja säännöillä. Tietyissä tapauksissa voidaan hyödyntää myös menettelyihin ja käytäntöihin nojautuvia ratkaisuja, jos esimerkiksi järjestelmän riskitaso on erityisen pieni, tekniset ratkaisut eivät ole mahdollisia tai muutoin oikeasuhtaisia.
2. Valvova viranomainen todentaa konfiguraatioista, että haittaliikenteen havaitsevat ja estävät suojaukset ovat käytössä. Lisäksi järjestelmien toimivuus on hyvä katselmoida hyödyntäen esimerkiksi lokitietoa. Jos haittaliikennettä torjutaan menettelyihin ja käytäntöihin perustuvilla organisatorisilla ratkaisuilla, voi näihin liittyvää tietoisuutta ja osaamista todentaa esimerkiksi haastatteluin.
3. Valvova viranomainen testaa toimijan avulla sekä luvalla haittaliikenteen havaitsevien ja estävien suojausten toimintaa. Nämä testit eivät kuitenkaan saa vaarantaa toimijan viestintäverkkoa tai tietojärjestelmää. Testaaminen voidaan tehdä esimerkiksi yrittäen ohittaa sähköpostin suojauksia eri tavoin, kuten käyttäen väärennettyjä osoitteita, yrittäen ajaa vaaratonta mutta luvatonta ohjelmaa eri kohteissa sekä kohdistaen palveluihin vaarattomia mutta kiellettyjä syötteitä.

Perustelut

Suuri osa onnistuneista hyökkäyksistä perustuu haittaohjelmiin, joita voivat olla esimerkiksi virukset, madot ja troijalaiset. Ohjelmistoissa voi olla myös haitallisia ominaisuuksia, kuten takaportteja, jotka mahdollistavat hyökkääjän pääsyn järjestelmään. On tärkeää, että ohjelmistot asennetaan turvallisista lähteistä ja haitallisia sovelluksia yritetään estää. Sovellusten kykyjen rajoittaminen voi myös toimia. Tällöin osa haitallisen sovelluksen toiminnasta saatetaan kyetä estämään.
Viitteet
IEC 62443-3-3:2019 (SR 3.2, 3.3) ISO/IEC 27001:2022 (A5.32, A8.7) ISO/IEC 27002:2022 (5.32, 8.7) ISO/IEC 27003:2018 NIST CSF 1.1 (DE.CM-4, DE.CM-5, DE.CM-7) NIST CSF 2.0 (DE.CM-01, DE.CM-03, DE.CM-09) NIS CG Reference document (3.9.10 Protection against malicious and unauthorized software)
Työkalut
Julkri (TEK-11) Kybermittari (ARCHITECTURE-3, SITUATION-2) Haittaliikenteen estoon: sähköpostille mm. Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) ja Sender Policy Framework (SPF), verkkosovelluksen palomuuri (web application firewall WAF), välityspalvelin, tunkeilijan havaitsemisjärjestelmä/murron estämisjärjestelmä (intrusion detection/prevention system IDS/IPS) Luvattomien sovellusten suorituksen estoon: SELinux, AppArmor, Windows Defender Application Control WDAC, AppLocker

4 Toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan d alakohtaan ja 21 artiklan 3 kohtaan. Näiden kohtien kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 4 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 4 kohdassa.

1. **Listaus toimittajista ja palveluntarjoajista**: Toimijalla on ajantasainen tieto kaikista välittömistä toimittajista ja palveluntarjoajista. (Ks. kohta 4.1).

2. **Toimitusketjujen riskienhallinta**: Toimijan ottaa riskienhallinnassaan huomioon toimitusketjuhäiriön vaikutus omaan toimintaan sekä varautua mahdolliseen toimitushäiriöön. Toimijan ottaa turvallisuusnäkökohdat huomioon suhteessa toimitusketjunsa välittömiin laite- tai palvelutoimittajiin. Riskien

hallintatoimenpiteitä harkitessa otetaan huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Nämä voivat sisältää erilaisia turvallisuuteen liittyviä vaatimuksia esimerkiksi saatavuuden, ylläpidettävyyden ja sopimusten osalta. NIS yhteistyöryhmä, Euroopan komissio ja ENISA tulevat yhteistyössä NIS2-direktiivin 22 artiklan mukaisesti laatimaan riskiarviointeja tietyistä toimitusketjuista. Toimijat voisivat hyödyntää riskiarvioita soveltuvin osin. (Ks. kohta 4.2).

4.1 Listaus toimittajista ja palveluntarjoajista

Toteutusesimerkki
• Toimija on pitänyt yllä hakemistoa kaikista välittömistä laite- ja palvelutoimittajistaan sekä tarvittaessa muista kyberturvallisuuteen vaikuttavista toimittajista. • Hakemisto pitää sisällään kontaktitiedot toimittajiin. Toimija on pitänyt erityistä huolta niiden toimittajien tietojen ylläpidosta, joilla on pääsy kriittisiin toimintoihin tai jotka ylläpitävät kriittisiä toimintoja. • Hakemisto kuvaa palvelut, järjestelmät ja tuotteet, joita toimittaja tuottaa. Lisäksi hakemistossa on hyvä olla sopimukseen liittyvät asiat, kuten sopimuskauden pituus ja elinkaareen liittyvät asiat.
Todennus
1. Valvova viranomainen katselmoi, että toimijalla on kattava listaus välittömistä laite- ja palvelutoimittajistaan. Listauksesta käy ilmi esimerkiksi yhteystiedot sekä toimittajan toimittamat palvelut, järjestelmät ja tuotteet.
Perustelut
Viitteet
ISO/IEC 27001:2022 (A5.22) NIST CSF 1.1 (ID.SC-2, ID.SC-3) NIST CSF 2.0 (GV.SC-03, GV.SC-05, GV.SC-07) NIS CG Reference document (8.2 Directory of suppliers and service providers)
Työkalut
Kybermittari (THIRD-PARTIES-1, CRITICAL-1)

4.2 Toimitusketjujen riskienhallinta

Toteutusesimerkki

- Toimija on tunnistanut kohdassa 4.1 tunnistettujen toimittajien osalta mahdollisten toimitusketjuhäiriöiden vaikutuksen omaan toimintaansa. Toimija on määritellyt tarpeelliset varautumistoimet mahdollisissa toimitushäiriöissä. Jatkuvuus- ja toipumissuunnittelua tarkennetaan kohdassa 10.1.
- Toimija on sisällyttänyt välittömät laite- ja palvelutoimittajat osaksi riskienhallinnan toimintamallia, tekee niihin riskiarvioinnin ja käsittelee niihin kohdistuvat riskit. Toimija on valinnut oikeasuhtaiset toimenpiteet toimitusketjuihin liittyen ja toteuttanut toimenpiteet sellaisiin toimittajiin, joihin kohdistuvilla riskienhallinnan toimenpiteillä on kyberturvallisuutta edistävä vaikutus. Ks. kohta 1.1 Kyberturvallisuuden riskienhallinnan toimintamalli.
- Riskienhallinnan toimenpiteitä harkitessa toimija on ottanut huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset
    - haavoittuvuudet, kuten sijainnista, tuotevalikoimasta tai toimialan luonteesta johtuvat haavoittuvuudet;
    - tuotteisiin ja palveluihin kohdistuvan yleisen laadun ja häiriönsietokyvyn;
    - tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, jotka voivat perustua toimittajan käyttämiin käytäntöihin, sertifiointeihin tai muihin näyttöihin.
- Toimija on tarvittaessa sisällyttänyt toimitusketjuihinsa erilaisia kyberturvallisuuteen liittyviä vaatimuksia esimerkiksi saatavuuden, ylläpidettävyyden ja sopimusten osalta. Toimijan pitäisi tunnistaa heille tärkeät, kyberturvallisuuteen liittyvät ominaisuudet ja asettaa oikeasuhtaiset vaatimukset. Näitä voivat olla esimerkiksi sopimuksiin asetettavat palvelutasosopimukset.
- Toimija on hallinnut toimitusketjujen kyberturvallisuusriskiä esimerkiksi sisällyttämällä kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita toimija tekee välittömien toimittajiensa ja palveluntarjoajiensa kanssa. Näitä voivat olla esimerkiksi kyberturvallisuusominaisuuksien arviointi sopimuskauden aikana, vaatimukset henkilöstön koulutuksesta ja sertifioinnista, ilmoittamiskäytännöt haavoittuvuuksista sekä palvelun ylläpitokäytäntöjen tarkastelu. Katso myös kohta 3.2 Hankinnan kohteen turvallisuus.
- Toimija on huomioinut toimittajien ja palveluntarjoajien valinnassa myös valvovan viranomaisen mahdolliset määräykset NIS2-direktiivin 22 artiklan toimitusketjujen riskiarvioinnin tuloksista.
- Toimija voi myös pyytää tarvittaessa kriittisistä tuotteista ja palveluista komponenttilistaa (esimerkiksi SBOM, software bill of materials, HWBOM, hardware bill of materials), jotta riippuvaisuudet ja näihin kohdistuvat haavoittuvuudet voidaan tunnistaa ja hallita.

Todennus

1. Valvova viranomainen todentaa, että toimija on toteuttanut riskienhallinnassaan toimitusketjujen turvallisuuteen liittyvät näkökohdat. Toimija on toteuttanut seuraavat asiat:
    - Toimija on ottanut huomioon mahdolliset toimitusketjuhäiriöt omassa toiminnassaan. Toimija on varautunut toimitusketjuhäiriöihin esimerkiksi varajärjestelyin, sopimusteknisesti tai osana jatkuvuudenhallintaa (ks. 10.1).
    - Toimija on ottanut huomioon turvallisuusnäkökohdat suhteessa välittömiin laite- tai palvelutoimittajiin. Valvova viranomainen todentaa esimerkiksi dokumentaatiosta, että miten turvallisuusnäkökohdat on otettu huomioon. Tämä voi ilmentyä esimerkiksi laite- ja palvelutoimittajiin kohdistuvista turvallisuusvaatimuksista, rajoituksista suhteessa toimijan

viestintäverkkoon ja tietojärjestelmään sekä vaadittavista menettelyistä ja käytännöistä (ks. esimerkiksi perustason tietoturvakäytännöt, 11).

- Toimija on ottanut toimitusketjuista aiheutuvat riskit osaksi riskienhallintatoimenpiteitä siinä määrin, kuin toimija on arvioinut tarpeelliseksi kyberturvallisuuden varmistamiseksi. Tämä voi tarkoittaa esimerkiksi toimittajalle tai palveluntarjoajalle ominaisten haavoittuvuuksien huomioimista. Toimija on tunnistanut tuotteiden ja palveluiden yleisen laadun ja häiriönsietokyvyn, sekä ottanut nämä asiat huomioon esimerkiksi osana jatkuvuudenhallintaa, kohdistaen tuotteisiin tai palveluihin riskienhallintakeinoja ja suojaten keskeisimpiä toiminteitaan.
- Toimija on ottanut toimitusketjuissaan huomioon tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet. Tämä tarkoittaa esimerkiksi sitä, että toimija selvittää toimitusketjujen kyberturvallisuuden tason siinä määrin, kuin on mahdollista, ja hallitsee tästä aiheutuvia riskejä osana riskienhallintaansa. Toimija on voinut selvittää kyberturvallisuuden tasoa esimerkiksi laite- tai palvelutoimittajan maineella, tietoturvasertifikaateilla, sopimuksen tai hankinnan osana (ks. 3.2) ja pyytämällä dokumentaatiota tai muuta materiaalia. Toimija on voinut hallita laite- tai palvelutoimittajalta periytyviä jäännösriskejä tunnistamalla ne ja ottamalla ne mukaan osaksi omaa riskienhallintaansa.
- Toimija on ottanut toimitusketjuissaan huomioon toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Näitä voi huomioida esimerkiksi edellä kohdassa d mainituilla tavoilla. Lisäksi toimija on yleensä määritellyt, millä käytännöillä toimittajat ja palveluntarjoajat tarjoavat palveluitaan toimijan viestintäverkkoon ja tietojärjestelmään. Käytännön esimerkkeinä toimija on voinut määrittää esimerkiksi sen, millä laitteilla tai millä etäyhteyskäytännöillä toimittaja tai palveluntarjoaja voi tuottaa palveluaan toimijan viestintäverkkoon tai tietojärjestelmään. Toimija on voinut määrittää myös ohjeita, velvoitteita ja koulutuksia (ks. 6), joita toimittajalta tai palveluntarjoajalta (henkilöstöltä) vaaditaan.

Perustelut

Toimitusketjuja hyödyntävät vakavat haavoittuvuudet ja hyökkäykset ovat yleistyneet viime vuosina huomattavasti. Toimitusketjujen haavoittuvuutta on hyödynnetty myös iskuissa perusinfrastruktuuria vastaan.

Viitteet

ISO/IEC 27001:2022 (A5.19, A5.20, A5.21, A8.30)

NIST CSF 1.1 (ID.BE-1, ID.SC-1, ID.SC-2, ID.SC-3, ID.SC-4)

NIST CSF 2.0 (GV.OC-05, GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-07)

NIS CG Reference document (3.8.1 Supply chain policy)

Työkalut

Julkri (HAL-06, TEK-16, TSU-16)

Kybermittari (THIRD-PARTIES-1, THIRD-PARTIES-2, CRITICAL-2, CRITICAL-3)

5 Omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan osittaiseen i alakohtaan. Alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 5 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 5 kohdassa.

1. **Omaisuudenhallinnan menettelyt ja ohjeet**: Toimijalla on säännölliset ja dokumentoidut omaisuudenhallinnan menettelyt ja ohjeet, jotka pitävät sisällään myös toimintojen, prosessien ja tietojen tunnistamisen. (Ks. kohta 5.1).

2. **Omaisuusluettelo ja omaisuuden luokittelu**: Viestintäverkkoon ja tietojärjestelmään liittyvä omaisuus tulisi tunnistaa ja luokitella suojaustarpeiden perusteella. Omaisuudesta tulisi ylläpitää ajantasaista luetteloa. Omaisuudella tarkoitetaan esimerkiksi tiloja, laitteita, ohjelmistoja, palveluita, henkilöitä, aineetonta omaisuutta ja resursseja kuten immateriaalioikeuksia tai IP-osoitteita. (Ks. kohta 5.2).

3. **Omaisuusluettelon käyttö**: Omaisuudenhallinnan tulisi olla oleellinen osa esimerkiksi henkilöstön, ulkoisten toimijoiden ja tietojärjestelmien muutoksia sekä laitteiden elinkaaren hallintaa käyttöönotosta turvalliseen poistamiseen asti. (Ks. kohta 5.1).

5.1 Omaisuudenhallinnan menettelyt ja ohjeet

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.2.

- Toimijan on laatinut menettelyt ja ohjeet omaisuudenhallintaan ja ne ovat yleensä linjassa organisaation turvallisuutta koskevien toimintatapojen ja menettelyiden kanssa. Turvallisuutta koskevista toimintatavoista ja menettelyistä on kirjoitettu tarkemmin kohdissa 2.1 ja 2.1.1 Turvallisuutta koskevat toimintaperiaatteet ja menettelyt.
- Toimija on sisällyttänyt omaisuudenhallinnan menettelyihin ja ohjeisiin järjestelmällisen toimintojen, prosessien ja tietojen tunnistamisen.
- Menettelyt ja ohjeet kattavat omaisuuden koko elinkaaren hankinnasta, turvallisesta kuljetuksesta, varastoinnista ja käytöstä aina turvalliseen hävittämiseen sekä tiedon poistamisen ja tuhoamisen asti.
- Menettelyt ja ohjeet voivat sisältää käytännöt omaisuusluettelon ylläpitoon ja ajan tasalla pitämiseen sekä säännölliseen katselmointiin (esim. kerran vuodessa ja merkittävien muutosten tai poikkeamien yhteydessä).

Todennus

1. Valvova viranomainen katselmoi toimijan laatimat dokumentit menettelyistä ja ohjeista omaisuudenhallinnalle. Menettelyt ja ohjeet ovat ajantasaisia ja niistä käy ilmi toimijan toimintojen, prosessien ja tietojen järjestelmällinen tunnistaminen sekä menettelyt omaisuusluettelon ylläpitoon, jota on tehty esimerkiksi suunnitelluin väliajoin ja merkittävien muutosten tai poikkeamisen tapahtuessa.

Perustelut

Omaisuudenhallinta on tehokas työkalu kyberturvallisuusriskien hallinnassa ja omaisuuden huolellinen hoitaminen ennaltaehkäisee riskien toteutumista ja auttaa riskien hallinnassa. Se on myös yksi halvimmista ja helpoimmin käyttöönotettavista turvallisuuden hallintakeinoista.

Viitteet

ISO/IEC 27001:2022 (A5.9, A5.10, A5.14, A7.10)

ISO/IEC 27002:2022 (5.9, 5.10, 5.14, 7.10)

IEC 62443-2-1:2013 (4.3.4.4.6)

IEC 62443-3-3:2019 (SR 2.4)

NIST CSF 1.1 (ID.AM-1, ID.AM-2)

NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-04, ID.AM-08)

NIS CG Reference document (3.4.2 Asset Handling)

Työkalut

Julkri (HAL-04)

Kybermittari (PROGRAM-2, ASSET-1, ASSET-2, ASSET-5)

5.2 Omaisuusluettelo ja omaisuuden luokittelu

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.2.

- Toimija on laatinut toimintaansa ja tarkoituksiinsa sopivan omaisuusluettelon toiminnoista, prosesseista ja tiedoista, joihin voi sisältyä myös toimijan tilat, laitteet, ohjelmistot, palvelut, henkilöt, aineeton omaisuus ja resurssit kuten immateriaalioikeudet tai IP-osoitteet. Omaisuusluettelo on ajantasainen.
- Omaisuusluettelo voi sisältää esimerkiksi seuraavanlaisia tietoja:
  - Omaisuus ja omaisuuden yksilöivä tunniste
  - Omistaja, hallinnoija ja käyttäjät
  - Kuvaus
  - Sijainti
  - Omaisuuden tyyppi (ohjelmistot ml. virtuaalikoneet, laitteistot sekä niiden käyttöjärjestelmät ja laiteohjelmistot, palvelut, tilat, LVI-järjestelmät, henkilöstö, fyysiset tallenteet)
  - Omaisuuden luokittelu
  - Riskiarviointiin perustuva riskiluokitus (ja tarvittaessa luokituksen vaikutus, vrt. kohtaan 5.3)
  - Laitteen ohjelmistoversio, ohjelmiston SBOM (software bill of materials)
  - Käyttötuen päättymispäivä
  - Varmuuskopiointi

- Omaisuusluokittelu on perustunut omaisuuden tietoturvatarpeisiin, kuten luottamuksellisuuteen, eheyteen ja saatavuuteen. Toimija on voinut sisällyttää tietoturvatarpeisiin myös aitouden ja kiistämättömyyden.
- Omaisuusluokittelulla voidaan määrittää omaisuuden suojaustarpeita sen kriittisyyden, arkaluonteisuuden, riskin ja liiketoiminta-arvon mukaan. Toimija on arvioinut omaisuuteen kohdistuvia riskejä osana kyberturvallisuuden riskienhallinnan toimenpiteitä. Toimija voi sisällyttää omaisuusluettelossa omaisuuteen kohdistuvan ulkoisen uhkan todennäköisyyden tai riskiluokituksen.
- Omaisuuden saatavuuteen liittyvien vaatimusten on hyvä olla linjassa liiketoiminnan jatkuvuuden ja palautumissuunnitelmien kanssa (ks. 10).
- Toimija on määritellyt luokittelun suojattavalle tiedolle ja se on esimerkiksi osana henkilöstön koulutusta. Toimija on viestinyt siitä henkilöstölle ja keskeisille sidosryhmille (ks. 6.5).
- Toimija on voinut hyödyntää tiedon luokittelussa esimerkiksi kansallista lainsäädäntöä, kansallisesti tai kansainvälisesti tunnettuja tiedonluokittelun suosituksia ja ohjeita.

Todennus

1. Valvova viranomainen katselmoi toimijan omaisuusluettelon. Omaisuusluettelo sisältää toteutusesimerkissä mainitut toimijan toiminnot, prosessit ja tiedot. Toimijalla on käytössä omaisuusluokittelu omaisuuden suojaustarpeiden perusteella. Toimija on katselmoinut ja päivittänyt omaisuusluetteloa säännöllisesti. Omaisuusluettelon oikeellisuus voidaan todentaa dokumentaatiokatselmoinnilla niin, että omaisuusluettelon sisältöä verrataan saatavilla olevaan muuhun dokumentaatioon, kuten verkkokuviin, hankintatietoihin, valvontanäkymiin ja valvonnassa saatuihin havaintoihin.
2. Valvova viranomainen tarkastaa omaisuusluettelon oikeellisuutta fyysisellä tarkastelulla. Valvova viranomainen voi esimerkiksi käydä läpi toimijan tilat ja verrata täältä löytyviä laitteita omaisuusluetteloon.

   Omaisuusluettelon oikeellisuutta voi tarkastella myös teknisin keinoin. Vaihtoehtoja ovat muun muassa konfiguraatiotarkastelu esimerkiksi ARP-taulujen (vain IPv4) sisältö, huomioiden kuitenkin, että kaikki laitteet, erityisesti ICS/OT (industrial control system/operational technology) -puolella, eivät välttämättä tee ARP-kyselyjä automaattisesti, DHCP-tietokanta (leases database), DNS-tiedot.
3. Valvova viranomainen todentaa omaisuusluettelon oikeellisuutta passiivisilla ja aktiivisilla skannauksilla. Passiivisessa skannauksessa hyödynnetään esimerkiksi verkkonauhoitusta, josta haetaan kaikki liikenteeseen osallistuneet toimijan laitteet. Aktiivisessa skannauksessa käydään läpi toimijan IP-osoiteavaruuksia (IPv4, IPv6).

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.2.3.4, 4.2.3.6, 4.3.4.4.2, 4.3.4.4.3, 4.3.4.4.6, A.2.3.3.8.3)

IEC 62443-3-3:2019 (SR 7.8)

ISO/IEC 27001:2022 (A5.9, A5.12, A5.13)

ISO/IEC 27002:2022 (5.9, 5.12, 5.13) ISO/IEC 27005:2022 NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5, PR.IP-1) NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01) NIS CG Reference document (3.4.1 Asset classification) NIS CG Reference document (3.4.4 Asset inventory)
Työkalut
Julkri (HAL-04.2) Kybermittari (ASSET-1 ja ASSET-2, THIRD-PARTIES-1) Skannausohjelmistoja: arp scan, nmap, Nessus, hping3

5.3 Omaisuusluettelon käyttö

Toteutusesimerkki
• Toimija on varmistanut, että omaisuusluettelo on ajan tasalla ja sen sisältö palvelee tarpeen mukaan muuta toimintaa kuten riskienhallintaa, päivitysten-hallintaa, liiketoiminnan jatkuvuutta ja omaisuuden elinkaaren hallintaa. • Omaisuusluetteloa on päivitetty säännöllisesti ja esimerkiksi merkittävien muutosten yhteydessä, joita voivat olla viestintäverkkoihin ja tietojärjestel-miin liittyvät muutokset mukaan lukien teknologiavalinnat, työkalut ja tilit. • Omaisuusluettelon muutoshistorian on hyvä olla jäljitettävissä. • Omaisuusluettelo tukee laitteiden elinkaaren hallinnassa laitteen turvallisesta käyttöönotosta sen käytöstä poistamiseen asti. Laitteen turvallista käyttöönot-toa on tarkennettu kohdassa 3.4 Muutosten- ja päivitysten hallinta. • Toimija on huomioinut laitteiden palauttamisen ja tietojen poistamisen, hal-lussa olleiden tilien ja käyttäjätunnusten lopettamisen työsuhteen tai alihan-kintasopimuksen päätyttyä. Tästä on lisää kohdissa 6.1 Henkilöstöturvallisuu-den menettelyt ja 6.2 Henkilöstöturvallisuuden menettelytavat.
Todennus
1. Valvova viranomainen katselmoi omaisuusluettelon kohdan 5.2. mukaisesti. Toimija on päivittänyt omaisuusluetteloa säännöllisesti tai muutosten yhtey-dessä. Valvova viranomainen katselmoi omaisuudenhallintaa esimerkiksi osana koh-dan 1 riskienhallinnan toimintamallin katselmointia. Tämä tarkoittaa esimer-kiksi sitä, että toimijan riskienhallinta on linjassa tunnistetun omaisuuden kanssa. Toimija on myös voinut sisällyttää omaisuusluetteloonsa esimerkiksi omaisuuteen kohdistuvan riskin ja luokituksen vaikutuksen.
Perustelut

Viitteet
IEC 62443-2-1:2013 (4.2.3.4, 4.3.3.2, A.2.3.3.8.3)
IEC 62443-3-3:2019 (SR 7.8)
ISO/IEC 27001:2022 (A5.9, A5.11, A5.18, A5.24)
ISO/IEC 27002:2022 (5.9, 5.11, 5.18, 5,24)
ISO/IEC 27005:2022
NIST CSF 1.1 (ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5 PR.IP-1)
NIST CSF 2.0 (ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, PR.PS-01)
NIS CG Reference document (3.4.4 Asset inventory)
NIS CG Reference document (3.4.5 Return or deletion of assets upon termination of employment)
Työkalut
Julkri (HAL-04)
Kybermittari (ASSET-1, ASSET-2, ASSET-3, ACCESS-1, ACCESS-2)

6 Henkilöstöturvallisuus ja kyberturvallisuuskoulutus

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan osittaiseen i alakohtaan ja g alakohtaan. Näiden alakohtien kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 6 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 6 kohdassa.

1. **Henkilöstöturvallisuuden menettelyt**: Henkilöstöturvallisuudella tarkoitetaan menettelyjä, joilla varmistetaan henkilöiden tietoturvavastuut ja velvollisuudet, tietoturvaosaaminen ja taustatarkastukset sekä avainhenkilöriskien hallinta. Lisäksi nämä menettelyt kattavat väärinkäytösten estämistä, kuten vaarallisten työyhdistelmien tunnistamista ja välttämistä, työtehtäväkiertoa, sekä työsuhteen tai sopimuksen päättymisen. (Ks. kohta 6.1).

