Haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostaminen

Oskari Laulainen

Opinnäytetyö, ylempi AMK
Toukokuu 2024
Teknologialiiketoiminnan johtaminen

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Laulainen, Oskari

Haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostaminen

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2024, 65 sivua.

Teknologialiiketoiminnan johtamisen tutkinto-ohjelma. Opinnäytetyö YAMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Uusia vakavia tietoturvahaavoittuvuuksia, jotka koskevat laajasti käytössä olevaa IT-infrastruktuuria julkaistaan 2020-luvulla useita kymmeniä päivässä. Haavoittuvuuksia käytetään yhä enemmän maailmalla hyödyksi erilaisissa kehittyneissä kyberhyökkäyksissä. Haavoittuvuuksien analysointi ja korjaaminen vaativat asiantuntijoilta laadukasta tilanneymmärryksen muodostamista sekä johtajilta nopeaa ja oikea-aikaista päätöksentekoa.

Tutkimuksessa perehdyttiin asiakokonaisuuksiin, jotka liittyvät haavoittuvuuksiin, haavoittuvuuden hallinnan tekniseen tilanneymmärrykseen ja korjaavista toimenpiteistä päättämiseen. Tutkimus aloitettiin keräämällä aiheeseen liittyvää teoriaa hyödyntäen viranomaisten verkkoon julkaisemaa tietoa, tietoturvallisuuden standardeja ja viitekehyksiä sekä aiheeseen liittyvää kirjallisuutta ja verkkomateriaalia. Teorian tueksi esiteltiin relevantteja tapausesimerkkejä sekä niihin liittyvän tilanneymmärryksen muodostamista.

Tieto- ja kyberturvallisen IT-järjestelmän luominen ja ylläpitäminen vaatii sen kannalta olennaisien riskien tunnistamista ja niiden hallintaa. Uuden järjestelmän luomisen tueksi on tarjolla erilaisia standardeja, viitekehyksiä ja toimintamalleja, joiden avulla ympäristöstä saadaan turvallisempi ja siinä voidaan käsitellä sensitiivistäkin dataa. Järjestelmistä ei ole kuitenkaan mahdollista rakentaa pysyvästi tietoturvallisia, sillä ne vaativat jatkuvaa ylläpitämistä ja käytössä olevien tuotteiden tietoturvallisten versioiden päivittämistä.

Jatkuvasti kehittyvässä toimintaympäristössä päätöksien tekeminen suhteessa aikaan korostuu, kun tunnistetaan erilaisia haavoittuvuuksia, joiden hyväksikäyttö antaa ulkopuoliselle taholle mahdollisuuden kohdistaa organisaatioon vihamielistä kybervaikuttamista. Haavoittuvuuksiin liittyvän tilanneymmärryksen muodostaminen teknisellä tasolla vaatii laajaa aihealueeseen perehtyneisyyttä sekä oman organisaation toimintaympäristön tuntemusta, jotta haavoittuvuuksien aiheuttamaa uhkaa ja niiden mahdollisia vaikutuksia voidaan arvioida.

Tuloksena syntyi aihealueen ympärille tehty tutkimus, jossa käsiteltiin haavoittuvuuden hallinnan sekä haavoittuvuuksien kannalta olennaisia aihealueita ja korjaavien toimenpiteiden johtamisen menetelmiä. Tutkimuksessa käsiteltiin myös aiheeseen olennaisesti liittyvää teoriaa ja sen hyödyntämistä tilanneymmärryksen muodostamisen tukena.

Avainsanat (asiasanat)

Kyberturvallisuus, haavoittuvuus, tilanneymmärrys

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Laulainen, Oskari

Situational Awareness from Technical Vulnerability Management

Jyväskylä: JAMK University of Applied Sciences, May 2024, 65 pages.

Master's Degree Programme in High-Technology Business Management. Master's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Tens of new severe security vulnerabilities affecting most widely used IT infrastructure are being disclosed daily in 2020's. The exploitation of new vulnerabilities in various advanced cyber-attacks is increasing globally. Patching and analyzing these vulnerabilities require high quality situational awareness from professionals. Time is also a critical factor, as quick and timely decisions are required from organization's leaders while handling vulnerabilities.

The research examined subjects related to vulnerabilities, situational awareness from technical vulnerability management and making decisions for patching vulnerabilities. The research began by collecting relevant theory from the subject by using information published on the Internet by officials, information security standards and frameworks and other topic related online materials. To support the theory relevant case examples were presented to gain understanding about making situational awareness related to them.

Creating and maintaining a system that is both information and cyber secure requires identification and management of relevant risks. Various types of standards, frameworks and operational models are available to support the development and implementation of a secure IT system for handling the organization's sensitive data. However, it is not possible to build permanently secure systems as they require continuous maintenance and installing the latest security updates and practices for the products used.

In a constantly evolving operational environment the decision-making in relation to time becomes crucial when identifying vulnerabilities that could allow the threat actors to target the organization's networks by exploiting them. The formation of technical level situational awareness from vulnerabilities requires deep understanding of the own organization's operational environment to assess the possible threats and impacts to the core business.

As a result, research centered around the subject area was made to address the topics related to vulnerability management and the leadership and implementation of the vulnerability corrective actions. The study also handled other relevant supporting theory of vulnerabilities and situational awareness.

Keywords/tags (subjects)

Cyber security, vulnerability, situational awareness

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

Taulukot

Lyhenteet ja määritelmät

API	Application Programming Interface
CAB	Change Advisory Board
CISA	Cybersecurity and Infrastructure Security Agency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
ECAB	Emergency Change Advisory Board
IOA	Indicator of Attack
IOC	Indicator of Compromise
IP	Internet Protocol
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
KEV	Known Exploited Vulnerability
MFA	Multi-Factor Authentication
NAC	Network Access Control
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
POC	Proof of Concept
SSH	Secure Shell
VPN	Virtual Private Network

1 Johdanto

Joulukuussa 2021 Traficomin Kyberturvallisuuskeskus julkaisi punaisen varoituksen, joka alkoi seuraavasti: *”Internetpalveluissa erittäin laajasti käytetyn, haavoittuvan Log4j-komponentin hyväksikäyttötapauksia havaitaan jatkuvasti lisää. Ylläpitäjiltä vaaditaan nopeaa reagointia”.* Tästä käynnistyi yksi 2020-luvun merkittävimmistä haavoittuvuustapahtumista, sillä kyseinen komponentti oli käytössä lähes kaikissa palveluympäristöissä ja sen hyväksikäyttöjen määrät kasvoivat räjähdysmäisesti maailmalla. Ympäristöjen suojaamiseksi ylläpitäjiltä vaadittiin erittäin nopeita toimenpiteitä päivitettyjen versioiden asentamiseksi, jotta palvelut saatiin turvattua. Hyväksikäyttämällä haavoittuvuutta hyökkääjän on mahdollista ottaa haavoittuva palvelu haltuunsa ja suorittaa mielivaltaisesti haluamiaan toimenpiteitä. Kaikkien haavoittuvien komponenttien päivittämien vie valtavasti aikaa, koska kaikki haavoittuvat komponentit tulee kartoittaa ja tuotantoon vietävät päivitykset tulisi todentaa toimiviksi ennen asennuksia (Log4j-komponentin haavoittuvuus on aktiivisen hyväksikäytön kohteena - päivitä välittömästi! 2021).

Järjestelmissä olevien komponenttien päivittämiseksi sekä haavoittuvuuden hallinnan toteuttamiseksi olisikin järkevää luoda toimiva, jatkuva ja dokumentoitu prosessi. Julkaistavat tietoturva- sekä järjestelmäpäivitykset tulisi testata ja asentaa ajallaan yhtenä osana järjestelmän kokonaisturvallisuutta. Kyberhyökkäysten määrän arvioidaan kasvavan merkittävästi seuraavien vuosien aikana, minkä lisäksi niistä aiheutuvat kustannukset tulevat arvioiden mukaan kasvamaan. Kriittisen infrastruktuurin järjestelmiin suoritetut onnistuneet kyberhyökkäykset saattavat aiheuttaa miljoonatappioita organisaatioille sekä massiivisia katkoja niiden tuottamien palveluiden saatavuudelle (Riggs, Tufail, Parvez, Tariq, Khan, Amir, Vuda & Sarwat 2023).

Suurien tuotantoympäristöjen päivittäminen voi aiheuttaa mittavia katkoksia järjestelmien käytössä. Käyttökatkokset voivat tulla kalliiksi, mikäli tuotannon tekeminen estyy alasajon seurauksena. Teknisen tilanneymmärryksen luominen ja uhkien kartoittaminen päätöksenteon tueksi korostuu, jotta päätöksiä tekevälle taholle voidaan esittää vahvat perustelut toimenpiteiden suorittamiselle mahdollisista taloudellisista tappioista huolimatta. Myös päätöksenteon roolien tulee olla selkeästi määriteltyjä, jotta tarvittavat toimenpiteet voidaan käynnistää luvan myöntämisen jälkeen. Vaikka haavoittuvan komponentin päivittämättä jättäminen voi kuulostaa riskin ottamisen arvoiselta, saattavat siitä aiheutuvan mahdollisen hyökkäyksen vaikutukset nousta todella

merkittäviksi. Joissain tapauksissa on mahdollista, että jopa koko tietojärjestelmä joudutaan rakentamaan uudelleen tai hyökkääjä saattaa vaatia valtavia lunnaita järjestelmän saatavuuden palauttamiseksi.

1.1 Opinnäytetyön aiheen valinta ja tausta

Opinnäytetyön aiheen valintaan vaikuttivat organisaation tarve kehittää haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostamista sekä tilannekuvan luomista tiedossa olevien haavoittuvuuksien ja niihin liittyvien toimenpiteiden osalta. Opinnäytetyön toimeksiantajana toimii Puolustusvoimien johtamisjärjestelmäkeskus, jonka tehtäviin kuuluu Puolustusvoimien kybertilannekuvan muodostaminen. Haavoittuvuuden hallinnan ja julkaistuihin haavoittuvuuksiin liittyvän tilanneymmärryksen muodostaminen sekä haavoittuvuuksien osalta tehtävien toimenpiteiden tunnistaminen on myös olennainen osa kybertilannekuvaa yleisellä tasolla. Opinnäytetyössä tehtyä tutkimusta voidaan hyödyntää myös taustamateriaalina tilanneymmärryksen muodostamiseksi muualla Puolustusvoimissa, ja sitä on mahdollista hyödyntää myös toiminnan kehittämiseen muissa organisaatioissa (Puolustusvoimien johtamisjärjestelmäkeskus N.d.).

Haavoittuvuuden hallinnasta on aiheena tehty paljon julkisia tutkimuksia, opinnäytetöitä ja julkaisuja, jotka kuitenkin painottuvat pääsääntöisesti haavoittuvuuden hallinnan prosessiin ja haavoittuvuuksien korjaamiseen. Tilanneymmärryksen muodostamista ja tilannekuvan ylläpitämistä käsitellään yleensä pintapuolisesti osana haavoittuvuuden hallinnan kokonaisuutta. Tässä opinnäytetyössä pyritään lähestymään aihetta eri näkökulmasta kuitenkin siten, että myös olennaiset asiat haavoittuvuuden hallinnasta aiheena tulee kerrottua. Opinnäytetyöhön pyritään löytämään olennaiset asiat, joita organisaatioiden tulee huomioida muodostettaessa tilanneymmärrystä erilaisien haavoittuvuuksien osalta.