2. **Henkilöstöturvallisuuden menettelytavat**: Toimijalla tulisi esimerkiksi olla henkilöstöön liittyvät menettelytavat, joissa huomioidaan myös ulkoiset toimijat, kuten alihankkijat. Menettelytavoissa voitaisiin huomioida myös työsuhteen päättymisen ja työtehtävien muutoksien jälkeiset vastuut ja velvollisuudet. (Ks. kohta 6.2).

3. **Salassapito ja velvollisuudet**: Henkilöstöä ja ulkoisia toimijoita voitaisiin tarvittaessa esimerkiksi tiedottaa heidän työtehtäviensä ja tarjoamiensa palveluiden turvallisuuteen liittyvistä vastuista ja velvoitteista, kuten esimerkiksi salassapitoon liittyen. (Ks. kohta 6.3).

4. **Taustatarkistukset**: Jos työtehtävien ja vastuiden katsotaan vaativan erityistä luotettavuutta, henkilölle voitaisiin tarvittaessa tehdä riittävät taustatarkistukset. (Ks. kohta 6.4).

5. **Henkilöstökoulutus**: Toimijan olisi huolehdittava siitä, että henkilöstöllä on kyvykkyys toimia kyberturvallisuuden toimintaperiaatteiden mukaisesti.

Tämän saavuttamiseksi olisi järjestettävä säännöllisesti koulutuksia menettelyistä ja käytännöistä, jotka tähtäävät yleisen kyberturvallisuustietoisuuden parantamiseen ja tietoisuuteen kyberturvallisuusriskeistä sekä työtehtäviin nähden riittävään osaamiseen liittyen viestintäverkon ja tietojärjestelmän suojaamiseen, kyberturvallisuusriskien tunnistamiseen, kyberturvallisuusriskien hallintakäytäntöjen ja hallintakäytäntöjen vaikutusten arviointiin toimijan tarjoamiin palveluihin. (Ks. kohta 6.5 ja 6.5.1).

6. **Johdon perehtyneisyys**: Erityisen tärkeää olisi saada toimijan hallintoelinten jäsenet osallistumaan koulutuksiin. (Ks. kohta 6.6).

6.1 Henkilöstöturvallisuuden menettelyt

Toteutusesimerkki
• Toimijalla on kirjalliset menettelyt, jotka kuvaavat henkilöiden tietoturvavastuut ja velvollisuudet. • Toimijan henkilöstöturvallisuuden menettelyissä kuvataan myös kolmannet osapuolet, kuten ulkoiset toimijat ja alihankkijat (ks. 6.2). • Toimijan henkilöstöturvallisuuden menettelyt kuvaavat, miten henkilöstön tietoturvaosaaminen varmistetaan (ks. 6.5). • Toimijan henkilöstöturvallisuuden menettelyt kattavat myös taustatarkistuksiin (ks. 6.4) ja avainhenkilöihin (ks. 6.6) liittyvät tarpeet. • Henkilöstöturvallisuuden menettelyt huomioivat tarvittaessa henkilöstön eri roolit. Tämä voi näkyä esimerkiksi johdon vastuun huomioimisessa osana menettelyitä. Toimija voi esimerkiksi määritellä, nimetä ja valtuuttaa viestintäverkkojen ja tietojärjestelmien turvallisuuteen ja riskienhallintaan liittyvät roolit toimijan tarpeiden mukaan. • Toimija voi määritellä roolit, vastuut ja valtuudet, jotka koskevat kyberturvallisuuden riskienhallinnasta annettavan lain velvoitteita, kuten esimerkiksi 9 § mukaisten kyberturvallisuuden riskienhallinnan toimenpiteiden suorittamista ja 11 § mukaista poikkeamista ilmoittamista toimivaltaiselle viranomaiselle ilmoittamista (ks. 9.1 ja 9.7). • Toimija on viestinyt henkilöstöturvallisuuteen liittyvistä menettelyistä ja keskeisistä turvallisuuteen liittyvistä rooleista henkilöstölle ja kolmansille osapuolille. • Toimija on huolehtinut, että rooleihin nimetyillä henkilöillä on riittävät tiedot ja taidot tehtäviensä suorittamiseen (ks. 6.5). • Toimijan menettelyt edistävät väärinkäytösten estämistä. Toimija on tunnistanut vaaralliset työyhdistelmät ja huolehtinut tehtävien eriyttämisestä. Tehtävien eriyttämisellä vältetään tilanteita, joissa muodostuu työyhdistelmiä, jotka muodostavat riskejä tai joissa on ristiriitaisia velvollisuuksia ja vastuualueita. Tyypillinen vaarallinen työyhdistelmä on esimerkiksi sellainen, että henkilö sekä pyytää että hyväksyy toimenpiteen, tai että henkilöllä on pääsy sekä valvottavaan kohteeseen että valvonnassa saatuihin tietoihin. • Toimijan henkilöstöturvallisuuteen liittyvät menettelyt kuvaavat menettelytavat, joilla estetään väärinkäytöksiä. Näihin menettelytapoihin voi liittyä esimerkiksi työsuhteiden muutokset, tehtäväkierto, sopimuksen tai työsuhteen muuttuminen sekä päättyminen.
Todennus
1. Valvova viranomainen todentaa, että toimijalla on kirjalliset menettelyt henkilöstöturvallisuuden osalta. Näissä menettelyissä on kuvattu tietoturvavastuut

ja velvollisuudet, joita henkilöstön tulee noudattaa turvallisuuden saavuttamiseksi. Menettelyt kuvaavat tietoturvakoulutukset, taustatarkistukset ja avainhenkilöt. Menettelyt koskevat tarvittaessa myös kolmansia osapuolia, kuten alihankintakumppaneita, vähintään toimintatapojen osalta (ks. 6.2). Menettelyt sisältävät väärinkäytösten estämiseen liittyvät asiat, kuten vaarallisten työyhdistelmien tunnistamisen ja tehtävien eriyttämisen, sekä työsuhteisiin ja sopimuksiin liittyvät muutokset ja päättymiset.

2. Valvova viranomainen todentaa esimerkiksi haastatteluilla henkilöstöturvallisuuden menettelyiden tunnettuutta ja toteutumista. Haastatteluista tulisi käydä ilmi esimerkiksi avainhenkilöroolien toiminta käytännössä niin, että tehtävän toteuttamiseen on varattu riittävät resurssit ja valtuudet. Lisäksi henkilöstöä haastatellaan vaarallisista tehtäväyhdistelmistä ja niiden eriyttämisestä käytäntöjen tasolla.

Perustelut

Tietoturvallisuus on kokonaisuus, jossa tärkein tekijä on henkilöstö. Henkilöstö on usein myös tietoturvan heikoin lenkki, jolloin henkilöstön tietoturvatietoisuus ja henkilöstöön liittyvät menettelyt sekä toimintatavat ovat äärimmäisen tärkeitä.

Organisaatioiden riskienhallinnassa henkilöstö on tärkein elementti. On tärkeää valjastaa henkilöstö kykyjensä mukaan tunnistamaan omaan työhön kohdistuvia riskejä. Yhteistyöllä saa yleensä parempaa riskienhallintaa aikaiseksi kuin rajatun joukon tekemällä työllä.

Viitteet

IEC 62443-2-1:2013 (4.3.3.2),

IEC 62443-2-4:2019 (SP 01.07)

ISO 27001:2022 (5.3, 7.1, 7.2, A5.2, A5.3, A5.5, A6.2, A6.3, A6.5)

ISO 27002:2022 (5.2, 5.3, 5.5, 6.2, 6.3, 6.5)

NIST CSF 1.1 (PR.AT-5, PR.IP-11)

NIST CSF 2.0 (PR.AT-02, GV.RR-04)

NIS CG Reference document (3.5.1 Human resources security)

NIS CG Reference document (3.5.4 Disciplinary process)

Työkalut

Julkri (HAL-02)

Kybermittari (WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, THIRD-PARTIES-1, ARCHITECTURE-2, ARCHITECTURE-3, ACCESS-1, ACCESS-2, ACCESS-3, Hallintatoimet)

6.2 Henkilöstöturvallisuuden menettelytavat

Toteutusesimerkki

- Toimijan henkilöstöturvallisuuden menettelytavat toteuttavat työsuhteiden muutoksiin ja päättymisiin liittyvät menettelyt.
- Muutoksiin liittyvät toimenpiteet voivat sisältää esimerkiksi käyttöoikeuksien muutoksia henkilön käyttämään laitteistoon työtehtävien muuttuessa.
- Menettelytavat kuvaavat myös toimenpiteet, joita tehdään työtehtävien päättyessä. Näitä voivat olla muun muassa käyttöoikeuksien ja laitteiden poisto, tiedon tuhoaminen sekä omaisuuden, osaamisen ja vastuiden siirtoon liittyvät toimenpiteet. Nämä toimenpiteet on myös kerrottu henkilöstölle.
- Henkilöstöturvallisuuden menettelytavat koskevat myös kolmansia osapuolia, kuten ulkoisia toimijoita ja alihankkijoita.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimijalla on menettelytavat työtehtävien muutosten ja päättymisen yhteydessä suoritettaviin toimenpiteisiin. Nämä menettelytavat koskevat myös kolmansia osapuolia, kuten ulkoisia toimijoita ja alihankkijoita.
2. Valvova viranomainen voi todentaa esimerkiksi järjestelmistä ja konfiguraatioista sen, että menettelytapojen mukaiset vastuut ja velvollisuudet on toteutettu. Tämä voi tarkoittaa esimerkiksi sitä, että tarpeettomaksi käyneet käyttöoikeudet on muutettu tai poistettu, laitteet on palautettu, tarpeettomat tiedot on poistettu ja vastuut on siirretty tarvittaessa muulle henkilöstölle.

Perustelut

Työtehtävien muutos on tilanne, jossa on suuri riski sille, että esimerkiksi tarpeettomia oikeuksia, tietoa tai laitteistoa jää henkilölle, joka ei ole näihin enää oikeutettu. Erityisesti tapaukset, joissa henkilön työtehtävät päättyvät, voivat joissain tapauksissa aiheuttaa suurenkin riskin organisaation tietoturvalle, ellei resursseihin pääsyä estetä.

Viitteet

IEC 62443-2-1:2013 (4.3.3.2)

IEC 62443-2-4:2019 (SP 01.07)

ISO/IEC 27001:2022 (A6.5)

ISO/IEC 27002:2022 (6.5)

NIST CSF 1.1 (PR.IP-11)

NIST CSF 2.0 (GV.RR-04)

NIS CG Reference document (3.5.3 Termination or change of employment procedures)

Työkalut

Kybermittari (WORKFORCE-1, THIRD-PARTIES-1, THIRD-PARTIES-2, ACCESS-1, ACCESS-2, ACCESS-3)

6.3 Salassapito ja velvollisuudet

Toteutusesimerkki
• Toimija varmistaa, että kohdassa 6.1 Henkilöstöturvallisuuden menettelyt kuvatut menettelyt sisältävät esimerkiksi laitteiston käsittelyyn, käyttäjätunnusten käyttöön, hallintaan ja ylläpitoon, Internet-käyttäytymiseen, sosiaaliseen mediaan, omien laitteistojen käyttöön, ohjelmistoturvallisuuteen ja ulkoisiin tallennusmedioihin liittyviä ohjeita ja velvollisuuksia. • Toimija varmistaa erityisesti, että salassapitoon liittyvät velvoitteet on kuvattu ja kerrottu henkilöstölle sekä tarvittaessa kolmansille osapuolille. Toimija on määrittänyt salassa pidettävät asiat selkeästi. Tämän voi toteuttaa esimerkiksi merkitsemällä salassa pidettävä tieto tai tietojärjestelmät. Lisäksi toimijan pitää varmistaa, että tietoa luovutettaessa ja vastaanottaessa sitä käsitellään oikein. • Henkilöstön, mukaan lukien kolmansien osapuolten henkilöstön, tulee ymmärtää, toteuttaa ja noudattaa henkilöstöturvallisuuteen liittyviä velvoitteita. Toimija on kuvannut myös sen, miten tietoturvavelvoitteista tiedotetaan henkilöstölle.
Todennus
1. Valvova viranomainen todentaa, että toimija on määritellyt tietoturvaan liittyvät velvoitteet. Nämä velvoitteet ovat kattavat ja tukevat toimijan tietoturvallisuuden toteutumista. Dokumentaatiosta tulisi lisäksi selvitä salassapitoon liittyvät määrittelyt ja vastuut sekä yleensä myös miten salassa pidettävän materiaalin oikea käsittely varmistetaan tietoa luovutettaessa ja vastaanottaessa. 2. Valvova viranomainen todentaa esimerkiksi haastatteluilla, että tietoturvavelvoitteet toteutuvat, henkilöstö on niistä tietoinen ja henkilöstö tunnistaa mahdolliset salassa pidettävät kohteet ja tuntee niihin liittyvät vastuut ja velvoitteet.
Perustelut
Viitteet
ISO/IEC 27001:2022 (A5.10, A6.6) ISO/IEC 27002:2022 (5.10, 6.6) NIST CSF 1.1 (PR.AT-3, PR.AT-4, PR.AT-5) NIST CSF 2.0 (PR.AT-02)
Työkalut
Julkri (HAL-15) Kybermittari (WORKFORCE-1, WORKFORCE-3, THIRD-PARTIES-2)

6.4 Taustatarkistukset

Toteutusesimerkki
• Toimija on tunnistanut ne työtehtävät ja vastuut, jotka vaativat erityistä luotettavuutta. Näissä tapauksissa on tarvittaessa todennettava henkilön kelpoisuus kyseisiin tehtäviin taustatarkistuksin. • Taustatarkistukset uusitaan esimerkiksi viiden vuoden välein tai henkilön työtehtävien vaihtuessa.
Todennus
1. Valvova viranomainen todentaa, että toimija on tunnistanut sellaiset työtehtävät ja vastuut, joihin valittavan henkilön tulee käydä läpi taustatarkistukset.
Perustelut
Viitteet
IEC 62443-2-1:2013 (4.3.3.2.2, 4.3.3.2.3) IEC 62443-2-4:2019 (SP 01.04) ISO/IEC 27001:2022 (A6.1) ISO/IEC 27002:2022 (6.1) NIST CSF 1.1 (PR.IP-11) NIST CSF 2.0 (GV.RR-04) NIS CG Reference document (3.5.2 Background checks)
Työkalut
Julkri (HAL-10) Kybermittari (ACCESS-1)

6.5 Henkilöstökoulutus

Toteutusesimerkki
Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.1. • Toimija on huolehtinut siitä, että henkilöstöllä on tieto ja riittävä osaaminen toimia kyberturvallisuuden toimintaperiaatteiden mukaisesti siinä määrin, kuin tämä on työtehtävien osalta oleellista. Tämän saavuttamiseksi on järjestetty säännöllisesti koulutuksia menettelyistä ja käytännöistä, jotka tähtäävät yleisen kyberturvallisuustietoisuuden parantamiseen ja tietoisuuteen kyberturvallisuusriskeistä sekä työtehtäviin nähden riittävään osaamiseen liittyen viestintäverkon ja tietojärjestelmän suojaamiseen, kyberturvallisuusriskien

tunnistamiseen, kyberturvallisuusriskien hallintakäytäntöjen ja hallintakäytäntöjen vaikutusten arviointiin toimijan tarjoamiin palveluihin.

- Toimija on määrittänyt tavat, joilla toimijan kyberturvallisuuteen liittyvistä toimintatavoista annetaan koulutusta koko henkilöstölle.
- Henkilöstölle annettava koulutus on kattanut kyberturvallisuusriskien hallintatoimenpiteet. Koulutuksen tehtävänä on varmistaa erityisesti se, että henkilöstö toiminnallaan tukee hallintatoimenpiteiden toteutumista niiltä osin, kuin tämä on työtehtävien kannalta oleellista.
- Toimija on kouluttanut henkilöstöään myös kyberriskien hallinnan osalta, niiltä osin kuin ne ovat työtehtävien kannalta oleellisia. Tämä voi tarkoittaa esimerkiksi tiedotusta tyypillisimmistä kyberriskeistä ja tarvittaessa hallintatoimenpiteiden vaikutusten arviointia esimerkiksi omiin työtehtäviin liittyvistä kyberriskeistä. Lisäksi toimija on kouluttanut henkilöstönsä tunnistamaan mahdollisia kyberriskejä esimerkiksi toimijan kyberriskien hallinnan tueksi.
- Toimija on voinut tunnistaa tehtäviä ja rooleja, joihin voi kohdistua erityistä mielenkiintoa. Näitä henkilöitä voi suojata räätälöidyillä koulutuksilla esimerkiksi sosiaalisesta manipuloinnista, vaikuttamisyrityksistä ja tiedonkalastelusta.
- Toimija voi edistää henkilöstön yleistä kyberturvallisuustietoisuutta myös kevyemmillä tavoilla. Tässä voidaan hyödyntää esimerkiksi lyhyitä tietoiskuja tuoreista huijausyrityksistä tai toimialan tapahtumista.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimija tarjoaa koulutusta henkilöstölleen kyberturvallisuusriskien hallinnasta, tunnistamisesta ja tarvittaessa arvioinnista. Koulutus pitää sisällään menettelyt ja käytännöt, joilla toimija edistää kyberturvallisuustietoisuutta sekä kyberturvallisuusriskien hallintaa. Koulutus tähtää siihen, että henkilöstöllä on työtehtäviinsä nähden riittävä osaaminen viestintäverkon ja tietojärjestelmän suojaamiseen ja kyberturvallisuusriskien tunnistamiseen. Tarvittaessa koulutuksella pitää myös varmistaa, että työtehtävien niin vaatiessa henkilöstöllä on kyky kyberturvallisuusriskien hallintakäytäntöjen ja niiden vaikutusten arviointiin koskien toimijan tarjoamia palveluita.

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.3.2.4)

ISO/IEC 27001:2022 (7.2, A6.3)

ISO/IEC 27002:2022 (6.3)

NIST CSF 1.1 (PR.AT-1)

NIST CSF 2.0 (PR.AT-01)

NIS CG Reference document (3.6.2 Security training)

Työkalut

Julkri (HAL-13)

Kybermittari (WORKFORCE-2, WORKFORCE-4)

6.5.1 Henkilöstökoulutus - laajennettu ohjeistus

Toteutusesimerkki
Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa. • Toimija on toteuttanut kyberturvallisuuteen liittyvän koulutuksen järjestelmällisesti ja seurannut koulutukseen osallistumista. • Koulutus on kattavuudeltaan riittävän laajaa ja sen osana voidaan myös mitata koulutukseen osallistuvien henkilöiden ymmärrys koulutuksen aiheesta. • Toimijalla on käytännöt, joita sovelletaan puuttuvan koulutuksen suorittamiseksi.
Todennus
1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on määritellyt koulutuksen tapahtuvan järjestelmällisesti. Lisäksi toimijalla on oltava käytännöt koulutukseen osallistumisen valvomiseen. 2. Valvova viranomainen todentaa esimerkiksi osallistumisrekisteristä tai vastaavasta, että henkilöstö osallistuu koulutuksiin ja tästä varmistutaan. Haastatteluilla voidaan lisäksi todentaa henkilöstön kyberturvallisuusosaamista ja -tietoisuutta.
Perustelut
Viitteet
IEC 62443-2-1:2013 (4.3.2.4) ISO/IEC 27001:2022 (7.2, A6.3) ISO/IEC 27002:2022 (6.3) NIST CSF 1.1 (PR.AT-1) NIST CSF 2.0 (PR.AT-01) NIS CG Reference document (3.6.2 Security training)
Työkalut
Kybermittari (WORKFORCE-4)

6.6 Johdon perehtyneisyys

Toteutusesimerkki

- Toimijan on varmistuttava siitä, että johdolla on riittävä osaaminen yleisestä kyberturvallisuusriskien hallinnasta. Tämä voidaan toteuttaa esimerkiksi koulutuksilla tai itseopiskelulla.
- Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa, toimitusjohtajaa, tai muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.
- Toimijan on varmistuttava siitä, että johto on perehtynyt toimijan kyberturvallisuusriskien hallintaan ja kykenee tekemään siihen perustuvia päätöksiä. Johto tuntee myös oman roolinsa, vastuunsa ja vaikutusvaltansa kyberturvallisuusriskien hallinnassa.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että johdon jäsenet ovat osallistuneet riittäviin koulutuksiin. Tämän myötä johdolla on esimerkiksi riittävä ymmärtämys kyberturvallisuusriskien hallinnasta ja he tuntevat roolinsa, vastuunsa ja vaikutusvaltansa asiassa. Organisaation johto on tietoinen organisaatiossa tehtävästä kyberturvallisuusriskien hallinnasta ja kykenee käsittelemään riskienhallinnan tuloksia.
2. Valvova viranomainen voi todentaa esimerkiksi koulutusrekisteristä tai haastatteluilla, että johdon jäsenet ovat osallistuneet kyberturvallisuuden riskienhallinnan koulutuksiin, opintojaksoihin tai osoittavat muutoin omaavansa riittävän osaamisen. Lisäksi valvova viranomainen voi selvittää, miten jäsenet ovat ottaneet kyberriskienhallinnan toimenpiteet huomioon päätöksissään ja toimissaan.

Perustelut

Toimiva kyberriskienhallinta vaatii johdon sitoutuneisuutta. Toisaalta kyberympäristön ja tähän liittyvien riskien ymmärtäminen vaatii osaamista. Kyberturvallisuusriskien hallinnassa johdolla on useimmiten suuri vastuu sekä keskeisiä tehtäviä, jotka liittyvät esimerkiksi hallintatoimenpiteiden valitsemiseen, jäännösriskeihin liittyviin päätöksiin, resurssien järjestämiseen sekä valtuuttamiseen.

Viitteet

IEC 62443-2-1:2013 (4.3.2.3.3, 4.3.2.6, 4.4.3)

ISO/IEC 27001:2022 (5.1, 9.3, A5.4)

ISO/IEC 27002:2022 (5.4)

NIST CSF 1.1 (GV.PO-01, -02, PR.AT-4)

NIST CSF 2.0 (PR.PS-04, PR.AT-02)

NIS CG Reference document (3.1 Top management commitment and accountability)

Työkalut

Kybermittari (RISK-1, RISK-2, RISK-3, RISK-4, RISK-5, PROGRAM-2, WORKFORCE-4)

7 Pääsynhallinnan ja todentamisen menettelyt

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan osittaiseen i alakohtaan ja osittaiseen j alakohtaan. Näiden alakohtien kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 7 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 7 kohdassa.

1. **Pääsynhallinnan menettelyt**: Pääsynhallinnan ja todentamisen menettelyiden tulisi koskea luonnollisia käyttäjiä kuten henkilöstöä ja ulkoisia toimijoita sekä järjestelmätunnuksia kuten laitteiden, ohjelmistojen, rajapintojen ja muiden oleellisten resurssien käyttämiä tunnuksia. Pääsynhallinnan tulisi koskea sekä ohjelmistolla todennettavaa pääsyä että fyysistä pääsyä. Menettelyiden tulisi perustua liiketoimintavaatimuksiin sekä tietoverkkoja ja tietojärjestelmiä koskeviin vaatimuksiin järjestelmien erityispiirteet huomioon ottaen. Toimijalla tulisi olla pääsynhallintaan liittyvät määrittelyt ja käytännöt, joilla varmistetaan kattavasti luotettava tunnistaminen ja joilla sallitaan pääsy vain tarvittaviin viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin sekä muihin resursseihin. (Ks. kohta 7.1).

2. **Pääsynhallinnan ja käyttöoikeuksien jatkuva ylläpito**: Toimijalla tulisi olla menettelyt koko käyttäjätunnusten ja käyttöoikeuksien elinkaaren ajalle ja käyttöoikeuksia olisi hallittava niiden mukaisesti. (Ks. kohta 7.2).

3. **Pääsynhallinnan valvonta**: Käyttöoikeuksia ja niiden käyttöä tulisi valvoa. (Ks. kohta 7.3 ja 7.3.1).

4. **Pääsynhallintaan liittyvä kirjanpito ja vähimpien oikeuksien periaate**: Käyttöoikeuksista ja käyttöoikeusrooleista olisi pidettävä ajantasaista kirjaa ja käyttäjille on annettava vain ne oikeudet, jotka ovat työtehtävien suorittamisen vuoksi välttämättömiä (vähimpien oikeuksien periaate). (Ks. kohta 7.4).

5. **Pääkäyttäjätunnukset**: Toimijoilla tulisi olla menettelyt vahvojen oikeuksien käyttäjätilien ja pääkäyttäjätilien hallintaan. Pääkäyttäjäoikeudet tulisi rajoittaa mahdollisimman pienelle käyttäjäjoukolle ja näitä tunnuksia on suojattava vahvoin menetelmin. Pääkäyttäjäoikeuksien käyttöä tulisi valvoa. (Ks. kohta 7.5).

6. **Turvallisten todennusmenetelmien valinta ja luotettava todennus**: Valittavien todentamiskäytäntöjen ja -tekniikoiden tulisi perustua tietojen saatavuutta koskeviin vaatimuksiin ja todentamisen menettelyihin. Todennusmenetelmien olisi oltava riittävän turvallisia niin, että oikeudeton käyttö on mahdollisuuksien mukaan estetty. Tarvittaessa todennusmenetelmänä tulisi käyttää vahvaa tunnistusta, monivaiheista todentamista tai jatkuvaa todentamista, mikäli niiden käyttö on mahdollista. (Ks. kohta 7.6).

7.1 Pääsynhallinnan menettelyt

Toteutusesimerkki
• Pääsynhallinnan ja todentamisen menettelyt koskevat luonnollisia käyttäjiä, kuten henkilöstöä ja ulkoisia toimijoita, sekä järjestelmätunnuksia, kuten laitteiden, ohjelmistojen, rajapintojen ja muiden oleellisten resurssien käyttämiä tunnuksia. • Toimijalla on pääsynhallintaan liittyvät menettelyt, määrittelyt ja käytännöt, joilla varmistetaan luotettava tunnistaminen (authentication, AuthN)

kattavasti viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin sekä muihin resursseihin.

- Toimijan pääsynhallinnan ja todentamisen menettelyt kattavat sekä ohjelmistolla todennettavan että fyysisen pääsyn.
- Menettelyt perustuvat liiketoimintavaatimuksiin sekä tietoverkkoja ja tietojärjestelmiä koskeviin vaatimuksiin järjestelmien erityispiirteet huomioiden.
- Pääsynhallinnan ja todentamisen menettelyillä on varmistettu, että tunnistaminen on mahdollisuuksien mukaan käyttäjäkohtaista ja siinä varmistutaan käyttäjän identiteetistä riittävällä tasolla. Tunnistusmenetelmän valinta on voinut perustua järjestelmän riskiarvioon. Järjestelmässä, jonka riskitaso on matala, voi myös käyttäjänimeen ja turvalliseen salasanaan perustuva tunnistaminen olla riittävää. Korkeamman riskitason järjestelmissä on mahdollisuuksien mukaan käytetty useaan tekijään perustuvia todennusmenetelmiä (monivaiheinen tunnistautuminen, multi-factor authentication, MFA). Näitä voivat olla käyttäjän salasanan lisäksi esimerkiksi aikaperusteiset kertakäyttökoodit, digitaaliset varmenteet, sirukortit, tunnistevälineet tai biometriset keinot.
- Jos toimijalla on käytössään yhteiskäyttöisiä tunnuksia, on hyvien käytänteiden mukaista varmistaa, että todennusmenetelmät ovat niihin oikeutettujen henkilöiden hallinnassa ja että todennusmenetelmät ovat helposti vaihdettavissa ja turvallisella tavalla jaeltavissa tunnuksen käyttäjille.
- Toimija on sallinut pääsyn (authorization, AuthZ) vain tarvittaviin viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin sekä muihin resursseihin. Nämä pääsyt on toteutettu määrittelyjen perusteella. Sallittu pääsy on määritelty vähimpien oikeuksien periaatteella. Yleensä käyttäjään perustuvia valtuutuksia kannattaa välttää, ja niiden sijaan on hyvä käyttää esimerkiksi roolipohjaista käyttöoikeuksien hallintaa.
- Toimija on huomioinut tehtävien riittävän eriyttämisen salliessaan pääsyn tarvittaviin resursseihin. Tehtävien eriyttämisestä on lisätietoa kohdassa 6.1 Henkilöstöturvallisuuden menettelyt.
- Fyysisen pääsynhallinnan menettelyt ja käytännöt on järjestetty toimijan liiketoimintatarpeiden ja riskienhallinnan perusteella. Kriittisten järjestelmien osalta on pyritty kykyyn tunnistaa käyttäjät yksilöllisesti esimerkiksi kulunvalvonnan keinoin. Fyysisestä turvallisuudesta ja tilaturvallisuudesta on lisää kohdassa 12.
- Toimija voi oman harkintansa mukaan ottaa käyttöön osittain tai kokonaan luottamattomuuden periaatteen (zero-trust) osaksi pääsynhallinnan periaatteitaan, mikäli se on sovellettavissa toimijan arkkitehtuuriin. Luottamattomuuden periaatetta käytetään yleensä etenkin pilvipalvelujen tai hybridipilven yhteydessä.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on menettelyt, määrittelyt ja käytännöt pääsynhallintaan ja todentamiseen. Menettelyt ovat kattavat ja huomioivat toimijan erilaiset toiminteet fyysisistä tiloista aina ohjelmistorajapintoihin. Näihin kuuluvat sekä henkilökäyttäjien että järjestelmätunnusten pääsynhallinta ja todentaminen. Toimija on huomioinut myös kolmannet osapuolet pääsynhallinnassaan. Valvova viranomainen varmistaa, että toimija on järjestänyt pääsynhallinnan ja todentamisen menettelyt, määrittelyt ja käytännöt siten, että tunnistaminen on luotettavaa ja perustuu vähimpien oikeuksien periaatteeseen.
2. Valvova viranomainen todentaa, että toimijan järjestelmät sallivat käyttäjille vain sellaiset toimenpiteet, joihin käyttäjillä on valtuudet. Tämä voidaan varmistaa esimerkiksi käyttöoikeuksien katselmoinnilla tai tietoturvatestauksella,

jossa testataan esimerkiksi, että käyttäjät eivät pysty tekemään heille määriteltyjä oikeuksia laajempia toimenpiteitä. Katselmoinnissa voi tarkistaa, että järjestelmissä asetetut roolit ja henkilöt vastaavat kuvattuja määrittelyitä (ks. 7.4) ja todentaa näin menettelyiden toteutuminen. Järjestelmistä voi myös todentaa, että turvalliset todentamisen ja tunnistamisen menetelmät ovat tosiasiallisesti käytössä. Tässä voi hyödyntää esimerkiksi konfiguraatiotietoa ja kuvaruutukaappauksia.

Perustelut

Pääsynhallinnan menettelyt ja käytännöt varmistavat sen, että pääsynhallinnan kontrollit ovat oikein mitoitettuja ja kattavat kaikki toimijan järjestelmät. Pääsynhallinnan kattavuus varmistaa sen, että kontrolli vaikuttaa kaikissa tarpeellisissa paikoissa. Menettelyiden ja käytäntöjen tulisi huomioida perinteiseksi kirjautumiseksi miellettyjen toimintojen (esimerkiksi tietokoneelle tai verkkosivulle sisäänkirjautuminen) lisäksi myös muut toiminnot, jotka edellyttävät pääsynhallintaa, kuten tiedostojaot. Pääsynhallinnan häiriötilanteet saattavat aiheuttaa tietovuotoja tai -murtoja oikeudettomien henkilöiden päästessä tietoihin, jotka eivät kuulu heille.

Viitteet

IEC 62443-2-1:2013 (4.3.3.6, 4.3.3.7)

IEC 62443-3-3:2019 (SR 2.1)

ISO/IEC 27002:2022 (5.3, 5.15, 5.16, 5.17, 5.18, 8.5)

NIST CSF 1.1 (PR.AC-4, PR.AC-7)

NIST CSF 2.0 (PR.AA-03, -05)

NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators7

NIS CG Reference document (3.7.1 Access control policy)

NIS CG Reference document (3.7.5 Identification)

Työkalut

Julkri (HAL-14, TEK-07, TEK-08)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3)

7.2 Pääsynhallinnan ja käyttöoikeuksien jatkuva ylläpito

Toteutusesimerkki

- Toimijan pääsynhallinnan menettelyt ja käytännöt varmistavat, että käyttäjätunnukset ja käyttöoikeudet ovat ajantasaiset.

[7] https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF

- Toimijan pääsynhallinnan elinkaariajattelussa on otettu huomioon työsuhteiden, sopimusten ja muiden vastaavien muutoksien tuomat vaikutukset. Esimerkiksi ylimääräiset käyttäjätunnukset ja käyttöoikeudet poistetaan tarpeen päättyessä.
- Menettelyissä on määritelty tarvittavat käytännöt ja vastuut pääsynhallinnan ja käyttöoikeuksien muutoksiin.
- Ylläpitotunnusten ja pääkäyttäjätunnusten käyttöoikeuksien hallinnointiin on kiinnitetty erityistä huomiota ja ne ovat jatkuvasti ajantasaiset.
- Toimijalla on ajantasainen kirjanpito tai vastaava menettely käyttäjätileistä ja niiden käyttöoikeuksista (ks. 7.4).

Todennus

1. Valvova viranomainen todentaa, että toimijan pääsynhallinnan menettelyissä ja käytännöissä on toimintatavat, joilla seurataan käyttöoikeuksien elinkaarta. Niissä on huomioitu mm. käyttäjänhallintaprosessi, pääsyoikeuksien poistaminen ja väliaikaisten tunnusten käyttö. Pääsyoikeuksien poistossa on huomioitu erityisesti käyttäjät, jotka eivät enää työskentele organisaatiossa tai joilla ei enää ole asiallista tarvetta kyseisiin resursseihin esimerkiksi työtehtävien muutoksen johdosta. Lisäksi toimijalla on toimintatavat mahdollisten väliaikaisten tunnusten käytöstä.
2. Valvova viranomainen todentaa, että toimijan pääsynhallinta on ajantasainen. Katselmoimalla voidaan todeta, että tarpeettomat käyttäjätilit on poistettu tai lukittu. Käyttäjätilien oikeudet katselmoidaan ja varmistetaan, että niillä on vain tarvittavat vähimmäisoikeudet, jotka vastaavat toimijan muuta dokumentaatiota (ks. 7.4).

Perustelut

Ylimääräiset käyttäjätunnukset ja pääsyoikeudet voivat mahdollistaa hyökkääjälle pääsyn järjestelmään. Liian laajat käyttöoikeudet voivat mahdollistaa työntekijälle oikeudet katsella tai käsitellä resursseja, joihin ei ole työtehtäviin perustuvaa asiallista tarvetta.

Viitteet

IEC 62443-2-1:2013 (4.3.3.5.1, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.8)

ISO/IEC 27002:2022 (5.18)

NIST CSF 1.1 (PR-AC.1)

NIST CSF 2.0 (PR.AA-01, PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

Työkalut

Julkri (HAL-14, TEK-07.3)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-6, WORKFORCE-1)

7.3 Pääsynhallinnan valvonta

Toteutusesimerkki

- Toimija on valvonut järjestelmien ja laitteiden pääsyä ja käyttöä. Jotta valvonta voidaan toteuttaa, toimija on muodostanut esimerkiksi lokitietoa pääsynhallintatapahtumista tai muuta tapahtumajäljityksen mahdollistavaa luotettavaa tietoa. Pääsynhallintaan liittyviä tapahtumia ovat esimerkiksi tunnusten muokkaaminen, kirjautumiseen liittyvät tiedot (kuka, mitä, mistä, mihin ja milloin), tunnusten käyttö ja pääkäyttäjätoimenpiteet.
- Pääsynhallinnan tapahtumista syntyvää lokia on säilytetty riittävän pitkään, jotta mahdolliset väärinkäyttötapaukset voidaan selvittää myös myöhemmässä vaiheessa, esimerkiksi poikkeaman tutkinnan yhteydessä.
- Tapahtumakirjauksen perusteella on valvottu esimerkiksi epänormaaleja kirjautumisyrityksiä ja muita riskienhallintaan perustuvia tapahtumia.
- Valvonta on voitu toteuttaa esimerkiksi manuaalisilla menettelyillä, automaattisia hälytyksiä tuottavalla järjestelmällä, trendejä seuraamalla ja ilmoituskanavia hyödyntäen. Valvonnasta on lisää tietoa tämän suosituksen kohdassa 9.3 Tapahtumien kirjaaminen ja havainnointi.
- Poikkeamien seurauksena käyttäjätili on tarvittaessa suljettu, lukittu tai sen todennusmenetelmä resetoitu. (Ks. 9.5)
- Joissain tapauksissa toimija on voinut käyttää myös manuaalista kirjanpitoa, esimerkiksi vierailijakirjaa. Tämä pätee erityisesti fyysiseen pääsynhallintaan tilanteissa, joissa automaattinen kirjanpito ei ole mahdollista. Manuaaliseen kirjanpitoon perustuvan pääsynhallinnan valvonnan voi järjestää esimerkiksi siten, että kirjanpito katselmoidaan säännöllisesti tai kun havaitaan poikkeama.

Todennus

1. Valvova viranomainen todentaa, että toimija on valvonut järjestelmien ja laitteiden pääsyä ja käyttöä. Toimija on voinut toteuttaa tämän esimerkiksi keräämällä pääsynhallinnan tapahtumista syntyvää lokia ja säilyttämällä sitä tarpeeksi pitkään. Toimijalla on käytännöt pääsynhallinnan tapahtumien läpikäyntiin. Toimija voi käydä tapahtumakirjauksia läpi esimerkiksi satunnaisesti, sovituin aikavälein tai kun on syytä epäillä poikkeamaa.
2. Jos toimija valvoo järjestelmien ja laitteiden pääsyä ja käyttöä kerryttämällä lokia, todentaa valvova viranomainen, että pääsynhallintaan liittyvät tapahtumat tosiasiallisesti tuottavat lokia. Lokista tulisi käydä ilmi vähintään käytön kohde, lähde, kellonaika, käyttäjä, sekä mahdollisesti muita pääsynhallintaan liittyviä seikkoja, kuten käytetyn monivaiheisen tunnistautumisen tyyppi. Lisäksi sen tulisi vastata toimijan mahdollisia pääsynhallinnan dokumentteja. Valvova viranomainen voi pyytää toimijaa osoittamaan haluamansa kohdat lokista, tai pyytää toimijaa toimittamaan lokin tai sen osia turvallisuus huomioiden.

Perustelut

Pääsynhallinnan valvonta on hyväksi tunnettu tapa havaita käyttäjätunnuksien oikeudetonta käyttöä ja esimerkiksi murtoyrityksiä sekä väärinkäyttöä. Valvonnan mahdollistamiseksi tapahtumakirjausten tuottaminen on useimmiten välttämätöntä.

Viitteet
IEC 62443-2-1:2013 (4.3.3.6.4)
ISO/IEC 27002:2022 (5.15, 8.15)
NIST CSF 1.1 (PR.PT-1, PR.AC-7)
NIST CSF 2.0 (PR.PS-04, PR.AA-03)
Kyberturvallisuuskeskus: Näin kerää ja käytät lokitietoja[8]
NIS CG Reference document (3.7.2 Management of access rights)
NIS CG Reference document (3.11.2 Monitoring and logging)
Työkalut
Julkri (HAL-07, TEK-12)
Kybermittari (SITUATION-1, SITUATION-2)

7.3.1 Pääsynhallinnan tapahtumakirjausten valvonta - laajennettu ohjeistus

Toteutusesimerkki
Tämä suositus on suunnattu sellaisten toimijoiden valvontaan, joiden kohdalla valvova viranomainen odottaa korkeampaa kypsyystasoa. • Toimija on valvonut tapahtumakirjauksen perusteella esimerkiksi epänormaaleja kirjautumisyrityksiä ja muita riskienhallintaan perustuvia tapahtumia. • Valvonta on toteutettu esimerkiksi automaattisia hälytyksiä tuottavalla järjestelmällä, trendejä seuraamalla, manuaalisilla menettelyillä ja lisäksi ilmoituskanavia hyödyntäen. • Tapahtumakirjaukset on tarvittaessa siirretty esimerkiksi SIEM- (Security Information and Event Management) tai muuhun keskitettyyn lokienhallintajärjestelmään, johon voidaan myös kerätä muiden järjestelmien tapahtumiin liittyvää lokitietoa.
Todennus
1. Valvova viranomainen todentaa toimijan dokumentaation pääsynhallinnan tapahtumakirjausten valvonnasta. Dokumentaation tulisi määritellä, miten ja mitä tietoja lokista valvotaan. Siinä on määritelty myös valvonnassa tehtyjen havaintojen jatkokäsittelytoimenpiteet, esimerkiksi automaattisten hälytysten viestintäkanavat ja niiden seuraaminen tai ylläpitäjän lokista havaitseman poikkeaman jatkokäsittelyn. 2. Valvova viranomainen todentaa, että valvonta on tuottanut tapahtumia ja ne on käsitelty asianmukaisesti. Lokin valvonnasta syntyneet tapahtumat tulisi olla säilytetty ja niiden käsittelyhistorian tulisi olla selkeä.
Perustelut

[8] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

Jatkuvan valvonnan mahdollistama viivytyksetön reagointi voi estää laajemmat vahingot.
Viitteet
IEC 62443-2-1:2013 (4.3.3.6.4, 4.3.3.6.7) ISO/IEC 27002:2022 (8.16) NIST CSF 1.1 (PR.PT-1, PR.AC-7) NIST CSF 2.0 (PR.PS-04, PR.AA-03) Kyberturvallisuuskeskus: Näin keräät ja käytät lokitietoja9 NIS CG Reference document (3.11.2 Monitoring and logging)
Työkalut
Julkri (HAL-07, TEK-12, TEK-13) Kybermittari (SITUATION-1, SITUATION-2, SITUATION-3)

7.4 Pääsynhallintaan liittyvä kirjanpito ja vähimpien oikeuksien periaate

Toteutusesimerkki
• Toimijalla on olemassa kirjanpito tai vastaava menettely, jolla käyttöoikeudet ja käyttöoikeusroolit kirjataan. Tämän kirjanpidon ajantasaisuuden ylläpitoon on olemassa menettely. • Kirjanpidon perusteella käyttäjälle on annettu vain ne käyttöoikeudet, jotka ovat välttämättömiä työtehtävien suorittamista varten (vähimpien oikeuksien periaate). Käyttäjään perustuvia valtuutuksia on pyritty mahdollisuuksien mukaan välttämään ja niiden sijaan on käytetty roolipohjaista käyttöoikeuksien hallintaa.
Todennus
1. Valvova viranomainen todentaa toimijan dokumentaation pääsynhallintaan liittyvän kirjanpidon menettelyistä. Dokumentaatiosta käy ilmi, miten käyttöoikeudet ja -roolit kirjataan. Toimijan pääsynhallintaan liittyvästä kirjanpidosta käy ilmi järjestelmien käyttöoikeudet ja käyttöoikeusroolit. Tämä kirjanpito voi olla joidenkin järjestelmien kohdalla manuaalista kirjanpitoa, mutta se voi olla myös automaattista ja esimerkiksi käyttäjäryhmiin perustuvan roolipohjaisen käyttöoikeuksien hallinnan järjestelmätason kirjanpitoa. 2. Valvova viranomainen todentaa toimijan järjestelmän käyttöoikeuksia ja niiden vastaavuutta kirjanpitoon. Tämä voidaan tehdä esimerkiksi käyttäjistä satunnaisotannalla tai tiettyjä käyttöoikeuksia, kuten järjestelmän pääkäyttäjä- tai muita korotettuja oikeuksia tarkastellen. Käyttöoikeuksien tulisi vastata niistä pidettyä kirjanpitoa. Mikäli järjestelmässä hyödynnetään esimerkiksi rooli- tai käyttäjäryhmäpohjaista käyttöoikeuksien hallintaa, ei näiden

[9] https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

lisäksi tulisi olla myönnetty etenkään dokumentoimattomia käyttäjään perustuvia käyttöoikeuksia.

Perustelut

Ylimääräiset käyttäjätunnukset ja pääsyoikeudet voivat mahdollistaa hyökkääjän pääsyn järjestelmään. Hyökkääjä voi hyödyntää dokumentoimattomia tai unohdettuja pääsyoikeuksia liikkuessaan järjestelmässä tai järjestelmästä toiseen. Liian laajasti myönnetyt pääsyoikeudet saattavat mahdollistaa myös muut epätoivotut tiedon paljastumiset.

Viitteet

IEC 62443-2-1:2013 (4.3.3.7)

ISO/IEC 27002:2022 (5.15, 5.18)

NIST CSF 1.1 (PR.AC-4)

NIST CSF 2.0 (PR.AA-05)

NIS CG Reference document (3.7.2 Management of access rights)

NIS CG Reference document (3.7.3 Privileged and administration accounts)

Työkalut

Julkri (HAL-14, TEK-07.2)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3)

7.5 Pääkäyttäjätunnukset

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.7.

- Toimijalla on olemassa menettely, jolla korotettuja oikeuksia tai pääkäyttäjäoikeuksia annetaan vain valtuutetuille henkilöille, laitteille tai sovelluksille. Oikeuksia on myönnetty mahdollisimman pienelle, mutta varajärjestelyt mahdollistavalle, käyttäjäjoukolle. Lisäksi oikeuksia on annettu vain siksi ajaksi, kun ne ovat välttämättömiä työtehtävien hoitamiseen. Tämä koskee myös esimerkiksi kolmannen osapuolen suorittamia ylläpitotöitä.
- Korotettuja oikeuksia ja pääkäyttäjäoikeuksia on suojattu vahvoin menetelmin. Tämä voi tarkoittaa esimerkiksi vahvempia todennusmenetelmiä, useampia todennusmenetelmiä tai todennusmenetelmien riittävän hyvää suojausta.
- Tarpeiden muuttuessa ylimääräiset oikeudet on ensisijaisesti poistettu.
- Korotettujen oikeuksien ja pääkäyttäjäoikeuksien käyttöä on valvottu mahdollisuuksien mukaan. Tämä voi tarkoittaa esimerkiksi sitä, että korotetuilla oikeuksilla tehdyt toiminteet kerryttävät valvontalokia tai toiminteiden suorittamiseen vaaditaan useampi henkilö (two-man rule).
- Toimija on voinut laatia ohjeen korotettujen oikeuksien ja pääkäyttäjätunnusten käytöstä. Korotettujen oikeuksien tunnuksia ja pääkäyttäjätunnuksia ei tule käyttää perustoimintoihin eikä peruskäyttäjätunnuksia tule käyttää

korotettujen oikeuksien toimintoihin tai pääkäyttäjätoimintoihin. Hätätunnuksia ei käytetä muuten kuin perustellusta syystä hätätilanteissa. Hätätunnusten osalta on myös varmistettu, että ne ovat hätätilanteessa saatavilla, mutta riittävästi suojattuna.

Todennus

1. Valvova viranomainen todentaa toimijan dokumentaation pääkäyttäjätunnuksien käyttöön ja ylläpitoon liittyvistä menettelyistä. Dokumentaatiosta käy ilmi koko korotettujen oikeuksien tai pääkäyttäjäoikeuksien hallinnan elinkaari. Dokumentaation tulisi ottaa kantaa oikeuksien myöntämiseen, epäämiseen, niiden valvontaan, niiden liittämiseen käyttäjätunnuksiin tai käyttäjäryhmiin sekä niihin liittyvät erityiskäytännöt, kuten niiden erottelun normaaleista käyttäjätunnuksista. Valvova viranomainen todentaa, että toimijalla on menettelyt valvoa pääkäyttäjäoikeuksien käyttöä ja että pääkäyttäjätunnuksia suojataan vahvoin menetelmin.
2. Valvova viranomainen todentaa katselmoimalla toimijan korotetut oikeudet ja pääkäyttäjäoikeudet ja näihin liitetyt käyttäjätunnukset tai käyttäjäryhmät. Oikeuksien elinkaarta tulisi tarkastella ja varmistua siitä, että korotettuja oikeuksia tai pääkäyttäjäoikeuksia on vain henkilöillä, joilla on niiden käyttöön asiallinen työtehtäviin perustuva tarve. Valvova viranomainen voi katselmoida valvontajärjestelmää tai valvontaprosessin toteutusta, esimerkiksi tutkimalla valvontajärjestelmän tilaa tai haastattelemalla ja katselmoimalla valvontaprosessin toteutumista.

   Valvova viranomainen todentaa järjestelmästä tai kuvakaappauksista, että pääkäyttäjätunnusten osalta käytetään vahvoja menetelmiä (esim. MFA). Hätätunnusten osalta tarkistetaan, että ne ovat hätätilanteessa saatavilla, mutta riittävästi suojattuna. Katselmoinnin yhteydessä voi varmistaa, ettei hätätunnuksia ole käytetty muuten kuin perustellusta syystä hätätilanteissa.

Perustelut

Korotetuilla oikeuksilla sekä pääkäyttäjäoikeuksilla on mahdollisuus tehdä merkittäviä muutoksia järjestelmiin. Niiden väärinkäyttö voi aiheuttaa vakavia tietovuotoja, jatkuvuuden häiriöitä, rahallisia menetyksiä tai muita liiketoiminnan häiriöitä. Niitä tulee suojata erityisen hyvin. Tämän vuoksi pääkäyttäjätunnukset tulee suojata vahvoilla menetelmillä.

Viitteet

IEC 62443-2-1:2013 (4.3.3.6.3, 4.3.3.6.4)

ISO/IEC 27002:2022 (5.15, 5.18, 8.2)

NIST CSF 1.1 (PR.AC-4)

NIST CSF 2.0 (PR.AA-05)

NIS CG Reference document (3.7.3 Privileged and administration accounts)

NIS CG Reference document (3.7.4 Administration systems)

Työkalut

Julkri (TEK-04, TEK-07, HAL-14)

Kybermittari (ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4)

7.6 Turvallisten todennusmenetelmien valinta ja luotettava todennus

Toteutusesimerkki

- Toimija on käyttänyt vain sellaisia todennusmenetelmiä, jotka ovat riittävän turvallisia kohteenturvallisuustarpeet huomioon ottaen.
- Toimija on käyttänyt monivaiheista todennusta oman riskiarvion ja järjestelmän kyvykkyyksien mukaan. Toimija on käyttänyt todennusmenetelmänä esimerkiksi monivaiheista todentamista (MFA), jatkuvaa todentamista, vahvaa tunnistautumista (mobiilivarmenne, pankkitunnukset, kansalaisvarmenne) tai vastaavia, mikäli niiden käyttö on ollut mahdollista.
- Toimija on huolehtinut siitä, että todennusmenetelmiin liittyvät luottamukselliset tiedot, kuten salasanat, pysyvät salassa. Tyypillisesti esimerkiksi salasanat tulee vaihtaa ensimmäisen kirjautumisen yhteydessä. Tunnuksia luodessa ja toimitettaessa käyttäjä tulee tunnistaa luotettavasti. Salasanoja luotaessa on vältetty esimerkiksi heikkoja tai ennalta-arvattavia salasanoja. Poikkeuksena voivat olla tilanteet, joissa heikon tai ennalta-arvattavan salasanan lyhytaikainen käyttö on perusteltua, kuten uuden työntekijän ensikirjautumisessa tai salasanaa nollatessa. Kohdassa 3.3 Järjestelmäkovennukset on tarkennettua tietoa salasanojen suojaamisesta.
- Mikäli mahdollista, käyttäjät on tunnistettu yksilöllisesti ja esimerkiksi yhteiskäyttöisten tunnusten käyttöä on vältetty. Jos toimija ei voi välttyä yhteiskäyttöisten tunnuksien käytöltä, niiden todennusmenetelmät tulisi olla riittävän turvallisia.
- Todennusmenetelmien käytöstä on pidetty lokia riittävällä tasolla ja siinä havaittuihin poikkeamiin, kuten väsytyshyökkäyksiin, on reagoitu esimerkiksi hidastamalla kohteena olevan käyttäjätilin kirjautumista. Lokikäytännöistä on tarkempaa tietoa suosituksen kohdissa 7.4 Pääsynhallinnan tapahtumakirjaus ja 9.3 Tapahtumien kirjaaminen ja havainnointi.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on dokumentaatio järjestelmiensä todennusmenetelmistä. Nämä kattavat esimerkiksi salasanakäytännöt, järjestelmäkohtaiset erityismäärittelyt ja todennusmenetelmien salaisuuksiin, kuten salasanoihin ja niiden jakeluun liittyvät käytännöt. Valvova viranomainen katselmoi dokumenteista toimijan menettelyt luotettavan todennuksen käyttöön (esim. MFA).
2. Valvova viranomainen todentaa kuvaruutukaappauksista tai katselmoimalla järjestelmästä, että toimijalla on käytössä dokumentoidut todennusmenetelmät. Todennusmenetelmät ovat kattavasti käytössä eri järjestelmissä ja määritelty eri käyttäjäryhmille. Lisäksi kuvaruutukaappauksista tai järjestelmän katselmoinnista käy ilmi luotettavan todennuksen käyttö ja valittu todennusmenetelmä.