1.2 Opinnäytetyön toteutus

Opinnäytetyö toteutetaan teoriapohjaisena tutkimuksena, jossa selvitetään menetelmiä haavoittuvuuden hallinnan tilanneymmärryksen muodostamisen tueksi ja tilannekuvan rakentamiseksi. Opinnäytetyö toteutetaan julkisena ja julkisiin lähteisiin perustuvana, eikä se sisällä turvallisuusluokiteltua materiaalia tai liitosta Puolustusvoimiin, Puolustusvoimien prosesseihin tai toiminta-

malleihin. Opinnäytetyön teorian tueksi esitellään ajankohtaisia toisistaan poikkeaviin haavoittuvuuksiin liittyviä tapausesimerkkiä, joiden kautta tilanneymmärryksen muodostamista ja haavoittuvuuden hallintaa lähestytään.

2 Tutkimusasetelma

2.1 Tutkimuksen tavoitteet

Tutkimuksen tavoitteena opinnäytetyössä on määritellä julkaistujen haavoittuvuuksien vaikutusta erilaisille kohdeympäristöille ja teknisen tilanneymmärryksen muodostamisen periaatteita. Vaikuttavuutta arvioidaan haavoittuvuuksien yleisten luokitteluperiaatteiden, hyväksikäytettävyyden, korjausmahdollisuuksien ja kohteen kriittisyyden kautta. Tutkimuksen lopputuloksena syntyy raportti, jota voidaan hyödyntää organisaation tilanneymmärryksen muodostamisen tukena. Tutkimuksen tavoitteena on myös määritellä korjaavien toimenpiteiden päätöksenteon tahoja ja toimenpiteitä sekä järjestelmän muutoksista aiheutuvaa mahdollista haittaa suhteessa saavutettuun hyötyyn järjestelmien turvallisuuden kannalta. Tutkimuksen avulla organisaatio voi tunnistaa myös kokonaisuuksia, joita tulisi kehittää tai joita ei ole vielä otettu huomioon haavoittuvuuden hallinnassa.

2.2 Tutkimuskysymykset ja työn rajaus

Ensimmäisenä tutkimuskysymyksenä työssä on tutkia vaatimuksia sille, että organisaatio kykenee muodostamaan riittävän teknisen tilanneymmärryksen haavoittuvuuden hallinnasta sekä mahdollisesta haavoittuvuuden aiheuttamasta uhkasta sen käytössä oleville järjestelmille. Toisena tutkimuskysymyksenä on, kuinka organisaation päätöksiä tekevälle pystytään luomaan tarpeeksi riittävät perusteet välittömien haavoittuvuuksia korjaavien toimenpiteiden käynnistämisestä tai jopa hätämuutoksesta, vaikka niiden suorittamisesta saattaa aiheutua taloudellisia tappioita ja millainen uhka haavoittuvaksi jätettyyn ympäristöön mahdollisesti kohdistuu.

2.3 Tutkimusmenetelmät

2.3.1 Laadullinen tutkimus

Tutkimusmenetelmänä opinnäytteessä käytettiin laadullista, eli kvalitatiivista tutkimusta. Opinnäytteessä ei keskitytty haavoittuvuuksien määrälliseen tarkasteluun tai haavoittuvuuksien lukumäärällisiin vaikutuksiin. Opinnäytteessä haavoittuvuuksia ja niihin liittyviä toimenpiteitä käytiin läpi näkökulmasta, jossa pyrittiin panostamaan laadukkaan analyysin ja tilanteenarvion tekemiseen erityyppisiin haavoittuvuuksiin liittyvien olennaisien yksityiskohtien kannalta. Haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostamiseksi laadullisen tutkimuksen kautta pyrittiin vastaamaan kysymyksiin: mitä, miten, milloin ja miksi?

Opinnäytteessä pyrittiin case-esimerkkien kautta tuomaan esille kohdeympäristöön perustuvan tilanteenarvion merkitystä käyttäen apuna esimerkiksi ohjelmistovalmistajien ja viranomaisten sekä tietoturvatalojen julkaisemia suosituksia haavoittuvuuksien käsittelystä ja niiden hyväksikäytön ehkäisemiseen liittyvistä toimenpiteistä. Menetelmiä ja ohjeistuksia hyväksikäyttäen saatiin tuotua kontrastia erilaisiin tilanteisiin, joissa tiettyjä haavoittuvuuteen ja sen hyväksikäytettävyyteen liittyviä ehtoja toteutuu.

2.4 Tiedonhaku ja lähdeaineisto

Tutkimuksen tietopohjaksi ja lähdeaineistoksi pyrittiin keräämään mahdollisimman monipuolisia lähteitä, sillä aihealueeseen liittyen löytyy paljon sivuavaa materiaalia niin julkisista lähteistä, kuin kirjallisuudestakin. Aineisto koostui viranomaistiedosta ja viranomaisten tekemistä julkaisuista sekä eri maineikkaiden tietoturvatalojen sivustoilla julkaistuista tietoaineistoista, kuten artikkeleista ja blogikirjoituksista. Tietoa haettiin myös akateemisesta aiheeseen liittyvästä kirjallisuudesta.

Tiedonhakuun käytettiin asiasanaperusteisesti kirjastoista löytyvää materiaalia. Asiasanoina käytettiin esimerkiksi haavoittuvuuden hallintaa ja tietoturvahaavoittuvuutta sekä muita aiheeseen ja tietotarpeeseen sopivia hakuja. Internetistä sekä julkisista lähteistä tietoa haettiin käyttäen eri hakukoneiden antamia tuloksia viranomaislähteistä, tietoturvatalojen artikkeleista ja blogikirjoituksista sekä voimassa olevasta lainsäädännöstä. Puolustusvoimiin liittyvään materiaaliin ei suoritettu tiedonhakua eikä opinnäytteessä käytetty Puolustusvoimien materiaalia.

Tutkimuksessa käytettiin myös kansainvälistä lähdeaineistoa, joka koostui julkisista lähteistä kerätyistä kansainvälisten kyberturvallisuusviranomaisten julkaisuista ja tiedotteista, kansainvälisistä akateemisista materiaaleista ja kansainvälisien tietoturvatalojen asiantuntija-artikkeleista. Aihealue on globaali, joten kansainvälisen lähdemateriaalin hyödyntäminen toi tutkimukseen syvyyttä ja vertailukohtia esimerkiksi suomalaisten ja ulkomaalaisten viranomaisten julkaisemiin ohjeistuksiin ja tiedotteisiin.

3 Tieto- ja kyberturvallisen toimintaympäristön periaatteita

3.1 Tieto- ja kyberturvallisuuden teoriaa

Yleisesti määriteltynä tietoturva voidaan jakaa hallinnollisten ja teknisten toimien osalta kolmeen osaan kuvion 1 mukaan. Judd mainitsee blogissaan, että ensimmäistä kertaa näitä kolmea määritelmää on käytetty yhdessä jo 1990-luvulla. Nämä mainitut kolme osaa ovat luottamuksellisuus, käytettävyys ja eheys. Kaikkien kolmen tietoturvan osa-alueen täydellinen toteutuminen voi kuitenkin osoittautua haastavaksi, jolloin organisaation tulee harkita tarkasti, mitä osa-alueita se haluaa painottaa, jotta sen jatkuva toiminta ei esty liian tiukasta tietoturvasta (Judd 2020).

Luottamuksellisuudella tarkoitetaan sitä, että esimerkiksi organisaation järjestelmässä olevaan tietoon pääsevät käsiksi vain ne henkilöt tai tahot, joilla siihen on oikeus tai osoitettu tietotarve. Käytettävyys on yksinkertaisuudessaan sitä, että tieto ja tietojärjestelmät ovat niihin oikeutettujen käyttäjien saatavilla ja käytettävissä. Eheydellä puolestaan tarkoitetaan sitä, että ulkopuoliset tahot, joilla ei ole oikeutta eivät pääse muuttamaan tai muokkaamaan tietoa tai tiedon, kuten dokumenttien tai julkaisujen sisältöä (Tietoturva 2020).

Kuvio 1: Confidentality, integrity and availability -kolmio (Judd 2020).

Tietoturva on kuitenkin Suomen tietosuojavaltuutetun mukaan vain yksi osa tietosuojaa. Tietoturvan tarkoituksena on suojata tietoaineisto- ja järjestelmät. Tietosuoja puolestaan on oma kokonaisuutensa, jolla turvataan henkilötietojen käsittelyä ja määritellään, kuinka henkilötietoja käsitellään. Henkilötiedoiksi lasketaan kaikki tiedot, jotka liittyvät tunnistettavissa olevaan tai tunnistettuun luonnolliseen henkilöön. Henkilötietoja saa kuitenkin säilöä lähes missä muodossa tahansa (Tietosuoja 2024).

Useilla erityyppisillä toimijoilla on velvollisuus huolehtia tietoturvasta verkkojensa sekä palveluidensa osalta. Pääosin velvoitteet tulevat lainsäädännöstä, jossa esimerkiksi laki sähköisen viestinnän palveluista määrittää toimenpiteitä tietoturvan toteuttamiseksi viestinnän välittäjän ja lisäarvopalvelun tarjoajan sekä muiden niiden lukuun toimivien osalta. Lait eivät tarkkaan määrittele keinoja, joilla esimerkiksi viestin lähettäjän ja vastaanottajan välinen viestintämahdollisuus turvataan, mutta antaa toimivaltuuden ryhtyä välttämättömiin toimiin, jotta tietoturva toteutuu. Eri tahoisten toimijoiden tulee suojata verkkojaan sekä palveluitaan perusteellisesti, mutta toimenpiteiden toteutus on lopetettava, mikäli lainsäädäntö ei enää anna niille toimivaltaa (L 917/2014, 272 §).

Kyberturvallisuus voidaan määritellä monella tapaa. Steinbergin mukaan esimerkiksi yksittäisen henkilön sosiaalisen median käyttäjätunnuksen turvaaminen ulkopuolisilta tahoilta tai työaseman pitäminen puhtaana haittaohjelmista on kyberturvallisuutta. Voittoa tavoittelevan yhtiön toimesta kyberturvallisuudella voidaan puolestaan tarkoittaa esimerkiksi sitä, että palvelimet, joissa säilytetään yhtiön toiminnan kannalta kriittistä ja salassa pidettävää tietoa tulee olla suojattu riittävällä

tasolla. Valtionhallinnon organisaation tapauksessa kyberturvallisuus voi tarkoittaa turvallisuusluokitellun materiaalin suojaamista digitaalisin keinoin lakien, ohjeiden ja politiikkojen vaatimalla tavalla (Steinberg 2022).

Kyberturvallisuuteen vaikuttaa myös kaikkien teknologioiden jatkuva kehittyminen. Haittaohjelmista tulee monimutkaisempia ja vaikeampia havaita, uusia kriittisiä tietoturvahaavoittuvuuksia julkaistaan jatkuvasti sekä uhkatoimijoiden taktiikat, tekniikat ja työkalut kehittyvät. Palveluiden ja verkkosivujen toimintaa kyetään häiritsemään palvelunestohyökkäyksillä, henkilöt voivat esiintyä verkossa varastetulla tai väärennetyllä identiteetillä saavuttaakseen halutun loppuasetelman esimerkiksi yksittäisen henkilön tai organisaation kyberturvallisuuden vaarantamiseksi (Steinberg 2022).

3.2 Ohjelmisto- ja järjestelmäkehitys

3.2.1 Nykyaikainen ketterä sekä turvallinen ohjelmistokehitys

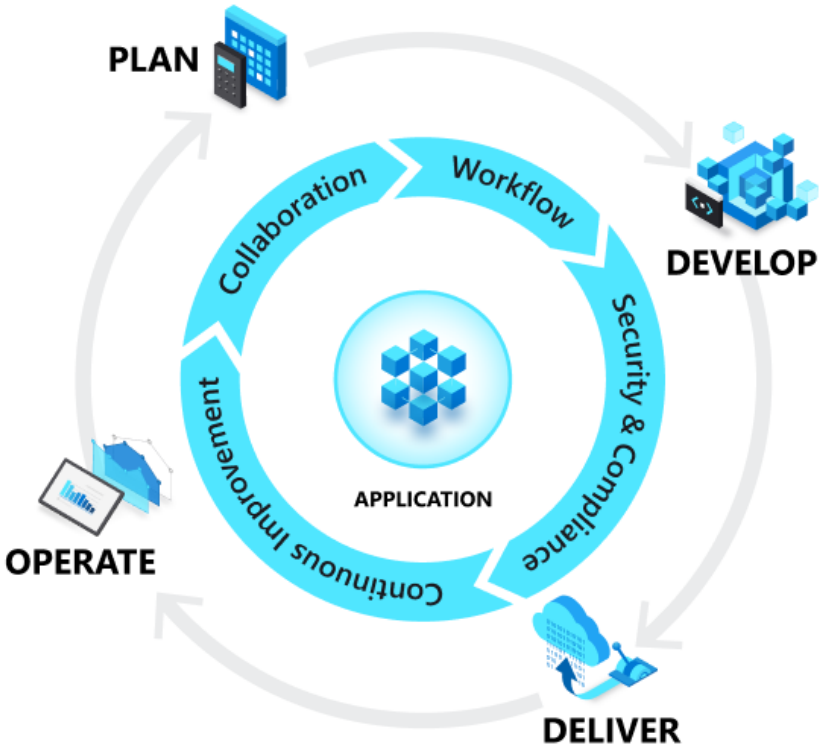
Microsoftin julkaisemassa (2023) artikkelissa kuvataan ohjelmistokehitystä termillä DevOps, joka tulee sanoista kehittäminen (development) ja operaatiot (operations). Yhdistelmällä kuvataan henkilöiden, prosessin ja teknologian yhdistämistä ohjelmistojen suunnittelun, toimittamisen ja operaatioiden kannalta. Turvallista ohjelmistokehityksen prosessia puolestaan kuvataan monesti termillä DevSecOps, joka pohjautuu samoihin perustoihin kuin DevOps, mutta keskittyy turvalliseen järjestelmä- ohjelmistokehittämiseen (Alvarenga 2022).

DevOps-kulttuurin omaksuminen sekä sen käytännöt ja työkalut tuovat luotettavuutta prosessin kautta syntyviin sovelluksiin. Tavoitteina on myös palvella paremmin asiakkaiden tarpeita ja saavuttaa liiketoiminnan kannalta asetetut tavoitteet nopeammin. DevOps auttaa projektiryhmiä tuottamaan arvoa asiakkaille, sillä Microsoftin mukaan sen kautta syntyy parempia ja luotettavampia tuotteita. (What is DevOps? 2023).

DevOps-ohjelmistokehitystä ohjaa sille luotu elinkaari, joka koostuu neljästä eri vaiheesta alla olevan kuvion mukaisesti. Elinkaaren vaiheet ovat suunnittelu, kehittäminen, toimittaminen ja operointi. Jokainen vaihe on riippuvainen toisistaan ja kaikilla projektiin osallistuvilla rooleilla on tehtäviä jokaisessa vaiheessa. Elinkaareen kuuluu myös kehitettävän tuotteen turvallisuuden

varmistaminen jatkuvan testaamisen ja prosessin kautta. Turvallisuuteen panostetaan heti projektin alusta asti, eikä sitä aleta rakentaa vasta, kun tuote on valmis. Lisäksi tuotetta kehitetään ja parannetaan jatkuvasti asiakkaan tarpeiden mukaisesti. Asiakkaan palautteen perusteella tehtävät korjaukset pyritään tuottamaan mahdollisimman pian esimerkiksi julkaistavana ohjelmistopäivityksenä. (What is DevOps? 2023).

Kaikkien edellä mainittujen elinkaaren vaiheiden toteutuminen vaatii jatkuvaa yhteydenpitoa asiakkaaseen sekä tehokasta projektiryhmän sisäistä tiedonvaihtoa. Elinkaaren vaiheiden noudattaminen on myös olennainen osa, jotta työn kulku toteutuu ja DevOps-prosessissa luotava tuote säilyy laadukkaana ja luotettavana. Uuden ominaisuuden tai tuotteen kehittäminen lähtee aina uudelleen liikkeelle suunnitteluvaiheesta ja päätyy lopulta tuotantoon vientivaiheeseen (What is DevOps? 2023).



Kuvio 2: DevOps sovelluskehityksen elinkaari (What is DevOps? 2023)

DevSecOps puolestaan on Alvarengan mukaan jatke DevOps-prosessille, joka takaa turvallisen tuotteen toimittamisen. Sekä DevOpsin että DevSecOpsin etu on, että niissä pyritään mahdollisim-

man nopeisiin toimituksiin. DevSecOps-prosessin mukaan turvallisuuteen liittyvät korjaavat toimenpiteet suoritetaan aina ensimmäisenä, jonka jälkeen uudet prosessissa suunnitellut ominaisuudet tehdään jo lähtökohtaisesti turvallisiksi. Puolestaan DevOps-prosessissa tuotteen turvallisuus tarkastetaan tyypillisesti ennen toimittamista. DevSecOps tähtää jatkuvaan kehittämiseen sekä jatkuvaan toimittamiseen neljän eri vaiheen kautta, jotka ovat rakentaminen, testaaminen, toimittaminen ja käyttöönotto (Alvarenga 2023).

DevSecOps-prosessissa tuotteen turvallisuus varmistetaan jatkuvalla tietoturvaskannaamisella ja koodin tuotetun koodin turvallisuuden tarkastelulla. Skannaamisella pyritään löytämään toimitettavasta tuotteesta haavoittuvuuksia ja tietoturva-aukkoja. Tuotettua koodia ja ohjelmistoa analysoidaan myös puhtaasti tietoturvallisuuden näkökulmasta. Analyysin ja skannauksen perusteella tehdyt havainnot ja löydetyt haavoittuvuudet pyritään korjaamaan mahdollisimman varhaisessa vaiheessa ja niiden toteutumista valvotaan ja tuotetta monitoroidaan jatkuvasti. Mikäli tuotannossa olevaan versioon julkaistaan haavoittuvuus, pyritään siihen vastaamaan korjaavilla toimenpiteillä mahdollisimman nopeasti (Alvarenga 2023).

3.3 Tietoturvastandardit ja -työkalut järjestelmäkehityksen tukena

Tietoturvastandardien tavoitteena on organisaation tietoturvallisuuden ajantasaisuuden, kehittymisen ja kattavuuden varmistaminen. Standardit auttavat myös suojelemaan organisaation tietojen ja toimintojen luottamuksellisuutta, eheyttä ja saatavuutta. Toteutettaessa riippumatonta arviointia järjestelmille toimivat standardit sekä niiden noudattaminen hyvänä apuvälineenä niihin valmistautumiseen. Kun valittua tietoturvastandardia noudatetaan organisaatiossa jo mahdollisimman varhaisessa vaiheessa tuotantoa, on sen periaatteiden toteutumiselle paremmat edellytykset (ISO/IEC 27000 Tietoturvallisuuden standardisarja 2023).

3.3.1 ISO/IEC 27000-sarja

Tieto- ja kyberturvallisen IT-järjestelmän rakentamisen tueksi on laadittu standardisarja ISO/IEC 27000, jossa määritellään suosituksia tietoturvallisuuden hallitsemiseksi, riskien vähentämiseksi ja kyberresilienssin luomiseksi. Standardisarja on luotu sellaiseksi, että se vastaa kaikenkokoisien or-

ganisaatioiden käyttötarpeisiin yleisluontoisten vaatimuksien kautta. Noudattamalla standardisarjan eri standardeja organisaatio voi myös valmistautua esimerkiksi tietoturva-auditointiin (ISO/IEC 27000 Tietoturvallisuuden standardisarja 2023).

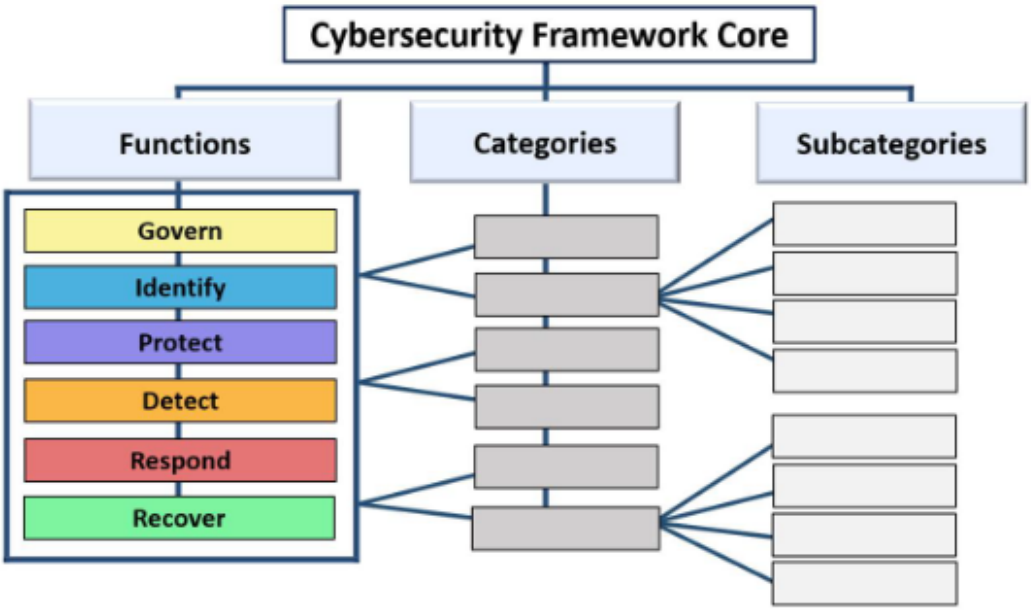
ISO27000-sarjassa on useita eri standardeja, joilla annetaan ohjausta eri tieto- ja kyberturvallisuuden osa-alueisiin. Esimerkiksi standardissa 27001 määritellään tietoturvallisuuden hallintajärjestelmien vaatimuksia. Standardissa esitetään, kuinka tietoturvallisuuden hallintajärjestelmä luodaan, toteutetaan ja ylläpidetään sekä esitetään vaatimuksia sen jatkuvalle parantamiselle. Standardi 27002 puolestaan on tarkoitettu käytettäväksi 27001-standardissa määritellyn järjestelmän toteuttamisprosessiin ja luomisen tueksi. Sitä voidaan hyödyntää myös organisaation tietoturvallisuuden hallintaohjeen kehittämiseen. Muissa sarjan standardeissa esitetään ohjeita esimerkiksi tietoturvariskien hallintaan ja henkilötietojen turvaamiseen (ISO/IEC 27000 Tietoturvallisuuden standardisarja 2023).

3.3.2 NIST:n julkaisemat viitekehykset

NIST julkaisi kyberturvallisuuden viitekehyksensä ensimmäistä kertaa vuonna 2013, viimeisin julkaistu versio viitekehyksestä on helmikuulta 2024. Viitekehys tarjoaa kyberturvallisuuteen liittyvää ohjausta organisaatioille, joiden tavoitteena on kehittää kyberriskien tunnistamista, havainnointia ja niihin vastaamista. Viegasin ja Kuyucun mukaan NIST:n kyberturvallisuuden viitekehys koostuu kolmesta pääosasta, joista ensimmäisenä on ydinosa. Ydinosa koostuu kyberriskien käsittelyyn liittyvistä toimenpiteistä ja referensseistä ohjeistuksiin sekä kontrolleihin, joita määritellään useissa eri standardeissa (Viegas & Kuyucu 2022).