Perustelut

Tunnuksiin ja todennusmenetelmiin kohdistuu erityisesti niiden julkiseen viestintäverkkoon auki olevaan osuuteen huomattavan paljon murtoyrityksiä, jonka vuoksi niiden turvallisuus on tärkeää. Myös sisäisessä viestintäverkossa olevien järjestelmien todennusmenetelmät tulee valita huolella eikä niihin tule jättää oletusarvoisia tunnuksia tai salasanoja. Luotettavat todennusmenetelmät lisäävät

niitä käyttävien järjestelmien turvallisuutta suojaamalla niitä erityisesti kalastelulta.
Viitteet
IEC 62443-2-1:2013 (4.3.3.6.1, 4.3.3.6.3) ISO/IEC 27002:2022 (8.5) NIST CSF 1.1 (PR.AC-7) NIST CSF 2.0 (PR.AA-03) NIS CG Reference document (3.7.5 Identification) NIS CG Reference document (3.7.6 Authentication) NIS CG Reference document (3.7.7 Multi-factor authentication)
Työkalut
Julkri (TEK-04, TEK-08) Kybermittari (ACCESS-1, SITUATION-1)

8 Salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan h alakohtaan ja osittaiseen j alakohtaan. Näiden alakohtien kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 8 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 8 kohdassa.

1. **Kryptografian toimintaperiaatteet ja menettelyt**: Toimijan olisi luotava kryptografian käyttöön liittyvät toimintaperiaatteet ja menettelyt, joilla suojataan tarvittaessa tiedon luottamuksellisuutta, aitoutta ja eheyttä. (Ks. kohta 8.1).

2. **Tiedon salaustekniikat**: Tiedon salaaminen voi olla tarpeen esimerkiksi silloin, jos sitä siirretään avoimessa tietoverkossa tai säilötään ilman riittävää fyysistä suojaa. Tällöin on valittava salaustekniikka, joka on suojaukseltaan riittävä salattavan tiedon laatuun, salausluokitukseen, suojausaikaan ja suorituskykyvaatimuksiin nähden. Salaustekniikan osalta olisi huomioitava algoritmien, käyttötapojen ja avainvahvuuksien lisäksi myös avaimen saatavuus sekä turvallinen säilytys, luonti ja hallinta. (Ks. kohta 8.2).

3. **Salauksen elinkaari**: Käytetyn salausmenetelmän vaatimusten tulisi olla ajantasaisia koko järjestelmän elinkaaren ajan, jolloin esimerkiksi salausalgoritmin tulisi olla vaihdettavissa (kryptoketteryys). (Ks. kohta 8.3).

8.1 Kryptografian toimintaperiaatteet ja menettelyt

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.8.

- Toimija on tunnistanut osana riskienhallintaa tiedot, jotka vaativat kryptografista suojaa.
- Toimija on määritellyt kryptografiaan liittyvät toimintaperiaatteet, kuten käytettävät salaustuotteet tietoa siirrettäessä ja säilytettäessä.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on tunnistanut ja luokitellut sellaisen omaisuuden, jota suojataan kryptografisin menetelmin luottamuksellisuuden (esim. salaus), aitouden (esim. allekirjoitus) ja eheyden (esim. tiiviste) varmistamiseksi. Dokumentaatio kuvaa myös kryptografiaan liittyvät toimintaperiaatteet, mikä voi tarkoittaa esimerkiksi sallittujen salaustuotteiden määrittämistä ja niihin liittyviä mahdollisia konfiguraatioita.

Perustelut

Tiedon salauksella voidaan estää tiedon päätymisen oikeudettomalle henkilölle luettavassa muodossa. Nykyisin tiedon salaaminen on useissa järjestelmissä kohtuullisen helppoa. Esimerkiksi web-liikenteen salaus on nykyään tavallinen toimenpide. Samaten useimmat käyttöjärjestelmät tarjoavat levyjen salausta vain muutamalla klikkauksella. Kryptografisilla menetelmillä voidaan varmistaa myös, ettei tieto ole tahattomasti tai tahallisesti muuttunut ja että tieto on peräisin oikeasta lähteestä. Näillä keinoilla voidaan yrittää estää esimerkiksi haitallisen materiaalin päätyminen tietojärjestelmiin tai varmistaa, ettei säilötty tieto ole korruptoitunut.

Viitteet

IEC 62443-2-1:2013 (SR 4.3)

ISO/IEC 27002:2022 (5.31, 8.24)

NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06)

NIS CG Reference document (3.10.1 Policies and procedures on cryptography)

Työkalut

Julkri (TEK-16)

Kybermittari (ARCHITECTURE-5)

8.2 Tiedon salaustekniikat

Toteutusesimerkki

- Toimijan kryptografiaa koskevat menettelyt määrittelevät käytettävät protokollat sekä esimerkiksi salausalgoritmit, salausvahvuudet ja salaustuotteet.

- Kryptografiaa koskevat menettelyt ja toimintatavat on suhteutettu tiedon suojaamisen tarpeisiin, kuten luokitukseen ja säilytysaikaan sekä suorituskykyvaatimuksiin.
- Toimija on määritellyt kryptografisten avainten (mukaan lukien varmenteet ja vastaavat) hallinnan niin, että se tukee salaustarpeita. Huomioon otettavia asioita ovat muun muassa:
- Avainten saatavuudesta huolehtiminen, mikä pitää sisällään muun muassa avainten jakelun ja avainten varmuuskopioinnin
- Avainten elinkaaren hallinta, kuten luonti, vaihto, säilytys, käytöstä poistaminen ja tuhoaminen
- Avainten tekniset ominaisuudet, kuten pituus, oikeudet ja käyttöikä
- Vaarantuneiden avainten poistaminen käytöstä (revokointi) sekä
- Avaimiin liittyvien tapahtumien kirjaaminen.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on määritellyt kryptografiaa koskevat menettelyt ja toimintatavat niin, että ne ovat sopivassa suhteessa tiedon suojaamisen tarpeisiin. Toimija on tunnistanut ne tapaukset, joissa tietoa siirretään tai säilytetään ilman riittäviä suojauksia ja joihin salauksen käyttäminen on tarpeellista. Toimija on valinnut salaustekniikan, joka on suojaukseltaan riittävä salattavan tiedon laatuun, salausluokitukseen, suojausaikaan ja suorituskykyvaatimuksiin nähden. Tarkasteltavia yksityiskohtia ovat salauksen osalta käytetyt algoritmit, joiden tulee olla suojausvaatimuksiin nähden riittävät, salauksen käyttötavat sekä avainten vahvuus. Avainten osalta on niiden pituuden ja esimerkiksi monimutkaisuuden (erityisesti symmetriset avaimet, jaetut avaimet eli PSK, Pre-Shared Key) osalta kiinnitettävä huomiota avainten hallintaan. Avainten hallinnassa huomiotavia asioita ovat esimerkiksi avainten turvallinen säilytys, saatavuus, turvallinen luonti ja elinkaaren hallinta. Luonnin voi todentaa esimerkiksi siten, että avaimet luodaan turvallisessa, yleensä eristetyssä, kohteessa ja siten, että niiden satunnaisuus (entropia) on riittävää. Elinkaaren hallinnassa huomioitavia yksityiskohtia ovat muun muassa avaimen poisto ja uusiminen.
2. Valvova viranomainen todentaa esimerkiksi haastatteluin ja konfiguraatiotarkasteluilla, että määritellyt kryptografisiin menetelmiin liittyvät toimintaperiaatteet toteutuvat. Tämä voidaan toteuttaa esimerkiksi tarkastelemalla salausta käyttäviä palveluita ja näiden salaukseen liittyviä määrittelyitä, kuten algoritmeja, avainten muodostamisen käytäntöjä ja avaimen turvallista säilytystä.
3. Valvova viranomainen todentaa riittävän salauksen käyttöä esimerkiksi skannaamalla salattua liikennettä tuottavia palveluita, järjestelmiä tai ohjelmia. Näillä skannausohjelmistoilla voi tarkastaa esimerkiksi salausalgoritmeja, joilla palvelu suostuu liikennöimään. Käytettyjen algoritmien tulisi olla määritysten mukaisia. Lisäksi voidaan tarkastaa avainten (erityisesti varmenteiden) voimassaoloaika yleisesti tunnettuja hyviä käytäntöjä vasten.

Perustelut

Tiedon salauksen tehokkuus perustuu lähes täysin valittuihin salausalgoritmeihin sekä erityisesti avainten hallintaan. Heikot salaukset ovat helposti murrettavissa. Vaarantuntunut tai heikko avain taas voi tuhota koko salauksen hyödyn. Jos avainta ei ole tuhottu luotettavasti ja se päätyy vääriin käsiin, voidaan sillä

purkaa kaikki sillä salattu liikenne. Yhtä tärkeää on myös salausavaimen saatavuus, jotta salattu tieto on käytettävissä sitä tarvittaessa.
Viitteet
IEC 62443-2-1:2013 (SR 1.8, SR 1.9, SR 3.1, SR 4.1, SR 4.3) ISO/IEC 27002:2022 (8.24) CISA: Quantum-Readiness: Migration to Post-Quantum Cryptography[10] NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.PT-4) NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.IR-01, PR.AA-06) On the State of Crypto-Agility[11] NIS CG Reference document (3.10.1 Policies and procedures on cryptography)
Työkalut
Julkri (TEK-04.2, TEK-05.1, TEK-16) Kybermittari (ARCHITECTURE-5) Skannausohjelmat: Nessus, nmap, sslscan

8.3 Salauksen elinkaari

Toteutusesimerkki
• Toimija on ylläpitänyt valittuja salaustekniikoita niin, että heikoksi osoittautuneet salaustekniikat on vaihdettu tarvittaessa uusiin, vahvempiin vaihtoehtoihin. Tulevaisuudessa tämä tulee näkymään erityisesti PQC-salauksen käyttöönotossa (Post-Quantum Cryptography). • Toimija on toteuttanut salauksiin liittyvät järjestelyt niin, että salauksen ja salausavainten vaihto on mahdollisimman helppoa. Tämä tarkoittaa esimerkiksi palveluiden konfiguraatioiden muuttamista uusiin vahvempiin salaustekniikoihin, varmenteiden elinkaaren hallintaa, avainten käyttämistä palveluissa ja tuotteissa siten, että niiden vaihtaminen on mahdollista kohtalaisella vaivalla.
Todennus
1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on toteuttanut salaus- ja kryptografiset menetelmänsä siten, että esimerkiksi salausalgoritmien ja avainten vaihto on toteutettavissa kohtalaisella vaivalla. Salausalgoritmien ja avainten vaihdon mahdollisuus voi olla myös osana hankintaprosessia, esimerkiksi tuotevalintoihin liittyvissä toimijan määrittämissä vaatimuksissa. 2. Valvova viranomainen todentaa katselmoimalla esimerkiksi konfiguraatioita, että kryptografiset järjestelyt tukevat elinkaaren hallintaa. Tämä tarkoittaa esimerkiksi sitä, että kryptografiaan liittyviä parametrejä ei ole esimerkiksi

[10] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
[11] https://eprint.iacr.org/2023/487

kovakoodattu ohjelmistoihin, vaan ne ovat hallittavissa esimerkiksi konfiguraatiotiedostoilla.
Perustelut
Laskentakapasiteetin kasvaessa ja algoritmien murtuessa salaustapoja päätyy tilaan, jolloin niiden murtaminen saattaa olla jopa triviaalia. Tämän vuoksi salausparametrien muuttaminen tulisi tehdä mahdollisimman helpoksi. Tulevaisuudessa myös kvanttitietokoneiden kehitys saattaa aiheuttaa muutospaineita käytettyihin salauksiin. Tämä tulee huomioida erityisesti sellaisissa järjestelmissä, joilla on pitkä elinkaari tai korkeat turvallisuustarpeet. Varmenteiden elinikä on rajattu. Toisaalta salausavaimet saattavat joskus vahingossa tai tahallisesti vaarantua. Tämän vuoksi myös avainten vaihdon pitäisi olla niin yksinkertaista, ettei salauksen teho heikkene avaimen heikkouden vuoksi.
Viitteet
IEC 62443-2-1:2013 (SR 4.3) ISO/IEC 27002:2022 (8.24) NIST CSF 2.0 (ID.AM-08, PR.PS-06) NIS CG Reference document (3.10.1 Policies and procedures on cryptography)
Työkalut
Julkri (TEK-16) Kybermittari (ARCHITECTURE-5)

9 Poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan b alakohtaan. Tämän alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 9 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 9 kohdassa.

1. **Poikkeamanhallinnan menettelyt**: Poikkeamien käsittelyä varten tulisi olla dokumentoidut menettelyt, roolit ja vastuut poikkeamien ehkäisemistä, havainnoimista, analysointia, hallitsemista ja palautumista sekä raportointia varten. (Ks. kohta 9.1).

2. **Poikkeamien raportointikanavat**: Poikkeamien havainnointia varten toimijalla tulisi olla raportointikanavat sisäisille ja ulkoisille toimijoille. (Ks. kohta 9.2).

3. **Tapahtumien kirjaaminen ja havainnointi**: Toimijalla tulisi olla työkaluja ja prosesseja tapahtumien kirjaamiseen ja havainnointiin. Havainnointi- ja analysointikyvyn kannalta on välttämätöntä, että toimijalla on kerättynä ja käytettävissä riittävät lokitiedot esimerkiksi ylläpidosta, muutoksista, käytöstä ja virheistä. (Ks. kohta 9.3).

4. **Poikkeaman analysointi ja luokittelu**: Toimijan tulisi arvioida tapahtumat sen selvittämiseksi, aiheuttavatko ne poikkeaman. Toimijalla tulisi olla käytännöt, joilla poikkeaman vakavuus ja vaikutukset voitaisiin arvioida ja tarvittaessa luokitella. (Ks. kohta 9.4).

5. **Poikkeaman käsittely**: Poikkeaman käsittelyyn tulisi olla käytännöt niihin reagoimiseen, sekä tarvittaessa poikkeaman rajoittamiseen, selvittämiseen ja vaikutusten poistamiseen. (Ks. kohta 9.5).

6. **Juurisyyanalyysi ja kokemuksista oppiminen**: Poikkeaman jälkeen tulisi arvioida poikkeamaan johtaneet syyt ja oppia kokemuksista, jotta voidaan varautua vastaavaan jatkossa paremmin. (Ks. kohta 9.6).

7. **Merkittävien poikkeamien lisävaatimukset**: Merkittäviin poikkeamiin tulisi olla olemassa menettelyt, vastuut ja viestintäkanavat muiden toimijoiden varoittamiseksi. (Ks. kohta 9.7).

8. **Tiedon jakamisen turvallisuus**: Poikkeamien käsittelyn tulisi sisältää myös menettelyt tiedon jakamiseen niin, ettei se vaaranna toimijaa tai muuta organisaatiota. (Ks. kohta 9.8).

9. **Poikkeamanhallinnan elinkaaren hallinta**: Poikkeamien käsittelyn menettelyjä tulisi ylläpitää ja kehittää koko elinkaaren ajan, ja niitä tulisi päivittää esimerkiksi kokemusten perusteella. (Ks. kohta 9.9).

9.1 Poikkeamanhallinnan menettelyt

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.12.

- Toimijalla on kattavat poikkeamanhallinnan menettelyt, joissa kuvataan poikkeamien käsittelyn toimenpiteet. Toimenpiteitä ovat esimerkiksi poikkeaman ehkäisy, havainnointi, analysointi, käsittely sekä palautuminen. Poikkeamanhallinnan menettelyt voivat tarvittaessa viitata muihin dokumentteihin, jos näissä on kuvattu oleellinen sisältö. Poikkeamien ehkäisy voi viitata esimerkiksi toimijan kyberturvallisuuden riskienhallinnan toimintamalliin ja riskienhallinnan toimenpiteisiin
- Poikkeamanhallinnan menettelyt pitävät sisällään tarvittavat roolit sekä ilmoitus- ja viestintäkanavat. Poikkeamanaikaista viestintää varten on suositeltavaa tehdä viestintäsuunnitelma, jotta tarpeellinen sisäinen ja ulkoinen viestintä on etukäteen määritelty. Lisäksi menettelyt kuvaavat poikkeamien käsittelyyn liittyviä toimenpiteitä, kuten poikkeamien luokittelun (kategorisoinnin), vakaviin häiriötilanteisiin liittyvät toimenpiteet ja raportoinnin. Turvallisuutta koskevista rooleista on lisää kohdassa 6.1 Henkilöstöturvallisuuden menettelyt.
- Poikkeamanhallinnan menettelyt sisältävät riittävän dokumentoinnin, joka kuvailee toiminnan poikkeaman käsittelyn aikana. Tämä voi tarkoittaa esimerkiksi poikkeaman tutkintaan liittyviä toimenpiteitä ja resursseja.
- Erityisesti vakavien poikkeamien jälkeen voi olla hyödyllistä pitää purkutilaisuus poikkeaman käsittelyyn osallistuneiden henkilöiden kesken. Näin tulevaisuudessa vastaavilta poikkeamilta voidaan parhaimmillaan välttyä ja toimintaa poikkeamatilanteessa voidaan parantaa. Tämä toimenpide edistää myös NIS2-poikkeamailmoitukseen liittyvän loppuraportin luomista.
- Toimija voi luoda poikkeamanhallintaa varten esimerkiksi seuraavia ohjeita:

- Poikkeamanhallinnan pelikirjat
- Eskalointiin liittyvät ohjeet ja taulukot
- Kontaktilistat
- Mallipohjat

- Poikkeamanhallinnan menettelyt kuvaavat jatkuvuuden (jatkuvuussuunnitelma, Business Continuity Plan, BCP) ja poikkeamanhallinnan väliset suhteet. Poikkeamanhallinta kuvaa myös palautumiseen liittyvät toimenpiteet. Usein tämä on erillinen dokumentti (palautumissuunnitelma, Disaster Recovery Plan, DRP).
- Poikkeamanhallinnan menettelyt kuvailevat lainsäädännölliset vaatimukset poikkeamanhallinnassa.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimijalla on poikkeamanhallintaan liittyvät menettelyt. Nämä ovat kirjallisena ja sijoitettuna sellaiseen paikkaan, että ne ovat poikkeamatilanteissa saatavilla. Menettelyiden lisäksi toimijalla on roolit ja vastuut poikkeamanhallinnan eri vaiheita varten. Näitä ovat poikkeamien ehkäisy, havainnointi, analysointi, hallitseminen, palautuminen sekä raportointi. Menettelyiden sisältö voi koostua esimerkiksi seuraavista kohdassa 1 Riskienhallinnan toimintaperiaatteet, 9 Poikkeamien havainnointi ja käsittely ja osittain kohdassa 10 Varmuuskopiointi, palautumissuunnittelu kuvatuista asioista:
   - Poikkeamien ehkäisy. Poikkeamien ehkäisy voi viitata esimerkiksi toimijan kyberturvallisuuden riskienhallinnan toimintamalliin ja riskienhallintatoimenpiteisiin (ks. 1).
   - Poikkeamien havainnointi. Poikkeamien havainnoinnin menettelyt kuvaavat keinot, joilla poikkeamia havaitaan. Nämä voivat olla esimerkiksi havainnointijärjestelmiä tai viestintäkanavia (ks. 9.3).
   - Poikkeamien analysointi. Poikkeamien analysointia varten on hyvä olla luokittelukriteerit, jotka perustuvat esimerkiksi välittömiin ja välillisiin vaikutuksiin, laajuuteen, aikaan ja resursseihin. Tarvittaessa analysointi voi kuvata myös teknisempiä menettelyjä (ks. 9.4).
   - Poikkeamien hallitseminen ja palautuminen. Näissä voi hyödyntää tarvittavia tarkentavia dokumentteja tai osioita, kuten viestintäsuunnitelman sekä jatkuvuuteen ja toipumiseen liittyvät kytkökset (BCP, DRP) (ks. 10.1).
   - Poikkeamien raportointikanavat (ks. 9.2).
   - Sisäiset roolit ja vastuut. Poikkeamanhallinnan aikaiset roolit, jotka pitävät sisällään esimerkiksi sisäisen ja ulkoisen viestinnän (ks. 2.2, 9.7), poikkeaman selvittämiseen tarvittavat henkilöresurssit ja johdon. Tämä on voitu toteuttaa esimerkiksi sovitulla prosessilla luotavalla (kriisi)ryhmällä.
   - Menettelyissä on lisäksi hyvä kuvata lainsäädännölliset vaatimukset. Näitä ovat esimerkiksi NIS-ilmoitukset ja tietosuojaloukkauksiin liittyvät ilmoitusvelvollisuudet ja näistä seuraavat menettelyt.
2. Lisäksi valvova viranomainen voi tapahtumakirjauksia, tikettejä, haastatteluja ja vastaavia lähteitä käyttäen todentaa, että menettelyjä noudatetaan.

Perustelut

Poikkeamanhallinnan menettelyt ovat olennainen osa varautumista. Hyvin suunniteltu toiminta poikkeaman aikana voi nopeuttaa ja sujuvoittaa poikkeaman

käsittelyä sekä toisaalta auttaa poikkeamien luokittelussa, jolloin reagoinnista saadaan oikeasuhteista.

Viestintäsuunnitelma osana rooleja on useissa poikkeamatilanteissa keskeinen työkalu. Se varmistaa tiedonkulun oikeille henkilöille ja toisaalta voi estää tilannetta pahentavan ylimääräisen viestinnän, esimerkiksi useat raportit samasta poikkeamasta.

Viitteet

IEC 62443-2-1:2013 (4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4)

ISO/IEC 27002:2022 (5.24, 5.30)

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

NIST CSF 1.1 (RS.RP-1, RS.CO-1, RS.IM-2)

NIST CSF 2.0 (RS.MA-01, PR.AT-01, IM.DE-03)

NIST SP 800-61 Rev. 2

NIS CG Reference document (3.11.1 Incident handling policy)

Työkalut

Julkri (HAL-08)

Kybermittari (RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-4, RESPONSE-5)

9.2 Poikkeamien raportointikanavat

Toteutusesimerkki

- Toimijalla on raportointikanava, jonne henkilöstö, toimittajat, haavoittuvuustutkijat, viranomaiset ja asiakkaat voivat raportoida poikkeamista, epäillyistä poikkeamista, haavoittuvuuksista ja muista vastaavista havainnoista.
- Toimija huolehtii siitä, että henkilöstö on tietoinen raportointikanavasta. Lisäksi raportointikanavat kerrotaan ulkoisille toimijoille.
- Raportointikanava on tarpeen mukaan luottamuksellinen. Raportteja käsittelevät henkilöt ovat tietoisia raporttien käsittelykäytännöistä. Tämä pätee erityisesti silloin, kun ne sisältävät esimerkiksi henkilötietoja tai muuta tietoa, jonka käsittelyyn liittyy lakisääteisiä velvoitteita.
- Raportointikanavia määriteltäessä on hyvä ottaa huomioon myös sellaiset tilanteet, joissa normaalit raportointikanavat saattavat poikkeaman takia olla vaarantuneita. Tärkeintä on tunnistaa tällaisen mahdollisuus ja luoda varasuunnitelma tai vaihtoehtoiset, riippumattomat kanavat tällaisia tilanteita varten.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on olemassa raportointikanavat, jotka ovat esimerkiksi henkilöstön, toimittajien, haavoittuvuustutkijoiden,

viranomaisten ja asiakkaiden saatavilla. Raportointikanavat on toteutettu siten, että niiden löytäminen onnistuu tarpeeseen nähden helposti ja niiden käyttäminen on tarvittaessa esteetöntä. Raportointikanavien tulee ottaa huomioon tilanteet, joissa raportointikanava on vaarantunut. Esimerkiksi sähköpostia ei voi käyttää silloin, kun sähköpostipalvelu on mahdollisesti hyökkääjän hallinnassa (ks. 10.4).

2. Raportointikanavien toimivuuden voi tarvittaessa testata esimerkiksi siten, että toimija tekee esimerkkiraportin kanavia pitkin ja valvova viranomainen seuraa raportin käsittelyä.

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5)

ISO/IEC 27002:2022 (6.8)

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

NIST CSF 1.1 (RS.CO-1, RS.CO-2)

NIST CSF 2.0 (PR.AT-01, RS.CO-02)

NIST SP 800-61 Rev. 2

NIS CG Reference document (3.11.3 Event reporting)

Työkalut

Kybermittari (RESPONSE-1, WORKFORCE-2)

9.3 Tapahtumien kirjaaminen ja havainnointi

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.13.