Kyberturvallisuuden viitekehyksen mukaan organisaation kyberturvallisuus jakautuu ydintoimintoihin kuvion 3 mukaisesti. Uusimassa viitekehyksessä funktiot jakautuvat kategorioihin, jotka ovat kyberturvallisuuden lopputulemia, joita funktioista muodostuu. Alakategoriat puolestaan jakavat kategoriat edelleen tarkempiin yksittäisiin teknisiin ja hallinnollisiin toimintoihin. Mallin avulla voidaan tunnistaa organisaation kannalta olennaisia toimenpiteitä, joita funktion toteuttaminen vaatii (The NIST Cybersecurity Framework (CSF) 2.0 2024).

Toiminnoista ensimmäisenä on esitelty riskien tunnistaminen (eng. identify). Toiminnon olennaisena ideana on kehittää organisaatiollinen ymmärrys, jonka pohjalta kyberriskejä käsitellään järjestelmien, laitteiden, sovelluksien, henkilöstön, datan ja kyvykkyyksien kannalta. Ymmärryksen muodostamisen tueksi Viegasin ja Kuyucun mukaan tulisi kaikkien fyysisten laitteiden ja järjestelmien sekä sovellusalustojen ja applikaatioiden olla listattuna ja säilöttynä, jotta tiedetään mitä tuotteita organisaatiolla on käytössä. Vastaavan listauksen ylläpitäminen helpottaa myös haavoittuvuuden hallintaa, sillä listauksen perusteella voitaisiin suoraan tehdä johtopäätöksiä siitä, löytyykö organisaation käytöstä mahdollisesti haavoittuvia tuotteita perustuen julkaistuun haavoittuvuustietoon (Viegas & Kuyucu 2022).



Kuvio 3: NIST kyberturvallisuuden 2.0 viitekehyksen ydintoiminnot (The NIST Cybersecurity Framework (CSF) 2.0 2024).

Seuraavina ydintoimintoina on mainittu suojaaminen sekä havainnointi. Suojaamisella tarkoitetaan NIST:n viitekehyksen mukaan suojaustoimenpiteiden kehittämistä ja implementointia organisaation kriittisen infrastruktuurin toimivuuden ja saatavuuden takaamiseksi. Suojaamisen toiminnot pitävät sisällään esimerkiksi identiteetin- ja käyttäjänhallinnan kontrollointia, henkilöstön kouluttamisen ja tietoisuuden ylläpitämistä sekä järjestelmiä suojaavien teknologioiden käyttöön-

ottoa ja ylläpitoa. Havainnoinnilla puolestaan tarkoitetaan esiintyvien kybertapahtumien löytämistä järjestelmistä hyväksikäyttäen siihen tarkoitettuja työkaluja ja prosesseja (Viegas & Kuyucu 2022).

Kahtena seuraavana ydintoimintona viitekehyksessä määritellään poikkeamiin vastaaminen ja niistä palautuminen. Poikkeamaan vastaamisella tarkoitetaan viitekehyksen mukaan toimintamallin luomista, jolla varaudutaan aloittamaan toimenpiteet havaitun kyberpoikkeaman vaikutuksien ehkäisemiseksi ja poikkeaman ratkaisemiseksi. Palautuminen puolestaan tarkoittaa poikkeaman aiheuttamien vaikutuksien korjaamista ja järjestelmien palauttamista tilaan, jossa ne olivat ennen poikkeamaa. Vastaavia viitekehyksen osia voidaan myös käyttää pohjana haavoittuvuuden hallinnan prosessia luotaessa tai suunniteltaessa (Viegas & Kuyucu 2022).

Uusimpana ydintoimintona vuonna 2024 julkaistussa viitekehyksessä on muiden ydintoimintojen toteutumisen hallinta, kertovat Dugas ja Sabett. Toiminto pitää sisällään organisaation kyberturvallisuuteen liittyvien riskien hallinnan strategian sekä odotukset ja vaatimukset sille, että kyberturvallisuuteen liittyvät toimintaperiaatteet on otettu käyttöön, kommunikoitu henkilöstölle ja niiden toteutumista valvotaan. Toiminto on kuvion 4 mukaisesti sijoitettu muiden toimintojen sisäkehälle, koska sen tarkoituksena on kertoa, kuinka organisaatio on toteuttanut viisi muuta viitekehyksen toimintoa. Kaikissa ydintoiminnoissa tulisi olla otettuna huomioon myös haavoittuvuuden hallinnan ja tilanneymmärryksen muodostamisen näkökulma (Dugas & Sabett 2024).

Ydintoimintojen lisäksi organisaation tulisi viitekehyksen mukaan tuottaa laadullinen mittaristo kyberriskien hallinnan käytännöistä. Mittaristo perustuu NIST:n riskienhallinnan neliportaiseen asteikkoon, jonka pohjalta arviointia tehdään. Organisaation tulisi valita asteikko kyvykkyyksiensä, tavoitteidensa ja taloudellisen näkökulman perusteella. Organisaation tulisi myös viitekehyksen mukaan profiloida liiketoimintansa vaatimuksia sekä tavoitteita, halua ottaa riskejä ja resurssien osoittamista edellä mainittuihin ydintoimintoihin. Organisaatio voi myös tehdä arvion nykytilanteestaan viitekehykseen verraten ja tehdä arviota puutteista perustuen luotuun arvioon. Organisaation profiilin luomisen vaiheet on esitelty alla olevassa kuviossa. (Viegas & Kuyucu 2022).

Kuvio 4: Organisaation profiilin luomisen vaiheet (The NIST Cybersecurity Framework (CSF) 2.0 2024)

3.3.3 Katakri

Viranomaisten tietoturvallisuuden auditointiin on laadittu työkalu, Katakri, jonka avulla voidaan arvioida organisaation kykyä kansallisen tai kansainvälisen turvallisuusluokitellun tiedon suojaamiseen sekä salassa pidettävien tietojen paljastumisen ehkäisemiseen. Katakri perustuu voimassa olevaan lainsäädäntöön sekä tietoturvallisuusvelvoitteisiin, jotka sitovat Suomea. Katakrin avulla varmistetaan, että auditoitava kokonaisuus täyttää siinä määritellyt vähimmäisvaatimukset. Katakriin peilaten voidaan eri tietojärjestelmille suorittaa toimivaltaisen viranomaisen toimesta tietoturva-auditointeja (Katakri 2020).

Auditoinnin suorittamisen jälkeen Liikenne- ja viestintävirasto voi myöntää hyväksynnän järjestelmälle, jossa käsitellään kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Turvallisuuden tason säilyttämiseen tulee myös sitoutua, sillä hyväksynnän voimassaolo raukeaa, jos hyväksytyssä ympäristössä tapahtuu muutos, joka vaikuttaa merkittävästi sen turvallisuuteen. Tarkastus tulee suorittaa uudelleen myös tapauksessa, jossa järjestelmään tehdään merkittäviä muutoksia tai tuodaan uusia ominaisuuksia (Katakri 2020).

3.4 Liiketoiminnan jatkuvuudenhallinta ja katastrofista palautuminen

Liiketoiminnan jatkuvuudenhallinnalla tarkoitetaan systemaattista prosessia, jonka tavoitteena on riskienhallinnan ja suunnittelun avulla palautua hyväksyttävään palvelutasoon häiriön jälkeen huolimatta siitä, millaisesta poikkeamasta tai tapahtumasta on kyse. Calderin mukaan liiketoiminnan jatkuvuudenhallinnan tavoitteena on varmistaa, että organisaatio selviytyy ennalta-arvaamattomistakin tapahtumista siten, että sen kriittinen liiketoiminta on mahdollisesta palvelualenemastakin huolimatta toiminnassa. Toimivalla prosessilla varmistetaan myös, että liiketoiminnan kriittiset ydintoiminnot jatkuvat häiriöstä huolimatta (Calder 2023).

Myös haavoittuvuuden hyväksikäytöstä alkavasta kyberhyökkäyksestä tai muusta merkittävästä kyberpoikkeamasta voi seurata merkittävä häiriö organisaation liiketoiminnan jatkuvuudelle. Toimivien ja tehokkaiden suunnitelmien laatiminen ennakoitavissa oleville ja ennalta-arvaamattomille skenaarioille on tärkeää, jotta toiminta kyetään käynnistämään häiriön sattuessa. Suunnitelmien toimivuuden varmistamiseksi niiden tulisi olla mahdollisimman selkeitä, luettavia ja ymmärrettäviä. Myös päätöksenteon roolit ja vastuujaot tulee olla selkeästi eriteltynä, jotta taho, joka saa tehdä poikkeavissa tilanteissa ratkaisevia päätöksiä on dokumentoitu. Laadittuja suunnitelmia tulisi myös testata ja kehittää kerättyjen havaintojen perusteella niiden toimivuuden varmistamiseksi tasaisin väliajoin. Jatkuvuudenhallintaan poikkeustilanteessa tehtyjen suunnitelmien tulisi myös olla saatavilla henkilöille tilanteesta huolimatta (Calder 2023).

Sutton toteaa, että liiketoiminnan jatkuvuuden varmistamiseksi kaikissa skenaarioissa tulisi organisaatiolla olla myös suunnitelmia erilaisien katastrofien varalle. Mikäli organisaation IT-järjestelmään kohdistuu merkittävä poikkeama, joka johtaa siihen, että järjestelmän käytettävyys laskee merkittävästi tai lähes kokonaan tulee suunnitelma olla valmiina, jotta palautumisen toimenpiteet voidaan käynnistää. Suunnitelmia tulee myös testata ja päivittää tasaisin väliajoin, jota ne ovat käytettävissä ja ajan tasalla silloin, kun niitä tarvitaan. Harjoittelemalla kehitetään myös organisaation henkilöstön kykyä toimia katastrofin sattuessa (Sutton 2022).

IT-järjestelmien osalta katastrofiin tulee varautua monella tapaa. Suttonin mukaan esimerkiksi järjestelmien monistaminen eri sijainteihin tai varalla olevien kokonaisuuksien toteuttaminen ovat yksi tapa varautua merkittävään poikkeamaan. Mikäli yksittäinen konesali, jossa järjestelmä fyysisesti sijaitsee, tuhoutuu esimerkiksi tulipalon tai luonnonkatastrofin seurauksena, voidaan toinen

identtinen järjestelmä ottaa tuotantokäyttöön toisessa sijainnissa. Toisessa sijainnissa olevan järjestelmän osalta tulee olla tarkka suunnitelma ja sen käyttöönottoa tulee harjoitella, tasaisin väliajoin (Sutton 2022).

Nopea varalla olevan järjestelmän käyttöönotto vaatii kuitenkin useimmissa tapauksissa, että käytöstä poistuneen järjestelmän sisältämä data on replikoitu ja käytettävissä uudessakin sijainnissa. Myös tietoverkkojen sekä reitityksien tulee olla rakennettuna siten, että järjestelmään ja sen palveluihin päästään käsiksi, vaikka varajärjestelmä otettaisiin käyttöön nopeallakin aikataululla. Varalla oleva täysin tuotantojärjestelmää vastaava toteutus, jossa kaikki data on ajantasaista voi kuitenkin olla kallis ylläpidettävä. Organisaation tulisikin arvioida varajärjestelmän ylläpidon kannattavuutta perustuen tuotantojärjestelmän tuottoon ja organisaation liiketoiminnan volyymiin (Sutton 2022).

4 Tietoturvahaavoittuvuudet

Tietoturvahaavoittuvuus määritellään Iso-Britannian kansallisen kyberturvallisuuskeskuksen mukaan heikoksi kohdaksi tai heikkoudeksi IT-järjestelmässä, jonka avulla pahan tahtoinen toimija voi suorittaa onnistuneen hyökkäyksen. Hyökkäys voidaan toteuttaa esimerkiksi käyttäen hyväksi järjestelmän ominaisuutta, vikaa tai loppukäyttäjän tekemää virhettä. Yleisesti hyökkääjän tavoitteena on hyväksikäyttää mitä tahansa sen löytämää mahdollisuutta tunkeutua järjestelmään tai saavuttaa haluttu loppuasetelma, hyväksikäyttäen yhtä tai useampaa eri menetelmää (Understanding Vulnerabilities 2015).

Haavoittuvuuksilla on monenlaisia julkaisijoita, joita voivat olla esimerkiksi normaalit kansalaiset, laitevalmistajat tai sovelluskehittäjät. Haavoittuvuuksia julkaistaessa niihin olisi tärkeää löytyä korjauskeino, kuten korjaava ohjelmistopäivitys tai ohjeet haavoittuvuuden hyväksikäytön rajoittamiseksi. Löydetyistä uusista haavoittuvuuksista onkin aina tärkeää ilmoittaa esimerkiksi oman organisaation tieto- ja kyberturvasta vastaavalle taholle tai kansalliselle kyberturvallisuusviranomaiselle, kuten Suomen tapauksessa Traficomin Kyberturvallisuuskeskukselle. Traficomin mukaan hyvänä periaatteena on, että tunnettuja heikkouksia tai haavoittuvuuksia ei käytettäisi tarpeettoman ongelman todentamisen kannalta hyväksi (Haavoittuvuudet – miten niistä ilmoitetaan oikein 2023).

Haavoittuvuus voidaan myös määrittää tulevaisuuden uhkaksi organisaation turvallisuudelle, kertoo kyberturvallisuusalan yhtiö Check Point (2023) artikkelissaan. Kustannustehokkain tapa haavoittuvuuksien hallintaan on tunnistaa haavoittuvuudet ennen kuin hyökkääjä kerkeää hyväksikäyttämään niitä organisaatioiden järjestelmissä. Mikäli hyökkääjä pääsee hyväksikäyttämään havaitsemaansa haavoittuvuutta IT-järjestelmässä, voivat tapahtuman kustannukset organisaatiolle ja sen asiakkaille nousta merkittäviin rahasummiin. Joissain tapauksissa hyökkääjä saattaa myös vaatia valtavia lunnaita varastamastaan datasta tai kaappaamastaan järjestelmästä tai salata järjestelmän tiedostot ja vaatia lunnaita niiden palauttamiseksi, joka johtaa palvelunalenemaan ja palauttaviin toimenpiteisiin.

4.1 Haavoittuvuuksien variaatiot

Tietoturvayhtiö Crowd Striken (2022) artikkelin mukaan haavoittuvuudet voidaan jakaa useaan yleiseen kategoriaan. Suurimpana uhkana artikkelissa mainitaan järjestelmissä tai sovelluksissa olevat konfiguraatiovirheet, jotka monesti johtuvat ylläpitäjän huolimattomuudesta tai inhimillisestä virheestä. Yksittäinen konfiguraatiovirhe kriittisessä tietoturvakontrollissa tai järjestelmän osassa saattaa antaa mahdollisuuden koko tietojärjestelmän haltuun ottamiselle. Myös sovellusten välisissä konfiguraatiorajapinnoissa (API) olevia tietoturva-aukkoja pidetään merkittävänä hyökkäysvektorina, sillä kyseiset rajapinnat ovat monesti organisaation ainoat ulkoverkkoon näkyvät IP-osoitteet. Mikäli rajapintoja ei ole tarpeeksi hyvin suojattu, muodostavat ne helpon kohteen hyökkääjän hyväksikäytettäväksi (Most Common Types of Cyber Vulnerabilities 2022).

Useasti varsinkin suuremmat IT-järjestelmät pitävät sisällään paljon eri toimittajien tai yhtiöiden valmistamia laitteita ja sovelluksia. Järjestelmän ylläpitäjille muodostuu tällöin helposti paljon työkuormaa, jotta kaikki komponentit saadaan pidettyä ajan tasalla. Monet toimittajat julkaisevat sovellus- ja tietoturvapäivityksiä tiheään tahtiin ja järjestelmään asennettavat päivitykset olisi hyvä validoida ennen tuotantoon vientiä. Tällöin on helposti mahdollista jäädä jälkeen päivityksissä, joka puolestaan jättää järjestelmään mahdollisesti tietoturva-aukkoja hyökkääjän hyväksikäytettäväksi. Tällaisissa tilanteissa tilanneymmärryksen muodostaminen julkaistuista haavoittuvuuksista korostuu, sillä on tärkeää tunnistaa järjestelmän kannalta kriittiset kohteet ja pitää ne ajan tasalla sekä turvattuna päivitysten ja haavoittuvuuksien osalta (Most Common Types of Cyber Vulnerabilities 2022).

Heikot ja yksinkertaiset salasanat ovat Stokel-Walkerin mukaan myös yksi yleisimpiä suureen tietoturvapoikkeamaan johtavia ratkaisukohtia. Yleisen tietoturvan kannalta olennaista on käyttää vahvoja salasanoja ja monivaiheista tunnistautumista (MFA). Samoja tunnuksia ei tulisi kierrättää palvelusta toiselle, vaan jokaiseen kirjautumista vaativaan järjestelmään tulisi käyttää vaihtuvaa ja uniikkia salasanaa. Hyökkääjä pyrkii usein murtamaan heikkoja käyttäjätunnuksia käyttäen väsytyshyökkäystä (eng. brute force), jossa lähetetään kirjautumislomakkeeseen mahdollisimman montaa erilaista vaihtoehtoa käyttäjätunnuksesta ja salasanasta niiden murtamiseksi. Hyökkäyksiin käytettävissä työkaluissa käytetään monesti apuna erilaisia listoja käyttäjätunnuksista ja salasanoista, jotka ovat tunnetusti yleisimmin käytössä olevia tai tietovuotojen myötä päätyneet hyökkääjän käytettäväksi (Stokel-Walker 2023).

Salasanojen arvaamiseen on myös mahdollista käyttää erilaisia generaattoreita, jotka pyrkivät kokeilemaan annetuilla parametreillä mahdollisimman montaa eri vaihtoehtoa kirjautumistunnuksista. Joissain tapauksissa on myös mahdollista, että hyökkääjä on saanut käsiinsä varastettuja kirjautumistunnuksia, joita se voi yrittää hyödyntää järjestelmään murtautumiseen. Onnistuessaan hyökkääjä pääsee käsiksi järjestelmään ja mahdollisesti siinä oleviin tietoihin, asentaa takaovia mahdollistaakseen sisäänpääsyn ja jalansijan usein eri menetelmin sekä kerää tietoa kohdeympäristöstä muiden haavoittuvuuksien ja hyökkäysmenetelmien käyttöä varten (Stokel-Walker 2023).

Käyttöoikeuksien hallinta luokitellaan myös Titteringtonin mukaan merkittäväksi haavoittuvuudeksi. Organisaatioilla on monesti tapana antaa käyttäjilleen suurempia käyttöoikeuksia järjestelmiin, mitä työtehtävien suorittamiseen vaaditaan. Peruskäyttäjällä olevat laajat käyttöoikeudet johtavatkin monesti tilanteeseen, jossa murtaessaan normaalin käyttäjätunnuksen hyökkääjä saakin käyttöönsä mahdollisesti jopa järjestelmä- tai ylläpitäjätason oikeuksia, joita hyväksikäyttämällä se saa suoraan laajemmat mahdollisuudet jatkaa hyökkäystään ja saavuttaa tavoitteensa (Titterington 2024).

Liian laajojen käyttöoikeuksien ongelman korjaamiseen on olemassa menetelmä, jotka kutsutaan minimaalisten käyttöoikeuksien periaatteeksi. Tietoturvayhtiö Kasperskyn blogissa määritellään periaate siten, että käyttäjälle annetaan järjestelmään oikeudet sekä pääsy vain ja ainoastaan niihin entiteetteihin, joita työtehtävien hoitaminen vaatii. Kaikkien uusien käyttöoikeuksien myöntä-

minen tulisi perustua aina tarpeeseen hoitaa tiettyä työtehtävää. Käyttöoikeuksista tulisi myös pitää ajantasaista kirjaa, jotta oikeudet, jotka eivät ole enää relevantteja myös poistettaisiin järkevässä aikaikkunassa (Titterington 2024).

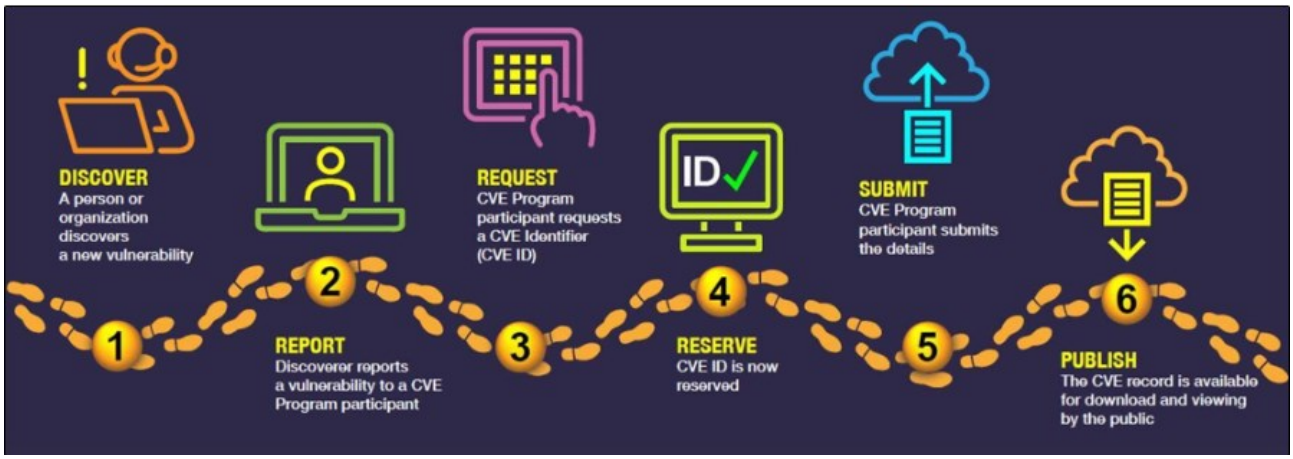
4.1.1 0-päivähaavoittuvuudet

Haavoittuvuuksia, joita ei ole vielä tuotu julki, eikä niille ole tiedossa olevaa tai julkaistua korjauskeinoa kutsutaan 0-päivähaavoittuvuuksiksi. Määritys 0-päivästä tulee Euroopan Unionin kyberturvallisuusviraston Enisan (2022) mukaan digitaalisesta piratismista, jossa nollapäivällä tarkoitetaan tuotetta, joka on saatavilla jostain ennen sen virallista julkaisua. Tietotekniikan osalta puolestaan voidaan määritellä, että 0-päivä viittaa aikaan, joka ohjelmistokehittäjällä on käytettävissä vian korjaamiseen. Monilla kehittyneellä uhkatoimijoilla saattaa olla tiedossaan ohjelmistojen tai sovelluksien haavoittuvuuksia, joita ei ole julkaistu. Tällaisen haavoittuvuuden, jota ei ole julkaistu tai johon ei ole virallista korjausta hyväksikäyttäminen antaa paremman mahdollisuuden onnistuneelle kyberhyökkäykselle tai tietomurrolle.

Yksi tietotekniikka-alan suurimmista ohjelmistotaloista, Microsoft (2022) puolestaan määrittelee omien tuotteidensa osalta 0-päivähaavoittuvuuden sellaiseksi, joihin ei ole olemassa Microsoftin itsensä toimittajana julkaisemaa virallista päivitystä. Periaate haavoittuvuuksien osalta on kuitenkin sama, mutta vaikka muu taho julkaisisi toimivan korjaavan toimenpiteen Microsoftin tuotteessa olevaan haavoittuvuuteen, on se Microsoftin mukaan 0-päivä haavoittuvuus niin kauan, kun sen tuottama virallinen päivitys julkaistaan.