- Toimijalla on prosesseja ja työkaluja poikkeamien havainnointiin. Lisäksi toimijalla on kyky havainnoida turvallisuuteen vaikuttavia tapahtumia ja käsitellä ne kriittisyyden mukaan.
- Toimija on kerännyt lokia riittävällä laajuudella ja tarkkuudella viestintäverkostaan ja tietojärjestelmästään. Kattavan havainnointikyvyn aikaansaamiseksi lokitietoa on mahdollisuuksien mukaan kerätty esimerkiksi seuraavista tapahtumista:
  - Ulos- ja sisäänpäin kulkeva verkkoliikenne
  - Käyttäjien luonti, muutos ja tuhoaminen sekä käyttöoikeuksien lisääminen
  - Järjestelmien ja sovellusten pääsynhallintaan liittyvät tapahtumat

- Pääkäyttäjätoimenpiteet tai korotetuilla oikeuksilla tehdyt toimenpiteet järjestelmissä, palveluissa ja ohjelmistoissa
- Toiminnan tai turvallisuuden kannalta keskeisten konfiguraatioiden ja varmuuskopiotiedostojen käsittely, mukaan lukien luku, muutokset ja tuhoaminen
- Turvallisuuteen liittyvien järjestelmien ja sovellusten tuottama loki (esim. endpoint detection and response EDR, tunkeilijan havaitsemisjärjestelmä/intrusion detection system IDS, palomuuri, etäyhteyspisteet)
- Järjestelmän resurssien käyttö ja suorituskyky
- Tarvittaessa fyysiseen pääsyyn tai käyttöön liittyvät toiminnot (esim. kulunvalvonta)
- Verkko- ja viestintälaitteiden pääsy ja käyttö
- Tarvittaessa ympäristöön liittyvät tapahtumat (esim. olosuhdehälytykset)
- Lokilähdettä ja sen turvallisuutta koskeva muutos, kuten käynnistys, sammutus ja keskeytys

- Lokeista on kyetty havaitsemaan normaalista poikkeavia tai ei-toivottuja tapahtumia. Valvonta on mahdollisimman automaattista, kuitenkin riskienhallinnallinen tarve ja resurssit huomioiden. Havainnoista luodaan hälytyksiä automaattisesti, jos mahdollista. Analytiikasta voi myös seurata trendejä. Tarvittaessa automatiikkaa voidaan korvata esimerkiksi säännöllisillä käytännöillä. Hälytysten käsittelyä varten on prosessi ja resurssit. Tarvittaessa toimija on voinut hyödyntää verkonvalvontakeskuksen (network operations center, NOC) tai turvallisuusvalvomon (security operations center, SOC) tyyppisiä ratkaisuja.
- Lokitietoa on säilytetty riittävän kauan ja ne on mahdollisuuksien ja tarpeen mukaan varmuuskopioitu. Säilytysaika voi riippua esimerkiksi lainsäädännöllisistä, rikosoikeudellisista tai riskienhallintaan perustuvista tarpeista. Esimerkiksi 6 kuukautta voi olla riittävää riskienhallinnan osalta vähemmän kriittiselle lokitiedolle, kun taas esimerkiksi rikosoikeudellinen tarve voi edellyttää useiden vuosien säilytysaikaa.
- Ensisijaisesti lokitiedot tulee viedä erilliselle laitteelle, joka on eristetty muusta järjestelmästä. Lisäksi toimija on toteuttanut tehtävien erottelua niin, että lokipalvelimelle pääsevä henkilö ei pääse käsiksi lokilähteisiin (ja toisinpäin). Tällaisilla toimenpiteillä on useimmiten mahdollista välttää todisteiden tuhoaminen väärinkäytöstapauksissa. Jos tehtävien eriyttäminen ei ole esimerkiksi resurssisyistä mahdollista, toimija on toteuttanut riittävät korvaavat toimenpiteet riskin pienentämiseksi.
- Toimijalla on luotettava, keskitetty aikalähde, ja kaikki lokilähteet tulisi konfiguroida siten, että lokien aikaleimat ovat yhdistettävissä.
- Toimija on ylläpitänyt ajantasaista listaa eri lokilähteistä ja näiden lähteiden tilaa sekä valvonnan toimivuutta ja saatavuutta on tarkasteltu säännöllisesti.
- Lokitietojen käsittely ja säilytys ottavat huomioon mahdolliset lainsäädäntöön tai sääntelyyn liittyvät vaatimukset. Lokeille on varattu riittävästi säilytystilaa ja yleensä hälytys, jos säilytystila on täyttymässä.
- Lokitietojen ja havainnoinnin suhteen on otettu huomioon myös fyysiseen turvallisuuteen liittyvät tapahtumat, erityisesti silloin kun fyysinen turvallisuus tuottaa kyberturvallisuusriskien hallintakeinoja.

Todennus

1. Valvova viranomainen todentaa toimijan tapahtumien kirjaamista ja havainnointikykyä hyödyntäen olemassa olevaa dokumentaatiota. Tällaista

dokumentaatiota voi olla esimerkiksi lokipolitiikka, lokilähteiden ja lokisisällön kuvaukset, lokia ja valvontaa koskevat lainsäädännölliset velvoitteet, valvontajärjestelmien kuvaukset, valvontaprosessien kuvaukset sekä lokijärjestelmän kuvaukset. Lisäksi loki- ja valvontajärjestelmistä voidaan pyytää kuvaruutukaappauksia tai otoksia, joista käy ilmi järjestelmän toimivuus ja kattavuus otannan koko huomioiden (ks. Toteutusesimerkit). Lokien pohjalta tehtyjen havaintojen käsittelyä voi todentaa esimerkiksi käsittelyhistoriasta, haastatteluilla sekä valvontanäkymistä.

2. Loki- ja valvontajärjestelmien tila voidaan todentaa tutkimalla eri järjestelmien konfiguraatioita sekä valvontanäkymiä tarvittaessa toimijan avustuksella. Tässä voi käyttää apuna myös haastatteluja. Riippuen viestintäverkkojen ja tietojärjestelmän koosta eri laitteiden, palveluiden ja muiden resurssien lokitietojen muodostamiseen liittyviä konfiguraatioita voidaan käydä läpi joko otantana tai kokonaisuudessaan. Otantaan sisällytetään vähintään viestintäverkon ja tietojärjestelmän ulkoreunoilla sijaitsevat laitteet (esim. palomuuri, etäyhteyspiste, salain), toiminnan ja turvallisuuden kannalta tärkeimmät resurssit sekä muut riskienhallinnasta ja omaisuusluettelosta poimittu kriittisin omaisuus. Lisäksi otantaan tulisi sisällyttää joukko muita kohteita riittävän kattavuuden saavuttamiseksi. Otantaan valittujen lokien osalta todennetaan, että lokeja syntyy kaikista keskeisistä järjestelmistä (ks. edeltä Toteutusesimerkit), niiden sisältö on toimijan tarpeisiin nähden kattavaa, aikaleimat ovat yhteneviä, lokit siirretään lokijärjestelmään sekä että lokia säilytetään riittävän kauan ja sille on varattu riittävästi säilytystilaa. Säilytysajan tulisi olla suhteessa esimerkiksi lainsäädännöllisiin, rikosoikeudellisiin ja riskienhallintaan liittyviin tarpeisiin. Säilytysaika voi vaihdella järjestelmästä toiseen ja voi olla 6 kuukaudesta yli 5 vuoteen. Lokilähteiden toimivuuden havainnointikyvyn voi katselmoida esimerkiksi siten, että tarkastaa tätä varten olevat säännöt valvontajärjestelmästä. Tapahtumakirjaukset, jotka tehdään esimerkiksi manuaalisesti, voi tarkastaa katselmoimalla. Näihin liittyviin katselmointeihin ja poikkeamahavainnointiin voi käyttää haastatteluja ja mahdollisia muita tietoja, kuten poikkeuksiin liittyviä tikettejä.
3. Loki- ja havainnointikyvykkyyttä voidaan testata esimerkiksi seuraamalla tuotettuja hälytyksiä. Tässä voidaan käyttää apuna esimerkiksi toimijan ylläpitohenkilöstöä tai tietoturvatestaajia. Testauksessa voidaan simuloida erilaisia tavallisuudesta poikkeavia tilanteita ja seurata tapahtuman kertymistä lokiin sekä varmistaa, että tapahtumasta tuotetaan hälytys. Simuloitu tapahtuma voi olla esimerkiksi epäonnistunut kirjautumisyritys, ylläpitotunnusten käyttö, luvattoman mutta turvallisen ohjelmiston ajon yritys tai EICAR-testivirustiedoston tuominen järjestelmään. Testitapauksissa on kuitenkin varmistuttava siitä, etteivät ne aiheuta uhkaa järjestelmälle. Mahdolliset ylimääräiset tunnukset, tiedostot ja pääsyoikeudet on siivottava pois testin jälkeen.

Perustelut

Poikkeamien havainnointikyky on tärkeää, jotta mahdolliset kyberuhkat tunnistetaan mahdollisimman varhaisessa vaiheessa. Tapahtumien kirjaaminen mahdollistaa tapahtumien jälkianalyysin, eikä ilman kattavaa lokia ole useimmiten mahdollista selvittää poikkeaman juurisyitä.

Lokijärjestelmät ja valvonta kannattaa pitää erillisenä muusta järjestelmästä, myös henkilöroolien osalta. Nämä järjestelmät tuottavat yleensä todisteita sille, että jotain pahaa on tapahtunut. Tällöin on tärkeää, että kukaan ei pysty tuhoamaan todisteita. Tarvittaessa nämä järjestelmät voivat tuottaa todisteita myös sille, että esimerkiksi ylläpitohenkilöstö ei ole tuottanut poikkeamatilannetta, vaikka epäilys tällaisesta olisi.

On tyypillistä, että poikkeamatilanteita ei usein huomata ajoissa. Erityisesti hyökkääjän ottaman jalansijan huomaamisessa voi mennä huomattavankin kauan aikaa. Tästä syystä havainnointikyky on tärkeää, sen estäessä parhaimmillaan vakavaa poikkeamaa tapahtumasta.
Viitteet
IEC 62443-2-1:2013 (4.3.3.6.4) IEC 62443-3-3:2019 (SR 1.11, SR 1.12, SR 1.13, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 6.1, SR 6.2) ISO/IEC 27002:2022 (5.24, 5.28, 8.15, 8.16, 8.17) ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 NIST CSF 1.1 (DE.CM, RS.AN-1) NIST CSF 2.0 (DE.CM, RS.MA-02) NIST SP 800-61 Rev. 2 Liikenne- ja viestintäviraston ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta (Traficom/376384/03.04.05.01/2022) NIS CG Reference document (3.11.2 Monitoring and logging) NIS CG Reference document (3.11.4 Event assessment and classification) NIS CG Reference document (3.11.5 Incident response)
Työkalut
Julkri (TEK-12) Poikkeamien testaukseen: EICAR-testivirustiedosto https://www.eicar.org

9.4 Poikkeamien analysointi ja luokittelu

Toteutusesimerkki
• Toimija on tunnistanut lokitiedoista turvallisuuteen liittyvät poikkeamat ja analysoinut poikkeamien vaikutuksen ja vakavuuden esimerkiksi kriteeristön perusteella. Poikkeaman vakavuuden arviointi voi perustua esimerkiksi poikkeamasta aiheutuvaan aineelliseen tai aineettomaan vahinkoon sekä taloudellisiin tappioihin, palvelun häiriintymisen laajuuteen, poikkeaman kestoon ja niiden palvelun vastaanottajien lukumäärään, joihin palvelu vaikuttaa. • Toimijalla on tarvittaessa menetelmät lokien analysointiin ja korrelointiin, jolloin poikkeamia saadaan varmemmin havaittua. • Tarvittaessa toimijalla on järjestelmä, joka analysoi ja korreloi lokitietoa automaattisesti ja hyödyntää tästä saatua tietoa esimerkiksi osana uhkien metsästystä (threat hunting, threat intelligence).
Todennus

1. Valvova viranomainen voi todentaa poikkeaman analysoinnin ja luokittelun toteutuksen esimerkiksi poikkeamanhallinnan menettelyjä kuvaavista dokumenteista. Toimija on kuvannut tapahtumien analysointiin liittyvät menettelyt. Toimijalla tulisi olla selkeät kriteerit, joilla tapahtumat tunnistetaan poikkeamaksi, poikkeamat luokitellaan ja arvioidaan, onko kyseessä kyberturvallisuuden riskienhallinnasta annetun lain mukainen merkittävä poikkeama. Tämän luokituksen tulisi olla selkeä ja perustua esimerkiksi lainsäädäntöön ja omaisuudenhallinnasta periytyviin luokituksiin. Luokittelu on tapauskohtaista, mutta poikkeaman vakavuuden arviointi voi perustua esimerkiksi poikkeamasta aiheutuvaan aineelliseen ja aineettomaan vahinkoon sekä taloudellisiin tappioihin, palvelun häiriintymisen laajuuteen, poikkeaman kestoon ja niiden palvelun vastaanottajien lukumäärään, joihin palvelu vaikuttaa. Menettelyiden toteutumista voi todentaa esimerkiksi tiketeistä ja haastatteluilla. Tässä voidaan käyttää havaittuja poikkeamia ja tarkastella niihin liittyneitä toteutuksia.
2. Jos toimijalla on tarve ja kyky tehdä lokitietojen analysointia ja korrelointia automaattisesti, voi valvova viranomainen todentaa tähän liittyvät menettelyt ja toimintatavat esimerkiksi dokumentaatiosta. Lisäksi voidaan katselmoida analysointia ja vertailua suorittavan järjestelmän toimivuus sekä asiantuntijoiden kyky tehdä analyysia. Haastatteluilla ja esimerkiksi tiketöintijärjestelmästä voi todentaa, että analysointia ja vertailua on tehty ja että sillä on ollut tarvittaessa vaikutusta. Tämä voi näkyä esimerkiksi löydöksien aiheuttamista muutoksista, jotka voi todentaa esimerkiksi muutoshallinnan lokista.

Perustelut

Poikkeamien analysoinnin ja luokittelun tarkoitus on, että poikkeaman hallinnan toimenpiteet ovat mahdollisimman oikeasuhtaisia. Tämä tarkoittaa sitä, että esimerkiksi ylimääräisiä resursseja ei käytetä epähuomiossa vaikutukseltaan olemattoman poikkeaman selvittämiseen ja toisaalta että merkittävät poikkeamat tunnistetaan ajoissa vakavien seurausten hallitsemiseksi.

Edistyneemmille hyökkäyksille on usein ominaista, että ensimmäinen jalansija saavutetaan huomattavan paljon aikaisemmin kuin varsinainen vahinko aiheutetaan. Tätä varten joillain toimijoilla voi olla riskiperusteinen tarve analysoida poikkeamia automaattisesti esimerkiksi perustuen korrelointiin.

Viitteet

IEC 62443-2-1:2013 (4.3.4.5.6, 4.3.4.5.7)

ISO/IEC 27002:2022 (5.25)

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

NIST CSF 1.1 (DE.AE-4, RS.AN-2, RS.AN-4)

NIST CSF 2.0 (DE.AE-04, RS.MA-03, RS.MA-04, RS.MA-05)

NIST SP 800-61 Rev. 2

NIS CG Reference document (3.11.4 Event assessment and classification)

Työkalut

Julkri (TEK-13) Kybermittari (SITUATION-1, SITUATION-2, SITUATION-3, SITUATION-4)

9.5 Poikkeaman käsittely

Toteutusesimerkki

- Toimijalla on olemassa kirjalliset menettelyt poikkeamien käsittelyä varten. Nämä menettelyt kattavat:
  - Käytännöt, joilla poikkeamiin reagoidaan.
  - Toimenpiteet, joilla estetään poikkeamasta aiheutuvat vakavammat seuraukset ja poikkeaman leviäminen.
  - Poikkeaman selvittäminen, jolloin selvitetään ja poistetaan poikkeaman vaikutus ja poikkeaman aiheuttaja.
- Poikkeaman selvittämisessä tulee varmistua, että poikkeaman ilmaantuminen tulevaisuudessa estetään.

Todennus

1. Valvova viranomainen todentaa esimerkiksi dokumentaatiosta, että toimijalla on poikkeaman käsittelyyn liittyvät menettelyt. Menettelyt kuvaavat käytännöt, joilla poikkeamiin reagoidaan.

   Poikkeamiin reagoinnin käytäntöjä voivat olla esimerkiksi poikkeamanhallintaan liittyvät toimenpiteet, kuten toimenpiteet, joilla minimoidaan poikkeaman vaikutukset ja estetään poikkeaman leviäminen esimerkiksi muihin toimijoihin ja muihin järjestelmiin. Dokumentaatiosta tulisi käydä ilmi myös toimintatavat, joilla poikkeaman vaikutus ja ilmaantuminen estetään jatkossa. Jotta tämä voidaan saavuttaa, pitäisi dokumentaatiosta ilmetä se, että poikkeamille tehdään kattavaa tutkintaa ja että toimijalla on riittävä osaaminen itsellään tai kolmannelta osapuolelta hankittuna. Edellä oleva tulisi tarkastaa erityisesti sitä vasten, että uudet poikkeamat saattavat johtua siitä, että vanhaa poikkeamaa ei ole aikoinaan selvitetty riittävästi. Poikkeaman vaikutuksen kasvamisen ja leviämisen estämiseksi toimijalla on riittävät tiedot tahoista, joihin poikkeama voi vaikuttaa. Edellä mainittujen tahojen informoinnin on oltava nopeaa, selkeää ja vastuutettua (ks. 9.7). Lisäksi tulee huomioida esimerkiksi lainsäädännöstä tulevat velvoitteet. Nämä ja näihin liittyvät vastuut tulisi olla selkeästi kirjattuna.
2. Valvova viranomainen selvittää menettelyiden toteutumisen, jos tämä on mahdollista. Tähän voidaan käyttää esimerkiksi haastatteluja, poikkeamien käsittelyssä syntynyttä dokumentaatiota, kuten tikettejä ja lokia sekä muutoksia ja viestintää.

Perustelut

Viitteet

IEC 62443-2-1:2013 (4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.4.5.9, 4.3.4.5.10)

ISO/IEC 27002:2022 (5.24, 5.25, 5.26, 5.37) ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 NIST CSF 1.1 (PR.IP-9, RS.RP-1, RS.CO-3, RS.CO-4, RS.AN-3, RS.MI-1, RS.MI-2, RC.RP-1, RC.CO-1, RC.CO-2, RC.CO-3) NIST CSF 2.0 (ID.IM-04, RS.MA-01, RS.MA-04, RS.CO-03, RS.AN-06, RS.MI-01, RS.MI-02, RC.RP-01, RC.CO-03, RC.CO-04) NIST SP 800-61 Rev. 2 NIS CG Reference document (3.11.5 Incident response)
Työkalut
Julkri (HAL-08, TEK-13) Kybermittari (RESPONSE-3)

9.6 Juurisyyanalyysi ja kokemuksista oppiminen

Toteutusesimerkki
• Toimija tekee erityisesti merkittävän poikkeaman jälkeen katselmoinnin poikkeamanhallinnasta. Tämä sisältää esimerkiksi poikkeaman havaitsemiseen, hallintaan ja ratkaisuun liittyvät seikat. • Jos toimija on havainnut poikkeaman käsittelyn aikana puutteita, toimija on parantanut toimintatapojaan, ohjeistuksiaan ja resurssejaan, kuten kyvykkyyksiä tai osaamisia.
Todennus
1. Valvova viranomainen todentaa dokumenteista, että toimijalla on käytännöt juurisyyanalyysin (root cause analysis, RCA) toteuttamiseen ja kokemuksista oppimiseen. Juurisyyanalyysiin ja kokemuksista oppimiseen on hyödynnetty dokumentaatiota. Juurisyyanalyysin toimenpiteiden tulisi olla kuvailtuja ja vastuutettuja. Tarvittava osaaminen ja resurssit tulisi olla saatavilla. Kokemuksesta oppimisen tulisi olla osa poikkeamanhallinnan menettelyiden toimenpiteitä. 2. Valvova viranomainen todentaa toimijan merkittävän poikkeaman sen käsittelyyn liittyvistä materiaaleista ja haastatteluin. Tarkoituksena on selvittää, että toimija on toteuttanut juurisyyanalyysin ja oppinut kokemuksesta. Kokemuksesta oppimisen voi todentaa esimerkiksi katselmoimalla, että toimija on suunnitellut tai toteuttanut korjaavia toimenpiteitä poikkeaman jälkeen.
Perustelut
Juurisyyanalysoinnin ja kokemuksista oppimisen tarkoitus on etsiä käytäntöjä, joilla voidaan ennaltaehkäistä poikkeamien syntymistä ja toimia niissä jatkossa paremmin ja tehokkaammin. Juurisyyanalyysi on sääntelyn vaatimusten apuväline, jotta toimija kykenee tuottamaan NIS-ilmoituksen loppuraportin.

Viitteet
IEC 62443-2-1:2013 (4.3.4.5.8, 4.3.4.5.11) ISO/IEC 27002:2022 (5.27, 5.28) ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 NIST CSF 1.1 (DE.AE-2, RS.IM-1) NIST CSF 2.0 (DE.AE-02, ID.IM-03) NIST SP 800-61 Rev. 2 NIS CG Reference document (3.11.6 Post-incident review)
Työkalut
Kybermittari (RESPONSE-3, RESPONSE-4)

9.7 Merkittävien poikkeamien lisäsuositukset

Toteutusesimerkki
Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.12. • Poikkeamanhallinnan menettelyt käsittävät merkittävien poikkeamien hallinnan. Toimija on määritellyt näiden varalta henkilöstön roolit ja vastuut sekä viestintäkanavat esimerkiksi tarvittaville viranomaisille. • Toimija on määritellyt menettelyt ensi-ilmoituksen ja jatkoilmoituksen tekemiseen merkittävistä poikkeamista NIS-ilmoituslomakkeella sekä loppuraportin toimittamiseen.
Todennus
1. Valvova viranomainen todentaa, että menettelyt merkittävissä poikkeamissa ovat kuvattuina erikseen dokumentaatiossa. Merkittävän poikkeamanhallinnan menettelyt sisältävät tyypillisesti poikkeaman eskaloinnin. Merkittävien poikkeamien arviointiin ja käsittelyyn sekä viestintään ja roolituksiin liittyvät tarpeet tulisi olla selkeästi määriteltynä poikkeamanhallinnan menettelyissä ja tähän liittyvissä dokumenteissa. Merkittävät poikkeamat vaativat usein erilaista viestintää esimerkiksi viranomaisille päin, ja tämä tulisi olla otettuna huomioon. Merkittävissä poikkeamissa tiedon jakamisen turvallisuus (ks. 9.8) ja erityisesti tähän liittyvät hätäviestijärjestelmät (ks. 10.4) tulisi olla ennalta kuvattuna ja määritettynä.
Perustelut
Viitteet

IEC 62443-2-1:2013 (4.3.4.5.3, 4.3.4.5.5) ISO/IEC 27002:2022 (5.26, 5.29, 5.30) ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 NIST CSF 1.1 (ID.GV-2, ID.GV-3, RC.CO-3) NIST CSF 2.0 (GV.RR-02, GV.OC-03, RC.CO-03) NIST SP 800-61 Rev. 2
Työkalut
Julkri (HAL-08, TSU-14) Kybermittari (RESPONSE-2, RESPONSE-3, RESPONSE-5)

9.8 Tiedon jakamisen turvallisuus poikkeamatilanteessa

Toteutusesimerkki
• Toimijan viestintäkanavat kyberturvallisuuspoikkeamien yhteydessä ovat riittävän turvallisia saatavuudeltaan, luottamuksellisuudeltaan ja eheydeltään. • Viestintäkanavien valinnassa tulisi ottaa huomioon tilanne, jossa tavanomaiset viestintäkanavat eivät ole saatavilla. • Mahdollinen vihamieliseen toimintaan liittyvä tieto jaetaan siten, ettei se päädy hyökkääjälle.
Todennus
1. Valvova viranomainen todentaa, että toimijalla on dokumentaatiossaan määriteltynä sellaiset viestintäkanavat, joilla on turvallista viestiä poikkeamatilanteissa. Viestintäkanavien saatavuus on keskeinen turvallisuusominaisuus ja tässä on otettu huomioon erityisesti tilanteet, joissa tavanomaiset palvelut eivät ole saatavilla (ks. 10.4). Lisäksi viestintäkanavien valinnassa tulisi ottaa huomioon se, ettei jaettu tieto vaaranna eri osapuolia. Tämä on voitu toteuttaa esimerkiksi hyödyntämällä salausta ja muuta, vaarantuneesta järjestelmästä erillistä tekniikkaa. Dokumentaatiossa ja suunnitelmissa tulisi myös huomioida tilanteet, joissa poikkeama vaikuttaa viestintäkanavaan ja tuottaa tällöin varasuunnitelma ja varaviestintäkanava (ks. 10.4). Lisäksi on hyvä katselmoida, että toimija ylläpitää ja testaa säännöllisesti viestintäkanaviensa toimivuutta. 2. Valvova viranomainen voi todentaa tiedon jakamisen turvallisuuden myös testaamalla. Toimijaa voidaan esimerkiksi pyytää lähettämään testiviestejä eri viestintäkanavia pitkin. Samalla voidaan todentaa se, että viestien suojaustapoja, kuten salausta, kyetään hyödyntämään.
Perustelut
Poikkeamatilanteissa on pidettävä huoli siitä, että poikkeamaan liittyvää tietoa jaetaan turvallisesti. On ensiarvoisen tärkeää, että tämä on määritelty etukäteen,

koska poikkeamatilanteen aikana resurssitarve kohdistuu muualle kuin tällaisten määrittämiseen.

Tiedon jakamisen turvallisuudessa on huomioitava useita asioita kuten onko hyökkäykseen liittyvä tieto luokiteltua ja sen vuoksi suojattavaa, miten estetään hyökkääjän pääsy tietoon ja miten tiedon jakamisen saatavuus varmistetaan. Tieto on suojattava hyökkääjältä, jotta hyökkääjä ei saa etua siitä, että tämä tuntisi toimijan mahdolliset heikkoudet sekä voisi hyödyntää toimijan tilannetietoa hyökkäyksen selvittämisestä.

Viitteet

IEC 62443-3-3:2019 (SR 4.1 RE 1)

ISO/IEC 27002:2022 (5.24, 5.26, 5.28, 5.29)

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

NIST CSF 1.1 (PR.DS-2, PR.PT-4)

NIST CSF 2.0 (PR.DS-02, PR.AA-06, PR.IR-01)

NIST SP 800-61 Rev. 2

Työkalut

Julkri (TEK-16)

Kybermittari (RESPONSE-3, RESPONSE-5, ARCHITECTURE-5)

9.9 Poikkeamanhallinnan elinkaaren hallinta

Toteutusesimerkki

- Kyberturvallisuuden poikkeamanhallinnan menettelyjä ylläpidetään ja parannetaan säännöllisesti sekä erityisesti merkittävien poikkeamien jälkeen.
- Toimija pitää poikkeamanhallintaan liittyvät roolit, resurssit, poikkeamaluokittelun kriteerit ja muun oleellisen tiedon ajantasaisena.