4.2 Haavoittuvuustunnisteet

Haavoittuvuuksien tunnistamiseen ja luettelointiin maailmalla yleisimmin käytetty menetelmä on CVE-tunniste. Jokainen julkisuuteen tuotu haavoittuvuus saa uniikin tunnisteen, jonka perusteella haavoittuvuuksista voidaan tunnistaa sekä luoda niistä kattava katalogi. CVE-tunnisteita uusille löydetyille haavoittuvuuksille saavat myöntää ainoastaan siihen oikeutetut tahot, joille uudet mahdolliset haavoittuvuudet jaetaan arvioitavaksi. Saadakseen CVE-tunnisteen tulee haavoittuvuuden löytäjän laatia ilmoitus, jossa määritellään haavoittuvuuden tyyppi, tuotteen toimittaja ja koodi tai konfiguraatio, johon haavoittuvuus vaikuttaa. Kaikki mahdolliset lisätiedot löydettyyn haavoittuvuuteen liittyen tulee myös toimittaa, jotta esitys todennäköisemmin hyväksytään (Process N.d.).



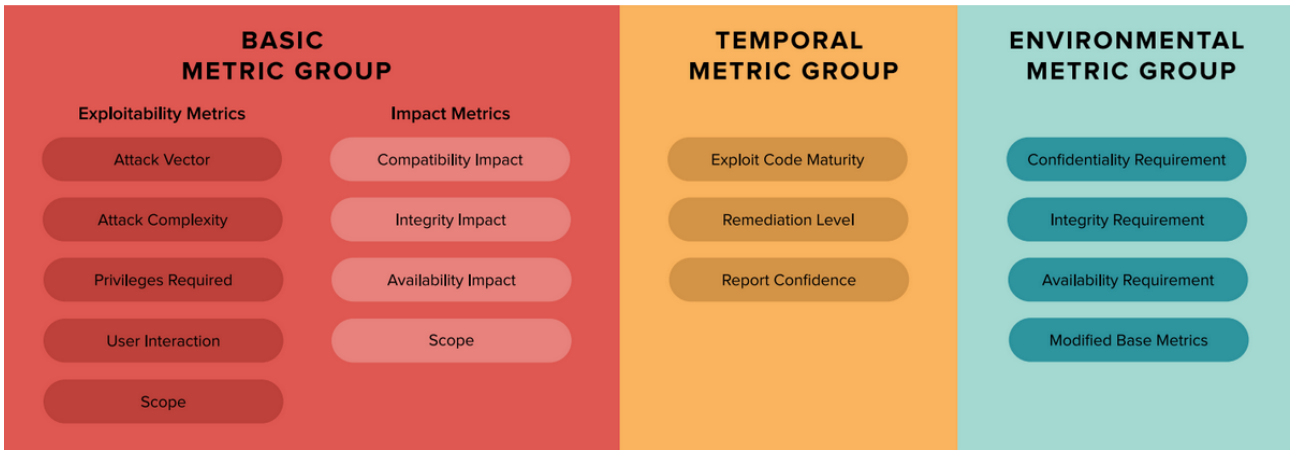
Kuvio 5: CVE-prosessi (Process N.d.)

Joissain tapauksissa laitevalmistajat ja sovellustoimittajat käyttävät haavoittuvuustiedotteissaan omia tunnisteitaan. Tunnisteiden alle on monesti kerätty tietoa esimerkiksi yhteenvedon muodossa tietyn ajanjakson sisään julkaistuista CVE-tunnisteen saaneista haavoittuvuuksista sekä niiden vaikutuksista ja vakavuudesta Esimerkiksi virtualisointiratkaisuja valmistava VMWare (2024) julkaisee omilla verkkosivuillaan tiedotteita, joissa se käyttää omaa nimeämisperustettaan tuotteissaan CVE-tunnisteen saaneiden ja julkaistujen haavoittuvuuksien tiedottamiseksi asiakkailleen ja yhteisölle.

Valmistajien julkaisemat omat tiedotteet saattavat myös sisältää valmistajan itsensä tekemiä arvioita haavoittuvuuksien vakavuudesta ja hyväksikäytettävyydestä sekä tiedon virallisista valmistajan julkaisemista korjaavista ohjelmistopäivityksistä. Valmistajien käyttämät tunnisteet eivät lähtökohtaisesti korvaa CVE-tunnisteen käyttöä, mutta joissain tapauksissa esimerkiksi viranomaisen tekemässä tiedotteessa saatetaan viitata myös valmistajan julkaisemaan tiedotetunnisteeseen.

4.3 Haavoittuvuuksien luokittelu ja arviointi

Haavoittuvuuksien vakavuuden luokitteluun maailmalla yleisimpänä menetelmänä käytetään CVSS-pisteytystä. Haavoittuvuuden pisteytys voidaan tehdä kolmelta eri kannalta, jotka ovat Base (yleinen pohjaluokittelu), Temporal (väliaikainen) ja Environmental (kohdeympäristökohtainen). Yhdysvaltain kansallinen haavoittuvuustietokanta (NVD) tuottaa jokaiselle julkaistulle CVE-tallenteelle Base-luokittelun käyttäen CVSS v2.0 ja v3.x -standardeja, joista uusien julkaistujen haavoittuvuuksien osalta käytetään vain uudempaa v3.x -menetelmää (Vulnerability Metrics 2023).



Kuvio 6: Pisteytykseen vaikuttavat tekijät (What are CVSS Scores 2022)

Haavoittuvuuden pisteytyksen perusteella määritellään sen vakavuus, jonka avulla haavoittuvuus saa vakavuuspisteytyksen väliltä nolla ja kymmenen taulukon 1 mukaisesti. Saadakseen vakavuusarviokseen kriittisen, tulee haavoittuvuuden saada vähintään yhdeksän pistettä. Jos haavoittuvuus ei saa yhtään pistettä, ei sen olemassaololle ole tarpeeksi perusteita. Yleisesti haavoittuvuuksien vakavuudet määritellään alla olevan taulukon mukaisesti. Haavoittuvuuden vakavuuspisteet lasketaan käyttäen avuksi laskuria, jossa määritellään parametrit eri alakategorioiden mukaisesti. Alakategoriat ja pisteytykseen vaikuttavat tekijät on selitetty myöhemmin tässä kappaleessa (Vulnerability Metrics, 2023).

Taulukko 1: CVSS-pisteytys (Vulnerability Metrics 2023)

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

4.3.1 Base-pisteytys

Base-pisteytys antaa hyvän lähtökohdan haavoittuvuuden tulkinnalle, sillä haavoittuvuuden saama base-pisteet eivät lähtökohtaisesti muutu alkuperäisestä, eivätkä ne ole riippuvaisia esimerkiksi

kohdejärjestelmästä. Base-pisteys jaetaan yleisesti kolmen eri kategorian avulla, jotka ovat hyväksikäytettävyys, laajuus ja vaikutus. Jokaiselle julkaistulle haavoittuvuudelle lasketaan base-pisteet julkaisun yhteydessä (Vulnerability Metrics 2023).

Haavoittuvuuden hyväksikäytettävyyttä määritellään käyttäen neljää eri alakategoriaa, joista ensimmäisenä käytetään hyökkäysvektoria. Hyökkäysvektori tässä tapauksessa tarkoittaa haavoittuvuuden hyväksikäyttämiseksi käytössä olevia väyliä tai mahdollisuuksia. Mikäli pisteytettävää haavoittuvuutta on mahdollista hyväksikäyttää etänä, saa se tällöin enemmän pisteitä ja jos haavoittuvuuden hyväksikäyttäminen vaatii fyysisen pääsyn järjestelmään, saa se vähemmän pisteitä (Vulnerability Metrics 2023).

Toinen alakategoria on haavoittuvuuden hyväksikäyttämisen haastavuus. Jos haavoittuvuuden hyödyntäminen ilman merkittävää ylimääräistä työtä on mahdollista, saa se enemmän pisteitä. Mikäli hyökkääjään tarvitsee nähdä huomattavaa ylimääräistä vaivaa hyödyntääkseen haavoittuvuutta, saa se vähemmän pisteitä. Ylimääräinen vaiva voi olla esimerkiksi tunnuksien tai pääsynhallintaan käytettävien avainten varastamista tai muita valmistelevia toimenpiteitä (Vulnerability Metrics 2023).

Kolmas vaikuttava osio ovat käyttöoikeudet, joita hyökkääjä tarvitsee haavoittuvuuden hyväksikäyttämiseen. Järjestelmän pääkäyttäjänä hyväksikäytettävä haavoittuvuus kerryttää lähtökohtaisesti enemmän pisteitä, kuin hyväksikäyttö ilman tunnistautumista. Järjestelmän pääkäyttäjäoikeuksilla hyökkääjä saa käyttöönsä laajemman valikoiman työkaluja, kuin peruskäyttöoikeuksilla. Peruskäyttäjänä hyväksikäytettävällä haavoittuvuudella puolestaan on lähtökohtaisesti pienempi vaikutus (Vulnerability Metrics 2023).

Viimeisenä hyväksikäytettävyyteen vaikuttavana tekijänä on käyttäjältä vaaditut toimenpiteet. Jos hyökkääjä kykenee toimimaan ilman järjestelmän käyttäjän toimia esimerkiksi automatisoiduilla haittaohjelmilla tai -haitallisella koodilla ovat pisteet suuremmat. Mikäli hyökkäys vaatii käyttäjän toimenpiteitä, kuten jonkin tietyn komennon suorittamista tai linkin klikkaamista, saa haavoittuvuus vähemmän pisteitä. Laskurilla pisteitä laskettaessa voidaan valita ainoastaan vaihtoehdot ”vaaditaan”, tai ei ”vaadita” (Vulnerability Metrics 2023).

Laajuutta (eng. scope) puolestaan määritellään esimerkiksi levittäytymisen perusteella. Jos hyökkääjä pystyy vaikuttamaan sovelluksen haavoittuvuutta hyväksikäyttämällä taustalla toimivaan käyttöjärjestelmään tai isäntään, saa haavoittuvuus enemmän pisteitä. Jos haavoittuvuuden hväksi käyttäminen ei mahdollista hyökkääjälle merkittävää pääsyä syvemmälle järjestelmään tai sen toiminnallisuuksiin, saa haavoittuvuus tästä osiosta vähemmän pisteitä (Vulnerability Metrics 2023).

Haavoittuvuuden hyväksikäyttämisestä aiheutuvat vaikutukset määritellään aiemmin opinnäytetyössä määriteltyjen luotettavuuden, saatavuuden ja eheyden mukaisesti. Mitä suurempaan määrän dataa hyökkääjä pääsee käsiksi haavoittuvuuden avulla, sitä enemmän pisteitä haavoittuvuus saa. Mikäli hyökkääjä ei pääse käsiksi mihinkään tietoon, ovat pisteet pienemmät. Jos hyökkääjän on mahdollista päästä muokkaamaan dataa ja täten vaikuttamaan sen eheyteen, kasvavat samalla laskettavat pisteet. Viimeisenä pisteytetään vaikutusta kohteen saatavuuteen. Jos hyökkääjän on mahdollista vaikuttaa kohteessa olevien toimintojen käytettävyyteen tai toimivuuteen, saa haavoittuvuus taas enemmän pisteitä (Vulnerability Metrics 2023).

4.3.2 Temporal-pisteytys

Väliaikaiseen pisteytykseen vaikuttavat muuttuvat tekijät, joita haavoittuvuuteen liittyy. Väliaikainen pisteytys saattaa muuttua ajan kuluessa ja se lasketaan kolmen alakategorian mukaan. Ensimmäisenä alakategoriana on hyväksikäyttökoodin maturiteetti. Maturiteetilla tarkoitetaan julkaistujen hyväksikäyttökoodien toimivuutta. Mitä pitempään haavoittuvuuden julkaisusta on, sitä enemmän sen hyväksikäyttämiseen tarkoitettu menetelmä kehittyy. Kun hyväksikäyttömenetelmä vakiintuu ja tulee laajasti saataville, pisteet nousevat (What are CVSS Scores 2022).

Toisena pisteisiin vaikuttavana tekijänä on saatavilla olevat korjausmenetelmät. Haavoittuvuuden julkaisuajankohtana siihen ei välttämättä ole saatavilla korjaavia toimenpiteitä tai ohjelmistopäivityksiä, jolloin myös väliaikaiset pisteet ovat suuremmat. Ajan myötä, kuin haavoittuvuuteen keksitään korjaavia ratkaisuja tai toimittaja julkaisee virallisen ohjelmistopäivityksen, joka estää haavoittuvuuden hyväksikäyttämisen, pisteet laskevat (What are CVSS Scores 2022).

Viimeisenä väliaikaisiin pisteisiin vaikuttavana kategoriana on raportoidun haavoittuvuuden luotettavuus. Luotettavuuteen tässä tapauksessa vaikuttavat todistusaineistot, jotka todistavat haavoittuvuuden olevan hyväksikäytettävissä, tai ylipäätään olemassa. Mikäli haavoittuvuudelle tai

sen hyväksikäyttämiselle ei ole tarjolla tukevaa materiaalia, ovat pisteet pienemmät. Jos taas haavoittuvuuden hyväksikäytöstä on julkaistu paljon todisteita ja esimerkkejä, ovat pisteet suuremmat (What are CVSS Scores 2022).

4.3.3 Environmental-pisteytys

Kohteen perusteella tehtävä pisteytys lasketaan organisaation näkökulmasta. Organisaatio voi pisteyttää omalta osaltaan haavoittuvuuden esimerkiksi haavoittuvan kohteen kriittisyyden perusteella. Organisaatioiden on mahdollista laskea pisteytys omaan kohdeympäristöön vaikuttavien tekijöiden perusteella, joka auttaa haavoittuvuuden korjaavien toimenpiteiden priorisoinnissa ja kiireellisyyden määrittelyssä sekä yleisen uhkakuvan luomisessa.

Mikäli haavoittuva kohde on organisaation kannalta kriittinen, eli se sisältää esimerkiksi turvaluokiteltua tai salassa pidettävää tietoa, ovat pisteet korkeammat. Jos haavoittuva kohde ei sisällä mitään kriittistä tai salassa pidettävää tietoa, tai sen käytön estäminen ei keskeytä tuotantoa, ei myöskään kohdeympäristökohtainen pisteytys saa tällöin suuria lukemia. Mikäli haavoittuva komponentti sijaitsee esimerkiksi yksittäisessä käyttäjän päätelaitteessa, jolla ei ole mahdollisuutta vaikuttaa muihin ympäristössä oleviin komponentteihin tai edetä esimerkiksi järjestelmänhallintaan, ovat pisteet pienemmät (What are CVSS Scores 2022).

Organisaatio voi myös laskea omakohtaisen CVSS-pisteytyksen perustuen järjestelmässään oleviin haavoittuvuuden hyväksikäyttöä estäviin tai mahdollistaviin yksityiskohtiin. Mikäli kohteeseen ei esimerkiksi ole mahdollista päästä käsiksi ulkoisesta verkosta tai jokin kohde on muutoin eriytetty, voi haavoittuvuuden hyökkäysvektoria koskeva pisteytys laskea alkuperäisestä yleisesti julkaistusta pisteytyksestä (What are CVSS Scores 2022).

4.4 Haavoittuvuuden hallinnan prosessi

Magnussonin mukaan haavoittuvuuden hallinta on käytäntö, jonka kautta muodostetaan tietoisuus ylläpidettävän ympäristön haavoittuvuuksista sekä suoritetaan haavoittuvuuksia korjaavia toimenpiteitä ympäristöön kohdistuvan uhan vähentämiseksi ja kokonaisturvallisuuden parantamiseksi. Haavoittuvuuden hallinta koostuu useista eri osa-alueista, joita toteuttamalla prosessista saadaan jatkuva ja toimiva. Haavoittuvuuden hallinnan elinkaari on jatkuva prosessi, joka koostuu

haavoittuvuusdatan keräämisestä ja sen analysoimisesta. Datan pohjalta tehdyn analyysin perusteella voidaan antaa toimenpidesuosituksia, jotka implementoidaan organisaation ympäristöön haavoittuvuuksien korjaamiseksi ja mahdollisen haitallisen vaikuttavuuden pienentämiseksi (Magnusson 2020).

Haavoittuvuuden hallinnan prosessi itsessään ei kuitenkaan ole todellisuudessa niin yksinkertainen, kuin edellisessä kappaleessa kuvataan. Haavoittuvuuksien löytäminen ja tunnistaminen on yleensä Magnussonin mukaan helppoa, mutta niitä koskevat korjaavat toimenpiteet sekä niiden vaikutuksien arvioiminen puolestaan vievät aikaa ja vaativat pahimmillaan paljon asiantuntijatyötä. Toimivaan haavoittuvuuden hallinnan prosessiin täytyy myös allokoida useita eri rooleja organisaation sisällä sekä ottaa huomioon liiketoiminnan kannalta kriittiset toiminnot ja niiden jatkuvuuden suunnittelu. Haavoittuvuuden hallinta on myös sidottu usein riskien hallintaan, sillä monet haavoittuvuudet ja niihin liittyvät toimenpiteet tulee myös kierrättää riskienhallinnan prosessin kautta varsinkin liiketoimintaan kohdistuvien vaikutuksien ja haittojen arvioinnin osalta (Magnusson 2020).

5 Tilanneymmärryksen muodostaminen

Kappaleessa tarkastellaan kokonaisuuksia, jotka liittyvät haavoittuvuuden hallinnan teknisen tilanneymmärryksen muodostamiseen ja tilannekuvan ylläpitämiseen. Tilanneymmärryksen muodostamisen tueksi kerättiin mahdollisimman paljon aihetta tukevaa haavoittuvuuksiin liittyvää aineistoa, joiden kautta kokonaiskuvan luominen organisaation järjestelmiä koskevan haavoittuvuuden kannalta on mahdollista.

5.1 Haavoittuvuuksien kartoittaminen ja seuranta

Uusia haavoittuvuuksia julkaistaan Gamblinin tilaston mukaan 2020-luvulla jopa useita kymmeniä päivässä. Vuonna 2023 julkaistiin tilaston mukaan 15 % enemmän haavoittuvuuksia, kuin vuonna 2022. Vuonna 2023 julkaistuja haavoittuvuuksia oli 28 902 kappaletta. Olennaisten organisaation järjestelmiä koskevien haavoittuvuuksien löytäminen vaatii paljon työtä ja käsittelyä. Haavoittuvuuksien tunnistamista varten organisaatiolla tulisi olla ajantasaiset tietovirrat, joista se kykenee keräämään mahdollisimman paljon olennaista tietoa haavoittuvuuksista pitääkseen järjestelmänsä ajan tasalla ja turvassa (Gamblin 2024).

5.1.1 Haavoittuvuustiedon kerääminen

Haavoittuvuustiedotteille on olemassa useita olennaista informaatiota sisältäviä lähteitä, joita seuraamalla voi ylläpitää oman organisaation tilannekuvaa maailmalla julkaistuista merkittävistä haavoittuvuuksista. Organisaatioiden haavoittuvuuden hallinnan kannalta on olennaista tunnistaa omaa ympäristöä ja siinä käytössä olevia komponentteja koskevat haavoittuvuudet, jotta niiden kannalta vaaditut toimenpiteet voidaan käynnistää mahdollisimman nopealla aikataululla. Monet sovellus- ja laitevalmistajat pitävät sivustoillaan yllä foorumeita tai blogeja, joissa kerrotaan heidän tuotteistaan löydetyistä haavoittuvuuksista (Haavoittuvuudet – miten niistä ilmoitetaan oikein 2023).

Monet suomalaiset sekä ulkomaalaiset viranomaiset ylläpitävät sivustoja, joihin kootaan merkittävimmät uudet maailmalla löydetyt tai julkaistut haavoittuvuudet. Tällaisesta sivustosta toimii hyvänä esimerkkinä Traficomin Kyberturvallisuuskeskuksen verkkosivuilla oleva haavoittuvuusosio. Haavoittuvuustiedotteiden osalta on olennaista, että niissä kerrotaan haavoittuvien komponenttien versiot, mahdollisesti tarjolla olevat korjaavat ohjelmistopäivitykset sekä tieto siitä, mitä haavoittuvuutta hyväksikäyttämällä voidaan saavuttaa. Myös mahdollisten hyökkäyksien toteutusmahdollisuudet on hyvä olla tiedossa oman kohdeympäristön vaikutuksen arvioimiseksi (Haavoittuvuudet – miten niistä ilmoitetaan oikein 2023).

5.1.2 Konfiguraationhallinta

Ajantasaisen konfiguraatioiden hallinnan myötä järjestelmien ylläpitäjille syntyy parempi käsitys siitä, mitä järjestelmässä tapahtuu ja mitä siinä olevien ohjelmistojen ja komponenttien kuuluisi tehdä. Järjestelmän konfiguraatioiden tulee olla ajantasaiset ja niiden täytyy olla mahdollisimman hyvin suojattu. Calder suosittelee, että konfiguraatioihin pääsy tulisi järjestää ainoastaan järjestelmään muutoksien tekemiseen oikeutetuille rooleille ja konfiguraatioihin kajoamista ilman vaadittavia käyttöoikeuksia tulisi valvoa. Käyttöoikeuksista tulee pitää ajantasaista listaa ja kaikki käyttöoikeudet, joille ei ole tarvetta tulisi poistaa (Calder 2023).

Calder toteaa, että myös kaikki sovellukset, jotka eivät ole tarpeellisia järjestelmän käytön kannalta tulisi poistaa riskien vähentämiseksi. Kun järjestelmässä käytetään mahdollisimman vähän eri

sovelluksia ja komponentteja siten, että vaaditut toiminnallisuudet kyetään suorittamaan, vähenee samalla mahdollisien hyökkäysvektoreiden määrä. Hyökkääjällä on tällöin vähemmän mahdollisia haavoittuvuuksia käytettävissään, jonka myötä erilaisten takaovien ja jalansijojen asentaminen vaikeutuu (Calder 2023).

Myös konfiguraationhallinta on mahdollista automatisoida käyttäen hyväksi siihen tarkoitettuja ohjelmistoja ja tuotteita. Seston mukaan automatisoitu ja tehokas konfiguraationhallinta säästää merkittäviä määriä aikaa ja vähentää myös riskiä mahdollisten inhimillisten virheiden suhteen. Käyttäen ohjelmistoa, joka on tarkoitettu automatisoituun konfiguraatioiden hallintaan, kaikki halutut muutokset ja päivitykset voidaan asentaa järjestelmään pienellä vaivalla, eikä jokaista ohjelmistoa tai yksittäistä konfiguraatiotiedostoa tarvitse erikseen päivittää käsin asiantuntijoiden tai ylläpitäjien toimesta (Sesto 2022).