Todennus

1. Valvova viranomainen todentaa dokumentaatiosta, että toimija on kirjannut menettelyiden säännölliseen kehittämiseen liittyvät toimenpiteet, kuten suunniteltu päivitysaikataulu ja päivityskäytännöt vakavien poikkeamien jälkeen opituista asioista.
2. Valvova viranomainen voi todentaa toteutunutta kehitystä muutoshistoriasta sekä haastatteluin.

Perustelut

Poikkeamanhallinnan menettelyiden säännöllinen ylläpito edistää poikkeamanhallintaa tositilanteessa. Menettelyiden jatkuva kehittäminen on tärkeää. Tosin on luonnollista, että myös poikkeamanhallintaan liittyvät resurssit muuttuvat

jatkuvasti, esimerkiksi henkilöstövaihdosten vuoksi. Poikkeamatilanteissa asioiden päivittämiseen ja selvittämiseen ei ole yleensä aikaa.
Viitteet
IEC 62443-2-1:2013 (4.3.4.5.8) ISO/IEC 27002:2022 (5.24, 5.27) ISO/IEC 27035-1:2023 ISO/IEC 27035-2:2023 NIST CSF 1.1 (PR.IP-7, DE.DP-5, RS.IM-1, RS.IM-2, RC.IM-1, RC.IM-2) NIST CSF 2.0 (ID.IM-03) NIST SP 800-61 Rev. 2 NIS CG Reference document (3.11.1 Incident handling policy)
Työkalut
Julkri (HAL-08) Kybermittari (RESPONSE-3)

10 Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan c alakohtaan ja osittaiseen j alakohtaan. Näiden alakohtien kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 10 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 10 kohdassa.

1. **Jatkuvuus- ja toipumissuunnittelu**: Toimijalla tulisi olla dokumentoidut menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta. Jatkuvuus olisi varmistettava esimerkiksi riskienhallinnan perusteella luodulla jatkuvuussuunnitelmalla sekä toipumissuunnitelmalla. Suunnitelmat voisivat sisältää esimerkiksi olosuhteet, joissa ne aktivoidaan sekä tarvittavia rooleja, resursseja, toimenpiteitä ja viestintäkanavia sekä tarvittavat suojatut varaviestintäjärjestelmät. Suunnitelmien tulisi sisältää myös kriisinhallintamenettelyt erittäin vakavien poikkeamien varalta. Muun riskienhallinnan mukaisesti suunnitelmia tulisi ylläpitää ja kehittää säännöllisesti sekä niiden mukaista toimintaa harjoitella. (Ks. kohta 10.1).

2. **Varmuuskopiot ja varajärjestelmät**: Toimijan olisi määritettävä riskienhallinnan perusteella tarvittavat varmuuskopiot tiedoista ja järjestelmistä sekä varajärjestelmät. Varmuuskopiot olisi säilöttävä riittävän kauan ja niitä olisi otettava tarpeeksi usein, jotta toiminnot voidaan palauttaa riittävän nopeasti ja tarpeisiin nähden riittävän tuoreella tiedolla poikkeama- ja kriisitilanteissa. (Ks. kohta 10.2).

3. **Palautustestaus ja varmuuskopioiden suojaaminen**: Palautuksen toimivuutta tulisi testata säännöllisesti sen toimivuuden varmistamiseksi ja

varmuuskopiot on suojattava niin, että niitä eivät koske samat uhkat kuin varmistettavaa järjestelmää. (Ks. kohta 10.3).

4. **Varaviestintäjärjestelmät**: Tarve suojattujen varaviestintäjärjestelmien käytölle voisi perustua esimerkiksi siihen, että riskiarviossa on todettu välttämättömäksi varmistaa viestintäkanavat myös silloin, kun tavanomaisesti käytössä olevat järjestelmät (esim. puhelin, sähköposti, pikaviestimet) eivät ole käytettävissä. Jos tarvetta on, toimija voisi määrittää esimerkiksi käytettävät varaviestintäjärjestelmät ja niiden tarve sekä tavan käyttöönotolle. (Ks. kohta 10.4).

10.1 Jatkuvuus- ja toipumissuunnittelu

Toteutusesimerkki

- Toimijalla on dokumentaatio, jossa kuvataan menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta. Dokumentaatio pitää sisällään esimerkiksi jatkuvuussuunnitelman (business continuity plan, BCP), toipumissuunnitelman (disaster recovery plan, DRP) ja häiriöiden vaikutusarvioinnin (business impact analysis, BIA), jotka perustuvat riskiarviointiin, toiminnan vaatimuksiin ja lainsäädäntöön (ks. 9.1).
- Jatkuvuus- ja toipumissuunnitelmat sisältävät esimerkiksi kuvauksen tilanteista, joissa suunnitelmien kuvaamat prosessit ja toimenpiteet otetaan käyttöön, viestintäkanavat ja henkilöstöresurssit rooleineen, toipumismenettelyt ja riippuvuudet muihin järjestelmiin (ks. 6.1).
- Jatkuvuus- ja toipumissuunnitelmat kuvaavat myös erittäin vakaviin poikkeamiin (kriiseihin) liittyvät toimenpiteet, viestintäkanavat sekä niiden tunnistamiseen liittyvät määritteet (ks. 9.7).
- Jatkuvuus- ja toipumissuunnitelmia ylläpidetään säännöllisesti ja niiden kuvailemia prosesseja, toimintatapoja ja resursseja kehitetään ja niiden mukaista toimintaa harjoitellaan.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on dokumentoidut menettelyt toiminnan jatkuvuudesta häiriötilanteista palautumisesta. Näitä varten toimijalla on vähintään riskienhallintaan perustuva jatkuvuussuunnitelma sekä toipumissuunnitelma, tai vastaavan sisältöistä dokumentaatiota. Suunnitelmat pitävät sisällään kattavat tiedot, joiden perusteella suunnitelman toimenpiteet käynnistetään. Lisäksi suunnitelmat sisältävät roolit, resurssit, toimenpiteet ja viestintäkanavat, joita käytetään poikkeamanhallinnan aikana. Suunnitelmissa on käsitelty myös vakavat häiriö- ja kriisitilanteet, joissa toimijaan tai toimijan toimintaympäristöön kohdistuu toimintaa vakavasti häiritsevä tilanne. Valvova viranomainen todentaa, että suunnitelmia on ylläpidetty, kehitetty ja harjoiteltu säännöllisesti. Nämä voi todentaa esimerkiksi dokumentaation päivityshistoriasta ja harjoituksiin liittyvistä dokumenteista. Harjoittelu voi kevyimmillään olla jatkuvuuteen ja toipumiseen liittyvien menettelyiden simulointia keskustelemalla (ns. työpöytäharjoitus, tabletop-harjoitus).
2. Valvova viranomainen todentaa esimerkiksi haastatteluilla, että toimijan jatkuvuus- ja toipumissuunnittelun menettelyt on jalkautettu toimintaan. Tämän voi todentaa esimerkiksi siitä, että suunnitelmien resurssit ovat olemassa ja että henkilöt ovat tietoisia tehtävistään suunnitelmien toimeenpanossa. Lisäksi valvova viranomainen voi haastatteluilla selvittää suunnitelmien ylläpitoa ja harjoittelua. Jos toimijalla on ollut poikkeamatilanteita, joissa

suunnitelmia on hyödynnetty, voi valvova viranomainen ulottaa haastattelunsa myös näihin tapahtumiin sekä katselmoida näihin tilanteisiin liittyvää dataa.

3. Valvova viranomainen voi osallistua toimijan jatkuvuus- ja toipumissuunnittelun harjoitukseen esimerkiksi tarkkailijaroolissa, yhteistyössä toimijan kanssa. Harjoituksissa voi halutessaan hyödyntää myös useiden toimijoiden välistä yhteistyötä ja järjestää esimerkiksi kansallisia kyberturvallisuusharjoituksia, joihin osallistuu viranomaiset, toimijat ja muut yhteistyökumppanit.

Perustelut

Jatkuvuus- ja toipumissuunnittelu ovat olennainen osa poikkeaman- ja kriisinhallintaa. Valmiiksi määritellyt toimintatavat, resurssit, olosuhteet ja viestintäkanavat edistävät poikkeamatilanteista toipumista ja toiminnan jatkuvuuden palauttamista.

Suunnitelmien harjoittelu etukäteen nopeuttaa tyypillisesti toipumista huomattavasti ja tekee siitä sujuvampaa. Jo työpöytäharjoitus voi auttaa löytämään ongelmia suunnitelmista ja estää näiden toteutumisen tositilanteessa.

Viitteet

IEC 62443-2-1:2013 (4.3.4.5)

ISO/IEC 27002:2022 (5.30, 5.37)

NIST CSF 1.1 (PR.IP-9-10, ID.BE-5, ID.SC-5, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (ID.IM-02, ID.IM-04, GV.OC-04, GV.SC-08, ID.IM-02, RC.RP-01, ID.IM-03)

NIS CG Reference document (3.12.1 Business continuity and disaster recovery plans)

Työkalut

Julkri (VAR-02, TEK-13, TEK-22.1)

Kybermittari (RESPONSE-3, RESPONSE-4, RESPONSE-5, CRITICAL-3)

Kyberturvallisuuskeskuksen Kyberharjoitusohje12

10.2 Varmuuskopiot ja varajärjestelmät

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Toimija on suunnitellut, toteuttanut, testannut ja kuvannut varmistus- ja palautusprosessit sekä varajärjestelmät. Nämä järjestelmät vastaavat lainsäädännön ja toiminnan vaatimuksia. Varajärjestelmät pitävät sisällään esimerkiksi toimitiloihin, laitteisiin, verkkoyhteyksiin, tietojärjestelmiin,

[12] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

viestintäkanaviin ja henkilöstöön liittyvää varautumiseen pohjautuvaa kykyä ja kapasiteettia.

- Varmuuskopioita on otettu riittävän usein niin, että järjestelmät ja niiden tieto voidaan palauttaa riittävän ajantasaisella tiedolla (recovery point objective, RPO). Lisäksi palautusjärjestelmä tulisi mitoittaa siten, että palautus voidaan tehdä riittävän nopeasti (recovery time objective, RTO).
- Varmuuskopioita on säilytetty turvallisesti ja riittävän kauan liiketoimintatarpeet ja lainsäädäntövaatimukset huomioiden.
- Varmuuskopiot on otettu kaikista tarvittavista tiedoista ja järjestelmistä. Kopioitavissa kohteissa tulisi ottaa huomioon myös esimerkiksi konfiguraatioiden ja pilvipalveluiden varmuuskopiointi.

Todennus

1. Valvova viranomainen todentaa, että toimija on määritellyt ne tiedot ja järjestelmät, joista on otettava varmuuskopiot toiminnan jatkumisen varmistamiseksi. Tässä määrittelyssä on huomioitu myös järjestelmät ja tiedot, joista muut palvelut ovat riippuvaisia ja joiden toimivuus on siksi toiminnan kannalta välttämätöntä. Lisäksi valvova viranomainen todentaa, että toimijalla on tarvittaessa riittävät varajärjestelmät. Varajärjestelmät ovat tarvittaessa kuvattuna esimerkiksi arkkitehtuurikuvauksissa sekä kohdan 10.2 suunnitelmissa. Varajärjestelmillä voidaan tietyissä tapauksissa korvata myös osa varmuuskopioinnista, tapauksesta riippuen. Valvova viranomainen todentaa, että toimija on määrittänyt arvot varmuuskopioiden säilytysajalle sekä varmuuskopioinnin tiheydelle. Valvova viranomainen varmistaa, että arvot ovat linjassa sen kanssa, miten paljon toimija voi menettää dataa poikkeamatilanteessa ja miten nopeasti data on kyettävä palauttamaan. Arvot voivat olla erilaisia eri järjestelmien ja tiedon osalta. Varmuuskopioinnin säilytysajan suhteen otetaan huomioon esimerkiksi lainsäädännölliset velvoitteet sekä erilaiset riskiskenaariot, joissa varmuuskopioita voidaan joutua hakemaan pidemmän ajan takaa esimerkiksi tiedon huomaamattoman korruptoitumisen, poikkeaman pitkän vasteajan tai muun syyn johdosta. Toimija voi olla määritellyt, että varmuuskopioita säilytetään pidemmän aikaa esimerkiksi pienissä määrin, esimerkiksi kerran kuukaudessa viedään täydelliset kopiot (nk. full backup) pidempiaikaiseen säilöön ja muutoin kopioita (esim. incremental) säilytetään esimerkiksi muutamia viikkoja.
2. Valvova viranomainen todentaa esimerkiksi kuvaruutukaappauksista tai katselmoimalla järjestelmiä, että toimija on toteuttanut todennuskohdassa 1 kuvatut varajärjestelmät ja varmuuskopiot. Jos toimijalla on ollut poikkeamatilanteita, voi haastatteluilla ja katselmoimalla tapaukseen liittyvää tapahtumalokia todentaa, että varajärjestelmien ja varmuuskopioinnin toteutukset ovat riittäviä.
3. Valvova viranomainen voi yhdessä toimijan kanssa testata varajärjestelmien ja varmuuskopioiden palautuksen toimivuutta.

Perustelut

Monissa, erityisesti vakavissa, poikkeamatilanteissa varajärjestelmät ja varmuuskopiot ovat hyvin tärkeässä roolissa toiminnan palauttamisessa. Poikkeamatilanteet voivat olla tahattomia tai tahallisia, ja erityisesti tietynlaisissa tilanteissa, kuten kaiken tiedon salaavissa hyökkäyksissä, on varmuuskopioiden olemassaolo erityisen tärkeää.

Lisäksi jotkin järjestelmät ja niiden toimimattomuus voivat aiheuttaa suuriakin ongelmia palautumisessa. Usein nämä ovat myös erityisen haluttuja kohteita

hyökkääjälle. Tällaisia ovat esimerkiksi pääsynhallintaan liittyvät palvelut (esim. Active Directory, AD), ja näiden ripeään palauttamiseen on syytä kiinnittää huomiota.

Viitteet

IEC 62443-2-1:2013 (4.3.4.3.9)

ISO/IEC 27002:2022 (8.13, 8.14)

NIST CSF 1.1 (PR.IP-4)

NIST CSF 2.0 (PR.DS-11)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Työkalut

Julkri (TEK-20, VAR-02, VAR-07, VAR-08)

Kybermittari (RESPONSE-4, ASSET-2, CRITICAL-2)

10.3 Palautustestaus ja varmuuskopioiden suojaaminen

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Varmuuskopioiden palautusta ja varajärjestelmien toimivuutta tulisi testata säännöllisesti, ensisijaisesti automaattisesti. Testauksessa pitäisi tarkastaa myös varmuuskopioiden eheys. Varmuuskopioiden palautustestaus on tehtävä turvallisesti niin, ettei se vaaranna tuotantojärjestelmää.
- Varmuuskopioita on säilytettävä turvallisessa tilassa, joka on toimijan riskienhallinnan perusteella riittävän eriytettynä varmuuskopioitavasta järjestelmästä. Tämä voi tarkoittaa esimerkiksi muuta toimitilaa tai erillistä palotilaa. Varmuuskopioita voi säilyttää tarvittaessa useassa muodossa, joiden palautusnopeuksissa voi olla eroa, kuten levylle otetut varmistukset sekä erilliset pitkäaikaisarkistot.
- Varmuuskopioiden suojaamisessa voidaan ottaa huomioon niiden eheyden, saatavuuden ja luottamuksellisuuden tarpeet. Tämä tarkoittaa esimerkiksi riittävää fyysistä suojausta ja muita kontrolleja, kuten salausta.

Todennus

1. Valvova viranomainen todentaa, että toimija on mahdollisuuksien ja tarpeen mukaan määrittänyt toimenpiteet, joilla varmuuskopioiden ja varajärjestelmien toimivuutta testataan säännöllisesti, esimerkiksi kerran viikossa. Tämä voi olla automatisoitua tai manuaalista. Keskeistä on, että mekaanisen palautuksen lisäksi tarkastetaan myös se, että tieto saadaan palautettua eheänä ja käyttökelpoisena, sekä mahdollinen varajärjestelmä pystytettyä oikealla tiedolla. Valvovan viranomainen todentaa, että varmuuskopiot on suojattu riittävästi. Esimerkiksi arkkitehtuurikuvauksissa, järjestelmädokumentaatiossa tai vastaavassa pitäisi olla kuvattuna se, miten varmuuskopiojärjestelmä tai sen osa on eriytetty muusta järjestelmästä. Tämän pitäisi varmistaa se, että jos

esimerkiksi viestintäverkkoon ja tietojärjestelmään pääsee hyökkääjä, ei tämä voi päästä käsiksi kaikkiin varmistuksiin.

2. Valvova viranomainen todentaa katselmoinneilla ja haastatteluilla, miten toimija testaa varmuuskopioiden toimivuutta mahdollisuuksien ja tarpeen mukaan. Tästä tulisi käydä ilmi esimerkiksi suoritetut toimenpiteet varmuuskopioiden eheyden varmistamiseksi sekä testauksen säännöllisyys. Valvova viranomainen voi tarvittaessa hyödyntää myös fyysisiä katselmointeja sen varmistamiseksi, että varmuuskopioita on eriytetty muusta järjestelmästä riittävästi. Katselmoinnissa tulisi varmistua esimerkiksi siitä, että uhkat kuten tulipalo, tulvat ja henkilöuhka, eivät koske sekä varmistettavaa järjestelmää että varmuuskopioita.
3. Jos kyseessä on fyysisen erottelun sijaan perusteltu looginen erottelu, voi valvova viranomainen hyödyntää esimerkiksi toimijan tekemiä skannauksia ja yhteydenottoyrityksiä sen varmistamiseksi, että eriytettyyn varmuuskopiointijärjestelmään ei pääse käsiksi varmistettavan viestintäverkon ja tietojärjestelmän puolelta.

Perustelut

Poikkeamatilanteista palautumisen yhteydessä tapahtuu liian usein niin, että palautus ei onnistu tai hyökkääjä onnistuu tuhoamaan sekä tietojärjestelmän että varmuuskopiot. Tämän vuoksi palautuksen kattava ja säännöllinen testaaminen sekä palautusjärjestelmän suojaaminen voivat olla toiminnan kannalta elintärkeitä.

Viitteet

IEC 62443-2-1:2013 (4.3.4.3.9)

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Työkalut

Julkri (TEK-20, VAR-09)

Kybermittari (ARCHITECTURE-1, ARCHITECTURE-5, RESPONSE-4)

10.4 Varaviestintäjärjestelmät

Toteutusesimerkki

- Toimijalla tulisi olla riskiarvioon perustuen viestintäkanavat, jotka mahdollistavat riittävän viestinnän viranomaisille, asiakkaille, palvelutoimittajille ja muille oleellisille tahoille. Näiden järjestelmien tulisi olla sellaisia, että ne toimivat myös vakavissa häiriötilanteissa sekä kriisien aikana. Katso myös kohta 9.8 Tiedon jakamisen turvallisuus.
- Varaviestintäkanava voi perustua esimerkiksi kuriirimenettelyyn, vaihtoehtoiseen pikaviestimeen tai mobiiliverkkoon.

Todennus
1. Valvova viranomainen todentaa, että toimija on määrittänyt tarpeelliset varaviestintäjärjestelmät riskiarvionsa perusteella. Varaviestintäjärjestelmiä käytetään silloin kun tavanomaisesti käytössä olevat järjestelmät eivät ole käytössä. Nämä järjestelmät ovat mainittuna esimerkiksi kohdan 10.1 suunnitelmissa. Valvova viranomainen todentaa erityisesti sen, etteivät valitut varaviestintäjärjestelmät ole riippuvaisia toimijan muusta infrastruktuurista. 2. Valvova viranomainen todentaa toimijan kanssa yhteistyössä, että varaviestintäjärjestelmät ovat toimivia. Tämän voi toteuttaa esimerkiksi lähettämällä testiviestejä varaviestintäjärjestelmällä.
Perustelut
Viitteet
ISO/IEC 27002:2022 (5.5, 5.29, 5.30, 7.13) NIS CG Reference document (3.12.3 Crisis management)
Työkalut
Julkri (VAR-06, TEK-22.1) Kybermittari (RESPONSE-3)

11 Perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan osittaiseen g alakohtaan. Tämän alakohdan kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 11 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 11 kohdassa.

Perustason tietoturvakäytännöillä tarkoitetaan perustason teknisiä ja muita toimenpiteitä järjestelmien, ohjelmien ja palveluiden turvallisuuden varmistamiseksi. Valvovan viranomaisen tulisi varmistaa, että toimija on suojannut tietojärjestelmänsä ja viestintäverkkonsa perustason tietoturvakäytännöin ja että työntekijät noudattavat niitä. Käytäntöjen ja niiden valvonnan taso tulisi mitoittaa riittäväksi perustuen toimintojen kriittisyyteen. Tämän ohella valittujen toimenpiteiden tulisi perustua yleisiin hyviin käytäntöihin sekä riskienarviointiin.

Tässä alaluvussa esitetyt perustason tietoturvakäytäntöjä koskevat suositukset on laadittu siten, että toimijat – myös sellaiset, jotka eivät kuulu NIS-sääntelyn soveltamisalaan – voisivat suosituksia seuraamalla arvioida organisaationsa kyberturvallisuuden kypsyystasoa ja parantaa kyberturvallisuuden tilaa. Perustason tietoturvakäytännöt ovat kevyessä muodossa esitetty kokoelma kaikista tässä suosituksessa esitetyistä toimenpiteistä, joten ne ovat siis osin päällekkäisiä muiden suosituksen alalukujen kanssa.

Valvova viranomainen voi hyödyntää perustason tietoturvakäytäntöjä luodakseen yleiskuvan valvottavien toimijoiden kyberturvallisuuden tasosta ja toimialan tilasta.

Tietoturvakäytännöt voivat sisältää sekä hallinnollisia että teknisiä toimenpiteitä. Suosituksessa esitetyt perustason tietoturvakäytännöt ovat:

1. Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille (ks. kohta 11.1).
2. Toimija on tunnistanut kriittisimmän omaisuutensa (ks. kohta 11.2).
3. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä (ks. kohta 11.3).
4. Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä (ks. kohta 11.4).
5. Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan (ks. kohta 11.5).
6. Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti (ks. kohta 11.6).
7. Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista (ks. kohta 11.7).
8. Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti (ks. kohta 11.8).
9. Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä (ks. kohta 11.9).
10. Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu (ks. kohta 11.10).
11. Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu (ks. kohta 11.11).
12. Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa (ks. kohta 11.12).
13. Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki) (ks. kohta 11.13).

11.1 Toimija on ohjeistanut perustason tietoturvakäytännöt henkilöstölle, alihankkijoille ja muille kumppaneille

Toteutusesimerkki
• Toimijalla on kirjalliset perustason tietoturvakäytännöt ja ne ovat saatavilla henkilöstölle, alihankkijoille ja muille kumppaneille. Nämä ovat myös tietoisia dokumenttien sijainnista. Käytäntöjä tarkastellaan ja tarvittaessa päivitetään säännöllisesti, esimerkiksi vuosittain.
Todennus

1. Valvova viranomainen todentaa, että toimijalla on kirjalliset perustason tietoturvakäytännöt, jotka ovat saatavilla koko henkilöstölle, alihankkijoille ja muille kumppaneille.

   Sisältö kattaa tietoturvakäytännöissä kuvatut toimintatavat, joita ovat mm. tietoturvallisuuteen liittyvät toimintatavat, ilmoituskanavat, tietojen ja laitteiden käsittelyohjeet, salasana- ja tunnuskäytännöt, etäkäyttöratkaisut, tietojenkalastelulta suojautumisen, laskutuspetoksilta suojautumisen, sekä muiden yleisimpien uhkien tunnistamisen.
2. Valvova viranomainen varmistaa toimijan henkilöstön tietämyksen ja tietoturvakäytäntöjen käytännön toteutumisen haastatteluilla.

Perustelut

Toimijan henkilöstön olisi tunnettava perustason käytännöt, jotta toimijan yleisen kyberturvallisuustietoisuuden voitaisiin sanoa olevan kohtuullisella tasolla. Perustason tietoturvakäytännöillä kyetään oikein ja kattavasti toteutettuna parhaimmillaan estämään yleisimmät tietoturvauhkat.

Viitteet

CCB CYFUN Basic (PR.AT-1)

IEC 62443-2-1:2013 (4.3.2.4.1-4.3.2.4.2)

ISO/IEC 27002:2022 (6.3)

NIST CSF 1.1 (PR.AT)

NIST CSF 2.0 (PR.AT)

Työkalut

Julkri (HAL-13, HAL-15)

Kybermittari (Yleisiä hallintatoimia, WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, WORKFORCE-4, PROGRAM-2)

11.2 Toimija on tunnistanut kriittisimmän omaisuutensa

Toteutusesimerkki

- Toimija on tunnistanut toimintansa kannalta kriittiset kohteet. Nämä kohteet ovat sellaisia, joita ilman toimija ei voi toimia, joihin kohdistuu toimialakohtaisia lakisääteisiä velvoitteita tai joihin kohdistunut tietoturvaloukkaus voi aiheuttaa suurta vahinkoa. Kohteet voivat olla esimerkiksi laitteita, ohjelmistoja, sovelluksia tai liiketoiminnan kannalta kriittistä dataa.
- Toimija on laatinut, viestinyt ja asettanut helposti saataville viestintäverkkojen ja tietojärjestelmien turvallisuuteen liittyvien toimintaperiaatteiden mukaiset käytännöt ja ohjeet omaisuudenhallintaan.
- Toimijan omaisuudenhallinnan tulisi olla säännöllistä ja johdonmukaista ja sen tulisi kattaa organisaation tunnistamat kriittiset toiminnot ja palvelut, tietovarannot ja muu aineeton ja aineellinen omaisuus, kuten käyttöönottamansa palvelut, tilit ja lisenssit.

Todennus
1. Valvova viranomainen todentaa, että toimijalla on omaisuudenhallintaan liittyvät käytännöt ja ohjeet. Omaisuudenhallinnan säännönmukaisuudesta ja johdonmukaisuudesta on kirjallista näyttöä. Omaisuudenhallinta kattaa vähintään toiminnan kannalta keskeisimmät komponentit. Käyttäjäohjeistuksessa tai -koulutuksessa kerrotaan näitä järjestelmiä koskevista turvallisuuteen liittyvistä käytännöistä.
Perustelut
Kriittisen omaisuuden tunnistaminen ja omaisuuden luokittelu mahdollistavat riskiperusteisen lähestymistavan. Riskiperusteinen lähestymistapa kyberturvallisuuteen parantaa toimijan kyberturvallisuuden tasoa tekemällä siitä järjestelmällisempää ja vähemmän satunnaista. Varsinkin toiminnan kannalta tärkeimpään omaisuuteen tulee kiinnittää erityistä huomiota, sillä siihen kohdistunut häiriö saattaa aiheuttaa toimijalle suurta vahinkoa.
Viitteet
CCB CYFUN Basic (ID.AM-1, ID.RA-1)) IEC 62443-2-1:2013 (4.2.3.4, 4.2.3.6) ISO/IEC 27002:2022 (5.9, 5.12) NIST CSF 1.1 (ID.AM-1, ID.RA-1) NIST CSF 2.0 (ID.AM-01, ID.RA-01)
Työkalut
Julkri (HAL-04) Kybermittari (CRITICAL-1, ASSET-1, ASSET-2, WORKFORCE-4)

11.3 Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä

Toteutusesimerkki
• Toimija on rajannut pääsyn palveluihinsa vähimpien oikeuksien periaatteella esimerkiksi rajaamalla pääsyn julkisissa viestintäverkoissa sijaitseviin palveluihin (rajapinnat, puhepalvelut, tiedostojaot, hallintapalvelut) identiteettien, käyttäjäryhmien, IP-osoitteiden, porttien tai protokollien perusteella. Vähimpien oikeuksien periaatetta ylläpidetään koko viestintäverkon elinkaaren ajan muutostenhallinnan avulla. • Toimijalla on käytössä ei-luotetuista viestintäverkoista tulevan haitallisen tai ei-toivotun liikenteen estävä ratkaisu, kuten palomuuri (erillislaitteena tai ohjelmistona) tai pääsylista (access control list, ACL). • Käytössä voi olla toimijan riskienhallintaan perustuen myös esimerkiksi tunkeutumisen havaitsemis- tai estämisjärjestelmiä (tunkeilijan havaitsemisjärjestelmä/intrusion detection system IDS, murron estämisjärjestelmä/intrusion prevention system IPS, endpoint detection and response EDR, extended

detection and response XDR) ja palvelunestohyökkäyksiä rajoittavia palveluita (esim. pakettipesurit).
- Toimijan viestintäverkoista ja tietojärjestelmistä on vähintään yksinkertaista dokumentaatiota, kuten verkkokuvat ja -kaaviot.

Todennus

1. Valvova viranomainen todentaa toimijan toimittamasta dokumentaatiosta, että pääsy toimijan palveluihin on rajattu vähimpien oikeuksien periaatteella erityisesti turvattomista viestintäverkoista.

   Dokumentaatiosta käy ilmi, että toimija on valinnut viestintäverkon suojaukset niin, että ne ovat riittäviä perustuen organisaation riskienhallintaan.

   Toimija on ohjeistanut muutosten toteuttamisen ja muutospyyntöjen tekemisen (Ks. 3.3 ja 3.4.).
2. Valvova viranomainen pyytää toimijaa todentamaan viestintäverkon suojaukset esimerkiksi esittämällä ne osat konfiguraatioista, jotka osoittavat esimerkiksi vähimpien oikeuksien periaatteen toteutumisen.
3. Valvova viranomainen todentaa viestintäverkon suojauksen omilla teknisillä testeillään, esimerkiksi skannauksin.

Perustelut

Internetiin yhdistettyihin viestintäverkkoihin ja tietojärjestelmiin kohdistuu huomattavan paljon automatisoitua haitallista liikennettä, jolla etsitään ja hyödynnetään järjestelmien heikkouksia. Rajoittamalla pääsy vain sallituista lähteistä tunnettuihin palveluihin sekä sulkemalla tarpeettomasti avoimena olevat tietoliikenneportit voidaan estää useimmat automatisoidut uhkat. Vastaava periaate pätee myös erilaisten luotettujen ja osittain luotettujen viestintäverkkojen välillä.

Toimijan kannattaa huomioida viestintäverkkonsa suunnittelussa myös sisäverkkonsa rakenne. Toimijan tulisi pyrkiä suojaamaan sisäverkkonsa niin, että mikäli hyökkääjä onnistuu pääsemään esimerkiksi sisäverkossa olevaan työasemaan käsiksi, olisi tämän hankala liikkua verkossa eteenpäin.

Viitteet

CCB CYFUN Basic (PR.AC-3)

IEC 62443-2-1:2013 (4.2.3.5)

IEC 62443-3-3:2019 (SR 1.13, SR 3.1, SR 5.2, SR 7.7)

ISO/IEC 27002:2022 (8.20, 8.21)

NIST CSF 1.1 (PR.AC-3)

NIST CSF 2.0 (PR.AA-03)

Työkalut

Julkri (TEK-01, TEK-02)

Kybermittari (ARCHITECTURE-2, ARCHITECTURE-3, ACCESS-1, ACCESS-2, ASSET-4)

11.4 Toimija on erottanut kriittiset ja haavoittuvat viestintäverkot ja tietojärjestelmät muista ympäristöistä

Toteutusesimerkki

- Toimija on eriyttänyt järjestelmät, jotka ovat hyvin haavoittuvia tai kriittisiä tai joiden vaarantuminen saattaa johtaa koko verkon tai järjestelmän vaarantumiseen. Järjestelmät on eriytetty vähintään loogisella tasolla muusta ympäristöstä. Tällaisia järjestelmiä ovat esimerkiksi hallintaverkot ja hallintatyöasemat.
- Erottelu voidaan toteuttaa monella eri tekniikalla, kuten fyysisellä tai loogisella erottelulla, käyttäen esimerkiksi seuraavia tai niiden yhdistelmiä: virtuaalilähiverkko (virtual local area network VLAN, virtual extensible local area network VXLAN), palomuuri, network access control NAC, tunkeilijan havaitsemisjärjestelmä/murron estämisjärjestelmä IDS/IPS, virtuaalinen erillisverkko (virtual private network VPN).
- Toimija on suojannut langattomat verkkonsa niin, etteivät ne vaaranna muita järjestelmiä.
- Toimijan eriytettyjen viestintäverkkojen välisessä liikenteessä on huomioitu vähimpien oikeuksien periaate (ks. 11.3).

Todennus

1. Valvova viranomainen todentaa toimijan toimittamasta dokumentaatiosta, että toimija on tunnistanut toimintaansa liittyvät kriittisimmät järjestelmät ja eriyttänyt ne. Nämä järjestelmät ja niiden eriyttämisen toteutus on kuvattuna. Eriyttämisessä on huomioitava julkiset verkot, toimijan omat verkot sekä mahdolliset liitännät kolmannen osapuolen verkkoihin.

   Tietyissä tapauksissa kuten hyvin pienissä viestintäverkoissa tai tietojärjestelmissä voi erottelu olla tarpeetonta riskienhallinnan kannalta. Tällöin riskienhallintaan perustuva jäännösriskien hyväksyntä voi olla riittävää.
2. Valvova viranomainen pyytää toimijaa todentamaan viestintäverkon erottelun konfiguraatiosta, kuten esittämällä siitä ne osat, jotka osoittavat esimerkiksi verkon jaottelun ja vähimpien oikeuksien periaatteen toteutumisen.
3. Valvova viranomainen todentaa viestintäverkon erottelun omilla teknisillä testeillä, esimerkiksi skannauksin.

Perustelut

Viestintäverkkojen erottelu on tärkeä suojauskeino ja se suojaa esimerkiksi haavoittuvimpia järjestelmiä. Erottelu voi estää monissa tapauksissa haitallisen liikenteen, kuten kiristyshaittaohjelman leviämisen järjestelmästä ja viestintäverkosta toiseen. Viestintäverkkojen erottelulla saadaan jaettua tietojärjestelmä pienempiin ja selkeämpiin kokonaisuuksiin, jolloin myös suodatussäännöt ja muut suojauskeinot ovat helpommin hallittavissa. Ongelmatilanteissa selvitystyö voi erottelun myötä kohdistua rajatumpaan osaan helpottaen palautumista.

Viitteet

CCB CYFUN Basic (PR.AC-5)

IEC 62443-2-1:2013 (4.3.3.4)

IEC 62443-3-3:2019 (SR 5.1)

ISO/IEC 27002:2022 (8.22) NIST CSF 1.1 (PR.AC-5) NIST CSF 2.0 (PR.IR-01)
Työkalut
Julkri (TEK-01, TEK-02, TEK-04) Kybermittari (ARCHITECTURE-2, CRITICAL-1)

11.5 Toimija on suojannut viestintäverkkonsa ja tietojärjestelmänsä haitallisia ja luvattomia ohjelmistoja vastaan

Toteutusesimerkki
• Toimijalla on tekniset kontrollit tai vähintään kirjalliset käytännöt ohjelmistojen asentamiseen ja haittaohjelmilta suojautumista vastaan (esimerkiksi kalastelusähköpostit, tuntemattomat ulkoiset tallennusmediat, piraattisovellukset, haitalliset verkkovierailut). • Toimijan tulisi hallita ohjelmistojen asentamista ja suorittamista sekä tallennusmedioiden käyttöä automaattisesti (esimerkiksi Windows Defender Application Control WDAC, AppLocker, AppArmor, SELinux). • Toimijalla on käytössä haittaohjelmasuojaus, kuten päätelaitteiden virustentorjuntaohjelmisto (Esim. Anti-Virus AV, EDR, XDR), IDS/IPS tai välityspalvelin. Haittaohjelmasuojausta voi olla myös esimerkiksi keskitetysti sähköpostipalvelussa (kalasteluviestien esto/anti-phishing, haittaohjelmien esto/anti-malware, DomainKeys Identified Mail DKIM, Domain-based Message Authentication, Reporting and Conformance DMARC jne.)
Todennus
1. Valvova viranomainen todentaa, että toimijalla on ohjeistus tai käytännöt haitallisten ja luvattomien ohjelmistojen asennuksen ja suorittamisen estämiseksi. Mahdolliset käytössä olevat haittaohjelmasuojaukset tai ohjelmien suorituksen estävät ohjelmistot ovat toiminnassa ja riittävän ajantasaisia. 2. Valvova viranomainen pyytää toimijaa todentamaan, miten toimija on toteuttanut haitallisten viestin tunnistamisen, luvattomien ulkoisten tallennusmedioiden ja sovellusten estämisen sekä haittaohjelmasuojausten pitämisen ajantasaisena.
Perustelut
Haittaohjelmia levitetään sekä kohdennetusti, esimerkiksi sähköpostien ja linkkien välityksellä, että luotetulta vaikuttavien lähteiden kautta, kuten aidon kaltaisen ohjelmiston välityksellä. Kalasteluviestit ja muut vastaavat haitalliset viestit ovat yksi yleisimmistä kyberuhkista. Haittaohjelmien leviämistä voidaan estää sekä hallinnollisin että teknisin menetelmin. Missä tahansa ohjelmistossa saattaa esiintyä haittaohjelmia esimerkiksi

toimitusketjuhyökkäyksien takia tai ohjelmisto voi itsessään lisätä hyökkäyspinta-alaa.
Viitteet
CCB CYFUN Basic (DE.CM-1, DE.CM-4, DE.CM-5) IEC 62443-2-1:2013 (4.3.4.3.8) IEC 62443-3-3:2019 (SR 3.2) ISO/IEC 27002:2022 (8.7, 8.19) NIST CSF 1.1 (DE.CM-1, DE.CM-2, DE.CM-4, DE.CM-5, DE.CM-7) NIST CSF 2.0 (DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-09)
Työkalut
Julkri (TEK-11) Kybermittari (ARCHITECTURE-3)

11.6 Toimija on järjestänyt tunnistautumisen sisäisiin ja ulkoisiin palveluihinsa ja laitteisiinsa turvallisesti

Toteutusesimerkki
• Toimijalla on salasanakäytännöt, jotka ohjeistavat valitsemaan turvallisia ja yksilöllisiä käyttäjätunnuksia sekä salasanoja, sekä ilmoittamaan tunnusten vaarantumisesta. • Turvallisten ja yksilöllisten käyttäjätunnusten ja salasanojen käyttöä voi edistää salasananhallintaohjelman avulla. • Toimija on tunnistanut järjestelmät, joissa voi ja tulee ottaa käyttöön vahvemmat tunnistus- ja todennusmenetelmät, kuten monivaiheisen tunnistautumisen (multi-factor authentication MFA).
Todennus
1. Valvova viranomainen todentaa, että toimijalla on olemassa salasanakäytännöt, jotka on ohjeistettu. Käytännöt sisältävät ohjeet tunnusten vaarantumisesta ilmoittamiseen. Toimija on analysoinut vahvojen todennusmenetelmien tarpeen ja ottanut ne käyttöön mahdollisuuksien mukaan. Toimijalla on lista järjestelmistä, joiden käyttöön vaaditaan vahva tunnistus- ja todennusmenetelmä. Toimijalla on lista järjestelmistä, joiden käyttöön ei vaadita vahvoja tunnistus- ja todennusmenetelmiä, sekä perustelu sille, miksi vahvoja tunnistus- ja todennusmenetelmiä ei niiden osalta ole otettu käyttöön. 2. Valvova viranomainen pyytää toimijaa esittämään järjestelmiensä konfiguraatiot niiltä osin kuin ne määrittelevät hyvät salasanakäytännöt tai vaativat vahvempia tunnistus- ja todennusmenetelmiä.
Perustelut

Laadukkaat salasanat ja useaan tekijään perustuvat todennusmenetelmät voivat estää tilien murtamisen. Mikäli samoja tunnuksia käytetään useassa paikassa, yhden tunnuksen varastaminen tarjoaa hyökkääjälle pääsyn myös muihin järjestelmiin luvatta. Tällaisia järjestelmiä voivat olla esimerkiksi sosiaalisen median alustat, jolloin organisaation tunnuksia voidaan väärinkäyttää haitallisiin tarkoituksiin. Heikoilla salasanoilla on mahdollista vaarantaa esimerkiksi sähköpostitunnuksia, joiden avulla voidaan levittää huijaus- tai haittaohjelmasähköposteja toimijan nimissä. Näillä tunnuksilla hyökkääjä voi päästä käsiksi myös toimijan sisäisiin järjestelmiin.

Viitteet

CCB CYFUN Basic (PR.AC-1)

IEC 62443-2-1:2013 (4.3.3.6)

IEC 62443-3-3:2019 (SR 1.1, SR 1.7)

ISO/IEC 27002:2022 (5.15, 5.17, 8.5)

NIST CSF 1.1 (PR.AC-1, PR.AC-7)

NIST CSF 2.0 (PR.AA-01, PR.AA-03)

Työkalut

Julkri (HAL-14, TEK-07, TEK-08)

Kybermittari (ACCESS-1, ACCESS-2, ASSET-1, ASSET-2)

11.7 Toimija on erottanut järjestelmiensä pääkäyttäjätunnukset ja korotettujen oikeuksien tunnukset muista tunnuksista

Toteutusesimerkki

- Toimijan pääkäyttäjä- tai ylläpitotehtäviä tekevällä henkilöstöllä on erilliset tunnukset näiden tehtävien tekemiseen.
- Toimijalla on käytännöt pääkäyttäjätunnusten ja korotettujen oikeuksien tunnusten myöntämiselle ja ylläpidolle. Käytännöissä määritetään tunnuksien elinkaaren hallinta, kuten esimerkiksi niiden myöntäminen, muutokset ja poistaminen.
- Pääkäyttäjätunnuksia ja korotettujen oikeuksien tunnuksia ei tule käyttää perustoimintoihin eikä peruskäyttäjätunnuksia tule käyttää pääkäyttäjätoimintoihin.
- Tarpeettoman laajoja käyttöoikeuksia tulee välttää. Käyttäjillä on esimerkiksi työasemiinsa vain peruskäyttäjäoikeudet, ellei työtehtävien suorittamiseen tarvitse työaseman pääkäyttäjäoikeuksia.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on käytännöt pääkäyttäjätunnusten tai korotettujen oikeuksien tunnusten myöntämiseen, niiden ylläpitoon ja niiden sallittuun käyttöön. Käytännöissä on huomioitu, että

pääkäyttäjätunnukset tai korotettujen oikeuksien tunnukset erotetaan peruskäyttäjätunnuksista.

Pääkäyttäjätunnuksia ja korotettujen oikeuksien tunnuksia annetaan vain tarvittaessa ja ne poistetaan tai niitä muutetaan esimerkiksi työtehtävien vaihtuessa tai muun toiminnallisen tarpeen muuttuessa.

2. Valvova viranomainen pyytää toimijaa todentamaan, että pääkäyttäjäoikeuksia on vain niillä henkilöillä, jotka tarvitsevat niitä työtehtävissään. Lisäksi voidaan vertailla dokumentoituja ja konfiguroituja pääkäyttäjäoikeuksia keskenään.

Perustelut

Pääkäyttäjäoikeuksilla on mahdollista saada huomattavasti enemmän vahinkoa aikaan kuin perustason rajatuilla käyttöoikeuksilla.

Pääkäyttäjätunnukset ovat kaikista halutuimpia kohteita hyökkääjille niiden tarjoamien mahdollisuuksien vuoksi. Siksi on erityisen tärkeää, että näihin kohdistuvat uhkat minimoidaan.

Viitteet

CCB CYFUN Basic (PR.AC-4)

IEC 62443-2-1:2013 (4.3.3.5)

ISO/IEC 27002:2022 (5.15, 8.2)

NIST CSF 1.1 (PR.AC-4, PR.AC-7)

NIST CSF 2.0 (PR.AA-05)

Työkalut

Julkri (TEK-04, TEK-07.2)

Kybermittari (ACCESS-2, ACCESS-3, ARCHITECTURE-3)

11.8 Toimija on varmistanut, että sen luottamuksellista tietoa käsitellään turvallisesti

Toteutusesimerkki

- Toimijalla on käytännöt, joilla määritetään tiedon luottamuksellisuus. Toimijan käytännöt sisältävät kirjalliset ohjeet tiedon käsittelyyn, kuten miten ja missä luottamuksellista tietoa säilytetään, käsitellään, siirretään eri järjestelmien välillä ja tuhotaan.
- Turvalliset käytännöt on ohjeistettu organisaation työntekijöille, alihankkijoille ja muille kumppaneille, jotka käsittelevät luottamuksellista tietoa.
- Luottamuksellinen tieto siirretään lähtökohtaisesti salattuna. Toimijan käyttämillä päätelaitteilla sijaitseva luottamuksellinen tieto (tietokoneet, puhelimet, ulkoiset tallennusvälineet) on tarvittaessa salattu, esimerkiksi levysalauksella (ks. 11.10).

Todennus
1. Valvova viranomainen todentaa, että toimijalla on ohjeistus, josta käy ilmi käytännöt luottamuksellisen tiedon turvalliseen säilytykseen, käsittelyyn, siirtämiseen ja tuhoamiseen. Nämä käytännöt koskevat tarvittaessa myös alihankkijoita ja muita toimijoita, jotka käsittelevät luottamuksellista tietoa. 2. Valvova viranomainen hyödyntää esimerkiksi haastatteluja ja katselmointeja luottamukselliseen tietoon liittyvien toimintatapojen tarkastelemiseen. Haastatteluilla todennetaan esimerkiksi sitä, miten henkilöstö käsittelee luottamuksellista tietoa. Lisäksi tiedon säilytyspaikkoja, säilytystapoja sekä tuhoamisen käytäntöjä voi katselmoida paikan päällä, tai hyödyntää toimijan toimittamaa materiaalia.
Perustelut
Tiedon huolimaton käsittely tai siirtäminen saattaa paljastaa sen oikeudettomille käyttäjille. Luottamukselliselle tiedolle saattaa olla myös lainsäädännöllisiä vaatimuksia, esimerkiksi EU:n yleinen tietosuoja-asetus (EU) 2016/679[13] tai sektorikohtaiset vaatimukset. Päätelaitteiden ja tallennusmedioiden katoamistilanteissa, esimerkiksi varkauksissa, on tärkeää, että kadonnut laite on salattu. Näin oikeudettomat käyttäjät eivät pääse käsiksi laitteessa oleviin tietoihin.
Viitteet
CCB CYFUN Basic (PR.DS-1, PR.DS-2) IEC 62443-2-1:2013 (4.3.4.4) IEC 62443-3-3:2019 (SR4.1, SR 4.3) ISO/IEC 27002:2022 (5.12, 5.14, 5.33, 5.34, 7.1, 7.9, 7.10, 8.3, 8.24) NIST CSF 1.1 (PR.DS-1, PR.DS-2, PR.DS-5, PR.IP-6) NIST CSF 2.0 (PR.DS-01, PR.DS-02, PR.DS-10)
Työkalut
Julkri (TEK-16, TEK-18) Kybermittari (ARCHITECTURE-5, THIRD-PARTIES-2, WORKFORCE-4)

11.9 Toimija on huolehtinut, että sen järjestelmiä päivitetään säännöllisesti ja kriittiset päivitykset asennetaan viivytyksettä

Toteutusesimerkki
• Toimijalla on käytännöt, joilla se seuraa käyttämiensä käyttöjärjestelmien, sovellusten ja laiteohjelmistojen kriittisiä turvallisuuspäivityksiä ja asentaa ne viivytyksettä riskiarvion perusteella, esimerkiksi automaattisilla päivityksillä.

[13] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

Toimija on laatinut tarkoituksenmukaiset kirjalliset ohjeet kriittisiin turvallisuuspäivityksiin.

- Järjestelmiä, joita ei voi päivittää, tulee suojata muilla menetelmillä ja päivitykset tulee asentaa hallitusti silloin kun se on mahdollista.
- Myös muita kuin kriittisiä turvallisuuspäivityksiä tehdään säännöllisin väliajoin, esimerkiksi kuukausittain, kun järjestelmän toimittaja julkaisee uudet päivitykset.

Todennus

1. Valvova viranomainen todentaa toimijan päivityskäytännöt sekä päivitysten toteutuman dokumentaatiosta. Lisäksi katselmoidaan käytännöt, joilla päivittämisen tarve havaitaan. Valvova viranomainen katselmoi myös tavan, joilla poikkeamat päivityksiin hallitaan. Tämä on voitu toteuttaa esimerkiksi dokumentoimalla poikkeukset tai riskienhallinnan menetelmin.
2. Valvova viranomainen todentaa päivityskäytäntöjen toteutumisen esimerkiksi pyytämällä tietoa (tapahtumaloki, kuvaruutukaappaukset ja vastaavat) tapahtuneista päivityksistä.
3. Valvova viranomainen todentaa päivityskäytäntöjen toteutumisen hyödyntämällä esimerkiksi skannauksia. Mahdolliset poikkeamat selvitetään toimijan avustuksella tai dokumentaatiosta.

Perustelut

Ohjelmistohaavoittuvuudet ovat tyypillinen tapa levittää haittaohjelmia, ja ne voivat mahdollistaa esimerkiksi järjestelmän väärinkäytön tai luvattoman pääsyn järjestelmään haavoittuvuutta hyväksikäyttämällä. Etenkin kriittisten haavoittuvuuksien laaja hyväksikäyttö on usein nopeaa, jolloin kriittisten turvallisuuspäivitysten viivytyksetön asentaminen on erityisen tärkeää. Järjestelmät, joita ei voi päivittää, voivat olla hyvin haavoittuvia, ja ne tulee suojata esimerkiksi eriyttämällä ne muista järjestelmistä.

Viitteet

CCB CYFUN Basic (PR.MA-1)

IEC 62443-2-1:2013 (4.3.4.3.7)

ISO/IEC 27002:2022 (8.8, 8.19, 8.32)

NIST CSF 1.1 (PR.IP-3, PR.MA-1)

NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03)

Työkalut

Julkri (TEK-17, TEK-19)

Kybermittari (THREAT-1)

11.10 Toimija on huolehtinut, että sen palvelut ja laitteet on turvallisesti konfiguroitu

Toteutusesimerkki

- Toimijalla on käytännöt, joiden perusteella se poistaa järjestelmistään tarpeettomat ominaisuudet. Näihin sisältyvät muun muassa ylimääräisten palveluiden tai laitteiden sammutus tai poistaminen käytöstä.
- Toimija on muuttanut järjestelmiensä tai laitteidensa oletusasetukset kuten oletussalasanat ja säilyttää päivitetyt salasanat turvallisesti. Mikäli toimija on luonut tunnuksia hätätilanteita varten, on niiden suojaamisesta, käyttöperusteista ja saatavuudesta hätätilanteiden yhteydessä huolehdittava.
- Toimija on ottanut järjestelmiensä tarjoamat turvallisuustoiminnot käyttöön. Näitä voivat olla esimerkiksi automaattiset ohjelmistopäivitykset, turvalliset tunnistusmenetelmät, salaus ja tapahtumakirjausten (loki) käyttöönotto.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on käytännöt laitteiden konfiguraation tarkastamiseksi ennen käyttöönottoa ja tarvittaessa päivitysten yhteydessä. Nämä käytännöt sisältävät tarpeettomien ja turvattomien ominaisuuksien poiston sekä turvattomien oletusasetusten muutokset. Monissa laitteissa on helposti käyttöönotettavia turvallisuusominaisuuksia, jotka toimijan on osana tätä prosessia syytä ottaa käyttöön, esimerkiksi työasemien tallennusmedioiden salaus, automaattiset päivitykset, turvalliset hallintayhteydet ja salausta käyttävät protokollat.
2. Valvova viranomainen todentaa turvallisten konfiguraatioiden toteutumisen esimerkiksi hyödyntämällä toimijan tekemää dokumentaatiota toteutuneista konfiguraatioista. Nämä voivat olla esimerkiksi kuvaruutukaappauksia tai konfigurointijärjestelmään liittyvää tilatietoa.

Perustelut

Tarpeettomien ominaisuuksien poistaminen pienentää hyökkäyspinta-alaa ja pienentää hyökkääjän mahdollisuuksia päästä toimijan järjestelmiin. Esimerkiksi oletuskäyttäjätunnukset ja -salasanat ovat sellaisia, joita hyödynnetään laajalti automatisoidun skannauksen yhteydessä. Mikä tahansa laite tai palvelu voi mahdollistaa pääsyn myös kriittisiin järjestelmiin tai laitteita voidaan hyväksikäyttää rikolliseen toimintaan. Suojaamattomat laitteet, kuten valvontakamerat, voivat paljastaa luottamuksellista tietoa.

Viitteet

IEC 62443-3-3:2019 (SR 7.6, SR 7.7)

ISO/IEC 27002:2022 (8.9, 8.27, 8.32)

NIST CSF 1.1 (PR.IP-1, PR.IP-3)

NIST CSF 2.0 (PR.PS-01, PR.PS-02, PR.PS-03)

Työkalut

Julkri (TEK-10)

Kybermittari (ASSET-3, ARCHITECTURE-3, SITUATION-1)

11.11 Toimija on huolehtinut, että sen kriittiset palvelut ja tieto-omaisuus on varmuuskopioitu

Toteutusesimerkki

- Toimijalla on käytännöt varmuuskopioiden ottamista, palautuskäytäntöjä ja varmuuskopioiden elinkaaren hallintaa varten. Mikäli varmuuskopiot sisältävät dataa, johon kohdistuu lainsäädännöllisiä vaatimuksia, on toimijalla käytännöt myös varmuuskopioiden oikea-aikaisesta tuhoamisesta.
- Kriittisistä tietovarannoista on otettu säännöllisesti varmuuskopioita. Varmuuskopiot on eriytetty fyysisesti ja loogisesti niistä järjestelmistä, joista ne on otettu. Varmuuskopioita on suojattu vähintään vastaavan tasoisilla menettelyillä kuin alkuperäistä dataa.
- Varmuuskopioiden palautuksen testaamista on tehty säännöllisesti.

Todennus

1. Valvova viranomainen todentaa, että toimijalla on käytännöt, joiden perusteella toteutetaan toiminnan kannalta tärkeäksi määriteltyjen tietovarantojen varmuuskopiointi. Käytännöistä käy ilmi myös se, miten varmuuskopiot on suojattu ja miten ne on eriytetty varmuuskopioitavista järjestelmistä. Toimija on myös dokumentoinut tavat, joilla varmuuskopioiden toimivuutta testataan säännöllisesti.
2. Valvova viranomainen todentaa esimerkiksi haastatteluilla, toimijan toimittamilla tiedoilla tai katselmoimalla, että varmuuskopioita koskevat käytännöt toteutetaan. Toimitettavat tiedot voivat olla esimerkiksi kuvaruutukaappauksia, konfiguraatioita ja tapahtumalokeja varmuuskopioihin ja niiden käytäntöihin liittyen. Fyysinen katselmointi voi sisältää esimerkiksi varmuuskopiojärjestelmän olinpaikan katselmoinnin tai tallennusmedian säilytyspaikan ja sen turvallisuuden katselmoinnin.

Perustelut

Varmuuskopioilla suojaudutaan tahallista tai tahatonta tiedon häviämistä vastaan. Varmuuskopioilla järjestelmä saadaan tarvittaessa palautettua myös sellaisessa tilanteessa, jossa esimerkiksi koko järjestelmä on salattu hyökkääjän toimesta. Näissä tapauksissa on erityisen tärkeää, että hyökkääjä ei pysty salaamaan myös varmuuskopioita.

Palauttamista on hyvä testata säännöllisesti, sillä varmuuskopioissa on usein virheitä ja palauttaminen epäonnistuu. Järjestelmien palautusta tarvitaan usein vakavissa häiriötilanteissa. Häiriötilanteista palautuminen kannattaa suunnitella kokonaisuutena esimerkiksi osana jatkuvuus- ja palautumissuunnittelua.

Viitteet

CCB CYFUN Basic (PR.IP-4)

IEC 62443-2-1:2013 (4.3.4.3.9)

IEC 62443-3-3:2019 (SR 7.3) ISO/IEC 27002:2022 (5.30, 8.10, 8.13) NIST CSF 1.1 (PR.IP-4, PR.IP-6, PR.IP-9, PR.IP-10) NIST CSF 2.0 (PR.DS-11) NIST SP 800-82 Rev. 2
Työkalut
Julkri (TEK-20, TEK-22) Kybermittari (RESPONSE-4, ASSET-2, ARCHITECTURE-5)

11.12 Toimija on varautunut, miten sen toiminta voidaan ylläpitää vakavissa poikkeamissa

Toteutusesimerkki
• Toimijalla on kirjalliset käytännöt, joilla määritetään vastuut ja toimenpiteet erityisesti vakavia poikkeamia varten. • Toimijalla on kirjalliset käytännöt NIS-ilmoituksen tai muun viranomaisilmoituksen tekemiseen poikkeamatilanteissa.
Todennus
1. Valvova viranomainen todentaa, että toimijalla on kirjalliset käytännöt poikkeamia varten. Käytännöistä käyvät ilmi ilmoitusvelvollisuudet, ajantasaiset ja konkreettiset yhteystiedot ja yhteydenottokanavat sisäisille ja ulkoisille kontakteille, vastuut ja velvollisuudet, mahdolliset hätätilanteiden käyttäjätunnukset sekä toimintaohjeet. 2. Siinä tapauksessa, että toimijalla on ollut poikkeamia, valvova viranomainen todentaa toimijan poikkeamanhallinnan käytännöt esimerkiksi haastatteluin ja poikkeaman käsittelyyn liittyvän dokumentaation avulla. Erityisesti todennetaan se, että poikkeamanhallinta on ollut riittävää, siinä on selvitetty poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi ja että poikkeamanhallinnassa on toteutettu lakisääteiset velvollisuudet kuten poikkeamailmoitukset. Näitä voidaan todentaa esimerkiksi toimijan toimittamasta materiaalista, kuten poikkeaman loppuraportista.
Perustelut
Hyvin suunnitellut toimintatavat ja käytännöt poikkeamatilanteissa lyhentävät palautumisaikaa. Käytännöt ilmoitusvelvollisuuksien suhteen varmistavat sen, että lakisääteisten ilmoituksien, kuten NIS2-direktiivin mukaisen ilmoituksen, tekeminen ei unohdu poikkeamatilanteessa.
Viitteet
CCB CYFUN Basic (RS.RP-1, RC.RP-1, RC.CO-3) IEC 62443-2-1:2013 (4.3.4.5)

ISO/IEC 27002:2022 (5.5, 5.24, 5.26) NIST CSF 1.1 (RS.RP, RC.RP, RC.CO-3) NIST CSF 2.0 (RS.MA-05, RC.RP-02, RC.CO-03)
Työkalut
Julkri (HAL-08) Kybermittari (RESPONSE-1, RESPONSE-2, RESPONSE-3, RESPONSE-4)

11.13 Toimijalla on käytössään kriittisten toimintojen tapahtumakirjaus (loki)

Toteutusesimerkki
• Toimija on varmistanut, että kriittisiin toimintoihin liittyvistä tapahtumista syntyy tapahtumakirjauksia. • Tapahtumakirjauksia syntyy esimerkiksi pääkäyttäjien tekemistä toimenpiteistä ja käyttöoikeuksiin liittyvistä muutoksista, sekä mahdollisuuksien mukaan kaikista turvallisuuteen liittyvistä tapahtumista koko viestintäverkon ja tietojärjestelmän laajuudella. • Tapahtumakirjauksia syntyy myös luottamuksellisen tiedon käsittelystä perustuen esimerkiksi lainsäädännön vaatimuksiin. • Tapahtumakirjauksen olisi hyvä vastata ainakin seuraaviin kysymyksiin mahdollisuuksien mukaan: kuka, mitä, mistä, milloin, mihin. • Tapahtumaloki on suojattu muutoksilta ja sitä hallinnoidaan erillisillä käyttäjätunnuksilla. Tapahtumaloki on varmuuskopioitu säännöllisin väliajoin tai kopioitu erilliseen järjestelmään.
Todennus
1. Valvova viranomainen todentaa, että toimija on määritellyt lokien tarpeen ja tarvittaessa tietojärjestelmän ja viestintäverkon lokiarkkitehtuurin. Lokijärjestelmän laajuus on suhteutettu toimijan tarpeisiin nähden. 2. Valvova viranomainen todentaa esimerkiksi toimijan toimittamasta materiaalista tai katselmoimalla, että lokia otetaan vähintään toiminnalle keskeisimmistä kohteista ja toiminteista ja sitä säilytetään turvallisesti niin, ettei sitä pysty luvatta muuttamaan.
Perustelut
Häiriötilanteissa tapahtumakirjaukset (lokit) ovat keskiössä tapahtuman kulun selvittämiseksi. Ilman kunnollisia tapahtumakirjauksia häiriön juurisyyn selvittäminen saattaa olla mahdotonta. Tapahtumakirjausten varmuuskopiointi on tärkeää varsinkin kiristyshaittaohjelmien vuoksi, sillä kiristyshaittaohjelmat salaavat usein koko tallennusmedian. Mikäli näin käy, ei tapahtumalokikaan enää ole luettavissa, ellei sitä ole erikseen varmuuskopioitu tai siirretty järjestelmään, johon hyökkääjällä ei ole pääsyä.

Viitteet
CCB CYFUN Basic (PR.PT-1, DE.AE-3)
IEC 62443-2-1:2013 (6.10.1, 10.3)
ISO/IEC 27002:2022 (5.28, 5.34, 8.15)
Liikenne- ja viestintäviraston ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta (Traficom/376384/03.04.05.01/2022)
NIST CSF 1.1 (PR.PT-1, DE.AE-3)
NIST CSF 2.0 (PR.PS-04, DE.CM-01)
Työkalut
Julkri (TEK-12)
Kybermittari (SITUATION-1, RESPONSE-1, ACCESS-3, ASSET-4)

12 Toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi

Suositukset perustuvat NIS2-direktiivin 21 artiklan 2 kohdan johtolauseeseen viestintäverkkojen ja tietojärjestelmien fyysistä ympäristöä suojaavien toimenpiteiden osalta. Tämän kansallisesta täytäntöönpanosta säädetään kyberturvallisuuden riskienhallinnasta annetun lain 9 §:n 2 momentin 12 kohdassa ja tiedonhallintalain 18 c §:n 2 momentin 12 kohdassa.

1. **Tilaturvallisuus ja fyysinen pääsynvalvonta**: Toimijan tulisi tunnistaa fyysisen ympäristön tekijät, joiden turvallisuus on toiminnan kannalta tärkeää ja suojata näitä fyysisten uhkien vaikutukselta ja häiriöiltä. Toimijan tulisi huomioida myös viestintäverkkoihin ja tietojärjestelmiin vaikuttavat fyysiset ympäristöt, jotka voivat olla hyvin erilaisia ja esimerkiksi maantieteellisesti laajoja tai suppeita. (Ks. kohta 12.1).

2. **Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan**: Fyysisiä uhkia ovat ympäristötekijät ja pahantahtoiset toimijat. Viestintäverkkoja ja tietojärjestelmiä tulisi valvoa ja niitä tulisi suojata luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä. Lisäksi on suojauduttava luonnollisilta ja yhteiskunnallisilta tapahtumilta, kuten tulipaloilta, tulvilta ja levottomuuksilta. (Ks. kohta 12.2).

3. **Toiminnalle välttämättömien resurssien jatkuvuuden varmistaminen**: Toimijan tulisi varautua välttämättömien resurssien, kuten sähkönjakelun, tietoliikenneyhteyksien ja jäähdytyksen häiriöihin ja estää viestintäverkkojen ja tietojärjestelmien tuhoutuminen, vahingoittuminen tai toimijan kriittisten toimintojen keskeytyminen välttämättömien resurssien puutteen tai häiriön vuoksi. (Ks. kohta 12.3).

12.1 Tilaturvallisuus ja fyysinen pääsynvalvonta

Toteutusesimerkki

- Toimija on tunnistanut viestintäverkkojen ja tietojärjestelmien turvallisuudelle kriittisimmät alueet. Toimija on suojannut turvallisuudelle kriittiset alueet luvattomalta pääsyltä sekä muilta vahingoilta ja häiriöiltä.
- Kriittisiä alueita voivat olla esimerkiksi toimistotilat, palvelintilat ja muut tekniset tilat. Toimijasta riippuen myös esimerkiksi piha-alue toimijan tilojen läheisyydessä voi olla tarpeen rajata esimerkiksi aidalla.
- Pääsy toimijalle kriittisille alueille on rajattu vain oikeutetuille henkilöille pääsynvalvonnan avulla. Pääsynvalvontaa voi toteuttaa esimerkiksi ovia lukitsemalla, rakenteellisilla esteillä, hälyttimillä ja vartioinnilla.
- Pääsynvalvonnasta on mahdollisuuksien mukaan pidetty tapahtumakirjausta. Tapahtumakirjauksesta tulisi käydä ilmi se, kuka on kulkenut tietystä ovesta tai kulkuväylästä, mihin aikaan ja millä tavalla esimerkiksi oven mahdollinen lukitus on avattu. Tapahtumakirjaukset voivat olla automaattisia tai paperikirjanpitoa.
- Tärkeimpiä ovia ja kulkuväyliä on tarvittaessa valvottu tallentavalla kameravalvonnalla. Valvonnan tarve perustuu toimijan tekemään riskiarviointiin (ks. 1).
- Toimijalla on kiinnittänyt huomiota erityisesti kolmansien osapuolten henkilöiden kulunvalvontaan.
- Toimijalla on käytännöt, joilla määritetään vierailijoiden kulkeminen turvallisuuskriittisille alueelle, alueella liikkuminen ja poistuminen alueelta.
- Toimija on määritellyt tarvittaessa muita tilaturvallisuuteen liittyviä käytäntöjä, kuten puhtaan pöydän ja puhtaan näytön periaatteet, tunnisteiden näkyvillä pitämisen sekä vieraiden pääsyn toimitilaan ovenavauksen yhteydessä estämisen (tailgating).
- Toimijalla on käytännöt vanhentuneen tai muuten käytöstä poistetun laitteiston tai tallennusvälineiden turvalliseen uudelleenkäyttöön, kierrätykseen tai muuhun hävittämiseen. Lisää tietoa kohdassa 5 Omaisuudenhallinta.

Todennus

1. Valvova viranomainen todentaa, että toimija on dokumentoinut viestintäverkkojen ja tietojärjestelmien turvallisuuden kannalta kriittisimmät alueet ja niiden pääsynhallinnan periaatteet. Periaatteista käy ilmi kriittisten alueiden määrittely riskiarvioinnin mukaisesti sekä esimerkiksi niihin liittyvät kulunvalvontakäytännöt ja muut tilojen turvallisuuteen liittyvät periaatteet, periaatteet tapahtumakirjauksesta sekä mahdollisesta kameravalvonnasta. Periaatteiden tulee kattaa mahdollisuuksien mukaan toimijan kaikki toimitilat, joissa sijaitsee viestintäverkkoja ja tietojärjestelmiä.
2. Valvova viranomainen todentaa toimijan tilaturvallisuuden ja suojaukset viestintäverkkojen ja tietojärjestelmien osalta katselmoimalla esimerkiksi fyysisen pääsynvalvonnan kyvykkyyden toimijan toimitiloissa. Viranomainen voi kiinnittää huomiota esimerkiksi kameravalvontaan ja sen kattavuuteen, kulunvalvontaan ja palvelinlaitteiston sijoitteluun sekä niiden fyysiseen suojaamiseen.

Perustelut

Asiattomien henkilöiden pääsy toimijan kriittisiin tiloihin saattaa vaarantaa toiminnan luottamuksellisuuden, eheyden tai saatavuuden. Erityisesti tilat, joissa

toimija säilyttää suojattavaa omaisuutta, henkilötietoja tai turvallisuusluokiteltua tietoa tulee suojata ulkopuolisilta henkilöiltä.
Viitteet
ISO/IEC 27002:2022 (7.1, 7.2, 7.4) NIST CSF 1.1 (PR.AC-2, DE.CM-2) NIST CSF 2.0 (PR.AA-06, DE.CM-02) NIS CG Reference document (3.13.1 Perimeter and physical access control)
Työkalut
Julkri (FYY-02, FYY-07, TEK-09) Kybermittari (RISK-2, ACCESS-3)

12.2 Suojaus fyysisiä ja ympäristön aiheuttamia uhkia vastaan

Toteutusesimerkki

- Toimija on huomioinut toiminnassaan fyysiset ja ympäristön aiheuttamat uhkat viestintäverkoille ja tietojärjestelmille ja mitoittanut riskienhallintatoimenpiteensä oikean suuruisiksi omaan toimintaansa nähden vallitsevissa olosuhteissa, valvomalla ja suojaamalla niitä luvattomalta fyysiseltä pääsyltä, vahingoilta ja häiriöiltä. Nämä uhkat voivat syntyä tahallisista tai tahattomista fyysisistä toimista tai luonnonmullistuksista. Näitä riskejä voivat olla esimerkiksi tulipalot, tulvat, myrskyt, vandalismi tai terrorismi.
- Riskien pienentämiseen vaikuttavia toimia ja suojausta fyysisiä ja ympäristön aiheuttamia uhkia vastaan voivat olla esimerkiksi automaattiset sammutusjärjestelmät, palo-osastointi, rakennuksen rakenteellisen vahvuuden varmistaminen ja oikein mitoittaminen, lämpötilan ja kosteuden seuranta, ylijännitesuojaus yms.
- Toimijan riskienhallinnan tulisi käsitellä edellä mainitut uhkat kaikki vaaratekijät huomioivan lähestymistavan pohjalta. Lisätietoa kohdassa 1.2 Kaikki vaaratekijät huomioiva lähestymistapa.
- Onnettomuuksien tai muiden häiriöiden sattuessa toimija on arvioinut siihen liittyvää riskienhallintaansa ja sen oikeasuhtaisuutta. Toimija on päivittänyt tarvittaessa toimintakäytäntöjään estääkseen kyseisten tapahtumien tapahtumisen uudelleen.

Todennus

1. Valvova viranomainen todentaa, että toimija on riskienhallinnassaan ja jatkuvuussuunnittelussaan huomioinut fyysiset ja ympäristön aiheuttamat uhkat viestintäverkkoihinsa ja tietojärjestelmiinsä. Toimintaa välittömästi vaarantavat riskit on hallittu soveltuvin hallintakeinoin. Toimijan tulee täyttää mahdolliset lakisääteiset vaatimukset esimerkiksi palosuojauksen osalta.

Perustelut

Fyysiset ja ympäristön aiheuttamat uhkat saattavat vaarantaa toiminnan jatkuvuuden. Pahimmassa tapauksessa uhkat voivat vaikuttaa toimijaan niin, että liiketoimintaa ei pystytä enää jatkamaan.
Viitteet
ISO/IEC 27002:2022 (7.3, 7.5) NIST CSF 1.1 (PR.IP-5) NIST CSF 2.0 (PR.IP-02) NIS CG Reference document (3.13.2 Protection against physical and environmental threats)
Työkalut
Julkri (FYY-02) Kybermittari (RISK-2, RISK-3, ACCESS-2, RESPONSE-3)

12.3 Toiminnalle välttämättömien resurssien jatkuvuuden varmistaminen

Toteutusesimerkki
• Toimija on huomioinut viestintäverkkojen ja tietojärjestelmien toiminnalle välttämättömien resurssien jatkuvuuden (tukipalvelut). Näitä ovat esimerkiksi sähkönsyöttö, veden- ja kaasunjakelu, jäähdytys, viemäröinti ja tietoliikenneyhteydet. • Toimija on suhteuttanut tukipalveluissa tapahtuvien häiriöiden aiheuttamat riskit omaan toimintaansa ja kompensoinut niitä tarvittaessa, esimerkiksi sähkökatkon varalta varavoimageneraattorilla, akkuvarmistuksella tai vaihtoehtoisilla voimanlähteillä. Tietoliikenneyhteyksien tulisi olla tarvittaessa vikasietoisia, esimerkiksi varayhteyksin. • Toimija on päivittänyt ja ylläpitänyt toimintaohjeitaan säännöllisesti sekä tarvittaessa häiriön jälkeen, jotta häiriöltä tai niiden seurauksilta voidaan jatkossa välttyä. • Toimijalla on selkeät toimintaohjeet vakavien häiriötilanteiden varalta. • Toimija on valvonut tukipalveluiden tilaa ja seurannut niihin liittyviä häiriötiedotteita. Toimijalla tulisi olla ajantasaiset yhteystiedot tukipalveluiden toimittajiin häiriötilanteiden varalla. • Toimijan olisi hyvä harjoitella ja testata varajärjestelmiään säännöllisesti. Harjoitukset on suunniteltu huolellisesti ja niissä on varmistuttu siitä, että häiriötilanteen simulointi ei aiheuta todellista vaaraa toiminnalle tai ympäristölle.
Todennus
1. Valvova viranomainen todentaa, että toimija on varautunut välttämättömien resurssien, kuten sähkönjakelun, tietoliikenneyhteyksien ja jäähdytyksen häiriöihin ja estänyt viestintäverkkojen ja tietojärjestelmien tuhoutumisen, vahingoittumisen tai toimijan kriittisten toimintojen keskeytymisen välttämättömien resurssien puutteen tai häiriön vuoksi. Toimija on arvioinut toiminnalleen ja jatkuvuudelleen tarvittavat välttämättömät resurssit ja tarvittaessa

määrittänyt niihin liittyviä riskejä kompensoivia hallintakeinoja. Hallintakeinot voivat olla esimerkiksi tarvittavia sopimuksia varajärjestelyistä, erillisiä varayhteyksiä ja suunnitelmia niiden käyttöönotosta. 2. Valvova viranomainen todentaa, että toimijan toiminnalle välttämättömien resurssien varajärjestelyjä on testattu tai niiden varassa toimimista on harjoiteltu käytännössä.
Perustelut
Häiriöt tukipalveluissa saattavat aiheuttaa pitkiäkin katkoksia tai häiriöitä toimijan toiminnalle, mikä saattaa aiheuttaa mainehaittaa tai vaarantaa toiminnan jatkuvuuden. Hyvin erilaiset poikkeavat tilanteet saattavat aiheuttaa tiedon menetyksen tai muita vaurioita. Esimerkkejä poikkeavista tilanteista ovat esimerkiksi sähkökatkot, ongelmat laitteiden jäähdytyksessä ja vesivahingot.
Viitteet
ISO/IEC 27002:2022 (7.11) NIST CSF 1.1 (ID.BE-1, ID.BE-2, ID.SC-2) NIST CSF 2.0 (GV.OC-01, GV.OC-05, GV.SC-03) NIS CG Reference document (3.13.3 Supporting utilities)
Työkalut
Julkri (VAR-05, VAR-07) Kybermittari (RESPONSE-3, RESPONSE-4, RESPONSE-5)

13 Lähdeluettelo

Suositukseen liittyvät säädökset ja ohjeet

Kansalliset

Laki kyberturvallisuuden riskienhallinnasta (xxxx/2024)

Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki)

Liikenne- ja viestintäviraston määräys teletoiminnan tietoturvasta (M67) (TRAFICOM/248815/03.04.05.00/2022) (voimaan 1.9.2024)

Digi- ja väestötietoviraston ohje: Turvallisen sovelluskehityksen käsikirja. Julkaistu 19.5.2020.

Liikenne- ja viestintäviraston ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta (Traficom/376384/03.04.05.01/2022)

Valtiovarainministeriön julkaisuja 2019:7: Ohje turvallisuuskriittisiin hankintoihin: Määräysvaltamuutoksiin varautuminen turvallisuuskriittisissä tieto- ja viestintäjärjestelmien sekä -ratkaisujen hankinnoissa: https://urn.fi/URN:ISBN:978-952-251-988-7

Valtiovarainministeriön julkaisuja 2023:54: Riskienhallinnan käsikirja valtiohallinnon toimijalle: https://urn.fi/URN:ISBN:978-952-367-633-6

Valtiovarainministeriön julkaisuja 2023:57: Suositus tietoturvallisuudesta hankinnoista, kohderyhmä tiedonhallintayksiköt ja viranomaiset: https://urn.fi/URN:ISBN:978-952-367-645-9

Kansainväliset

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa (NIS 2 -direktiivi, kyberturvallisuusdirektiivi)

NIS Cooperation Group: NIS CG Reference document (on security measures for important & essential entities

Suositukseen liittyvät standardit ja viitekehykset

Kansalliset

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö: https://urn.fi/URN:ISBN:978-952-367-275-8

Liikenne- ja viestintäviraston Kybermittari: kybermittari.fi

Kansainväliset

CCB CYFUN (CyberFundamentals) Framework Basic

COSO Enterprise Risk Management Framework

IEC 62443-2-1:2013 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 2-1: Tietoturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten

IEC 62443-2-4:2019 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers

IEC/TR 62443-3-1:2013 Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Osa 3-1: Tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille

IEC 62443-3-3:2019 Industrial communications networks - Network and system security - Part 3-3: System security requirements and security levels

IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

ISO/IEC 27001:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmä. Vaatimukset

ISO/IEC 27002:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot

ISO/IEC 27003:2018 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta

ISO/IEC 27005:2022 Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Ohjeita tietoturvariskien hallintaan

ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

ISO 31000:2018 Riskienhallinta. Ohjeet

NIST CSF 1.1 Cybersecurity framework 1.1

NIST CSF 2.0 Cybersecurity framework 2.0

NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations: https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide: https://doi.org/10.6028/NIST.SP.800-61r2

NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security: https://doi.org/10.6028/NIST.SP.800-82r3

OWASP Application Security Verification Standard

OWASP Top Ten

The STRIDE Threat Model

The DREAD risk assessment model

Muut julkaisut

Traficomin Kyberturvallisuuskeskus: Haavoittuvuudet, miten niistä ilmoitetaan oikein

Traficomin Kyberturvallisuuskeskus: Näin keräät ja käytät lokitietoja

Traficomin Kyberturvallisuuskeskus: Kyberharjoitusohje

NSA, CISA: Identity and Access Management: Recommended Best Practices for Administrators