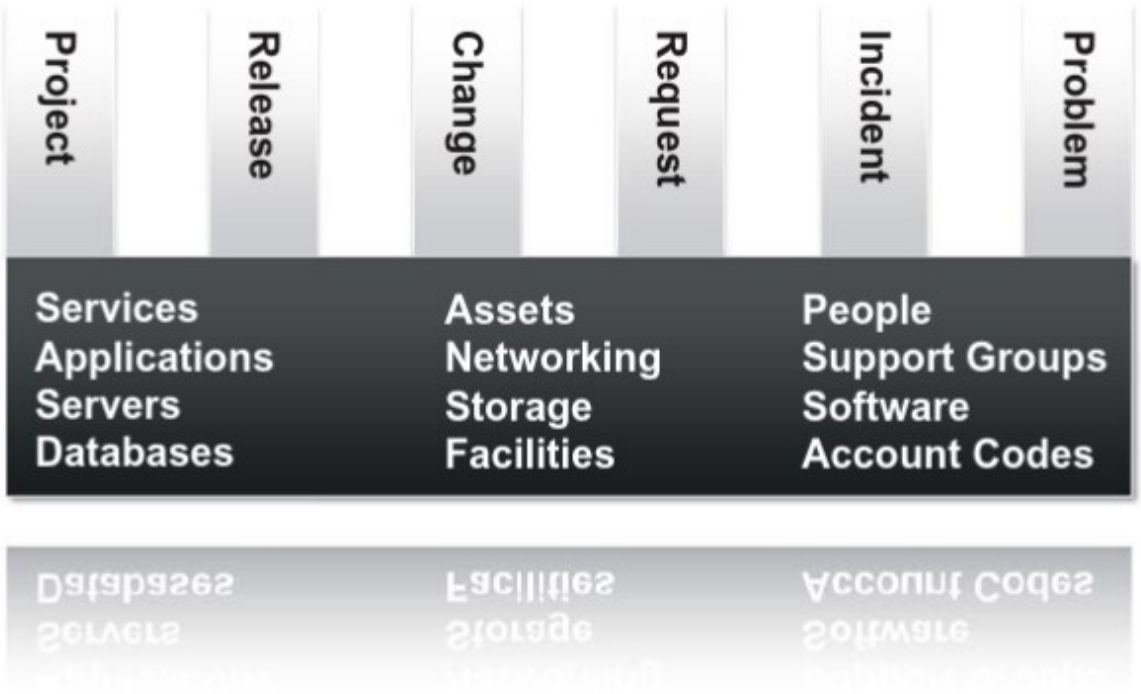
5.1.3 CMDB

Ajantasainen konfiguraationhallinnan tietokanta, eli CMDB on parhaita välineitä organisaation laitteiden, sovellusten, ohjelmistoversioiden ja konfiguraatioiden hallintaan. Drogsethin, Sturmin ja Twingin mukaan CMDB voidaan kuvata kriittisien tietojärjestelmien informaation keskitettynä tietovarastona. Ajantasainen CMDB tarjoaa myös helposti käytettävää dataa monien eri IT-alan prosessien tueksi, kuten kappaleen lopussa olevasta kuviosta voidaan havaita. Lisäksi hyvin toteutettua keskitettyä tietokantaa voidaan käyttää myös muun organisaation kannalta hyödyllisen tiedon, kuten dokumentaation tai henkilöstön tietojen säilömiseen (Drogseth, Sturm & Twing 2015).

CMDB ei ole kuitenkaan ratkaisu kaikkiin IT-alan ongelmiin, ja ajantasaisen tietokannan ylläpitäminen ja tuottaminen voi olla varsinkin isojen IT-ympäristöjen osalta haastavaa. Lisäksi laajaan keskitettyyn tietokantaan liittyy tunnistettavia riskejä, sillä kaiken olennaisen tiedon kohdejärjestelmästä ja sen käytöstä sisältävä kohde on erittäin todennäköisesti yksi järjestelmään mahdollisesti kohdistuvan kyberhyökkäyksen pääkohteista (Drogseth, Sturm & Twing 2015).

Drogseth, Sturm ja Twing toteavat, että CMDB tuo mukanaan huomattavan parannuksen järjestelmän turvallisuuteen ja sisäiseen valvontaan. Haavoittuvuuden hallinnan näkökulmasta hyvin ja kattavasti toteutettu CMDB toimisi hyvänä välineenä haavoittuvien komponenttien kartoittamiseen ja niiden päivittämisen tilannekuvan ylläpitämiseen. Optimaalisessa tilanteessa tietokannasta

voitaisiin nopeasti ja tehokkaasti hakea kaikki versiotiedot julkaistuihin haavoittuvuustiedotteisiin verraten. Tällöin organisaatiossa voitaisiin myös tunnistaa tarve käynnistää korjaavat toimenpiteet tehokkaammin, mikäli tieto haavoittuvista komponenteista on helposti ja keskitetysti saatavilla (Drogseth, Sturm & Twing 2015).



Kuvio 7: CMDB ja IT-prosessit (Drogseth, Sturm & Twing 2015)

5.1.4 Haavoittuvuusskannerit

Tunnettujen haavoittuvuuksien etsimiseen omasta järjestelmästä on tarjolla työkaluja, jotka tekevät sen automatisoidusti, tällaisia työkaluja kutsutaan haavoittuvuusskannereiksi. Haavoittuvuusskannerit keräävät yleisesti kaiken mahdollisen tiedon käyttöjärjestelmästä ja siinä ajettavista palveluista. Skannerille määritellään tarkastettavat kohteet, jonka jälkeen automatisoitu skannaus suoritetaan. Skannauksen aikana skanneri tutkii järjestelmästä määriteltyjä kohteita ja etsii niistä tunnettuja haavoittuvuuksia (Magnusson 2020).

Kun skannaus on valmis, skanneri kirjoittaa tekemistään löydöksistä raportin, joka sisältää tiedot skannatuista kohteista sekä listan tunnetuista haavoittuvuuksista, joita kohteet mahdollisesti sisältävät. Magnusson toteaa, että skannerit käyvät läpi kohteesta löytämiään versiotietoja esimerkiksi sovelluksista tai järjestelmäversioista ja vertaavat niitä omaan haavoittuvuustietokantaansa. Mikäli skanneri havaitsee version, joka on tunnetusti haavoittuva jollekin haavoittuvuudelle, tulee siitä kirjaus raporttiin (Magnusson 2020).

Järjestelmän skannaamisen jälkeen tuotettu raportti kannattaa Magnussonin mukaan analysoida huolellisesti, jotta järjestelmän kannalta olennaiset ja tärkeät korjattavat haavoittuvuudet tunnistetaan. Skannauksen perusteella haavoittuvia kohteita on syytä tutkia ja päivittää ne haavoittuvuudet korjaaviin versioihin. Järjestelmää tulisi myös skannata satunnaisesti tai tasaisin väliajoin, jotta mahdolliset uudet julkaistut haavoittuvuudet ja niiden vaikutukset järjestelmään tulee tarkastettua (Magnusson 2020).

Vaikka haavoittuvuusskannerit ovat tehokas työkalu haavoittuvuuksien löytämiseen järjestelmistä, eivät ne kuitenkaan tarjoa täydellistä suojaa haavoittuvuuksilta. Skanneri tunnistaa ainoastaan järjestelmästä haavoittuvaksi versiot, jotka sen tietokannassa ovat määriteltynä. Skanneri saattaa myös aiheuttaa Magnussonin mukaan virheellisiä tuloksia tapauksessa, jossa jokin versio on luokiteltu haavoittuvaksi ennen tiettyä versiopäivitystä, mutta uuden haavoittuvuuden korjaavan version julkaisun jälkeen haavoittuvuudet on korjattu myös vanhempiin tarjolla oleviin versioihin. Lisäksi skannerin tulee olla laadukas, ajan tasalla ja sisältää tarpeeksi tietoa haavoittuvuuksista, jotta sen antamaa tulosta voidaan pitää luotettavana. Skannereiden kanssa tulee olla myös tarkkana, sillä ne saattavat ajettaessa kuormittaa järjestelmää ja aiheuttaa toiminnallaan joidenkin palveluiden hitautta tai ongelmia niiden käytettävyydessä (Magnusson 2020).

5.2 Tunnistettujen haavoittuvuuksien korjaaminen

5.2.1 Korjaavat ohjelmistopäivitykset ja versionhallinta

Tehokkaimpia tapoja haavoittuvuuden korjaamiseen toimintojen jatkuvuuden kannalta on tarjolla olevan korjaavan ohjelmistopäivityksen asentaminen. Tieto haavoittuvuuden korjaavasta ohjelmistopäivityksestä julkaistaan useimmiten valmistajan verkkosivuilla tai muun tahon laatimassa haavoittuvuustiedotteessa. Mikäli julkaistuun haavoittuvuuteen on tarjolla korjaava päivitys kannattaa

se asentaa tuotantoon mahdollisimman nopeasti, jos haavoittuva komponentti sijaitsee kohteessa, josta sitä on mahdollista suoraan hyväksikäyttää esimerkiksi Internetin yli. Päivitykset kannattaa myös asentaa mahdollisimman nopeasti tapauksessa, jossa haavoittuvuudesta aiheutuu suuri uhka organisaatiolle. Organisaatiolla tulisi myös olla tiedossa ohjelmistoversiot, jotka sen järjestelmissä on käytössä, jotta haavoittuvuuksien vaikuttavuutta käytössä oleviin versioihin voidaan tulkita (Calder 2023).

Calder väittää, että kriittiseksi luokiteltujen tai korkean riskin organisaatiolle aiheuttavien haavoittuvuuksien osalta päivitykset olisi syytä tehdä kahden viikon sisällä julkaisusta, mutta toisaalta mikäli päivitykset on mahdollista suorittaa heti, ei niiden asentamista kannata jäädä odottamaan. Työmäärän vähentämiseksi päivityksien asentaminen tulisi aina automatisoida, mikäli sille on mahdollisuus. Päivitykset kannattaa kuitenkin aina mahdollisuuksien mukaan testata ennen tuotantoympäristöön asentamista siltä varalta, että päivityksen mukana tulevat muutokset estävät tai hankaloittavat jonkin toiminnon suorittamista (Calder 2023).

Korjaavien ohjelmistopäivityksien nopea vieminen tuotantoon sisältää kuitenkin riskejä ja saattaa aiheuttaa haittaa kohdejärjestelmän toiminnoille. Sovelluksen tai järjestelmän päivittäminen saattaa tuoda muutoksia toimintoihin, joka saattaa puolestaan estää tai haitata jonkin kriittisen toiminnon käytettävyyttä. Mikäli mahdollista Calder toteaa, että päivitykset kannattaisi testata tuotantoympäristöä vastaavassa hiekkalaatikossa ja todentaa niiden toimivuus. Myös päivityksien mukana tulevat ohjeet ja dokumentaatiot tulisi Calderin mukaan käydä läpi ennen kuin päivityksiä aletaan asentamaan (Calder 2023)

5.2.2 Haavoittuvuuden hyväksikäyttöä rajoittavat toimenpiteet

Mikäli julkaistuun haavoittuvuuteen ei ole suoraan saatavilla korjaavaa ohjelmistopäivitystä on mahdollista, että valmistaja tai muu taho on julkaissut haavoittuvuuden hyväksikäyttöä rajaavia toimenpiteitä tai konfiguraatiomuutoksia. Toteuttamalla suositellut toimivaksi todetut muutokset komponentteihin voidaan ehkäistä julkaistun haavoittuvuuden hyväksikäyttöä. Väliaikaiset korjaustoimenpiteet eivät kuitenkaan suurimmassa osassa tapauksista ole lopullinen toimenpide, joka korjaa haavoittuvuuden. Korjaavien tai rajoittavien toimenpiteiden tarkoitus on ehkäistä haavoittuvuuden hyväksikäyttöä, kunnes virallinen korjaava ohjelmistopäivitys julkaistaan asennettavaksi (Calder 2023).

Järjestelmiin tehdyt korjaavat toimenpiteet on aina syytä dokumentoida, jotta tiedetään mitä muutoksia on tehty. Joissain tapauksissa korjaavan toimenpiteen suorittaminen saattaa aiheuttaa ongelmia tai rajoitteita organisaation tuottaman palvelun saatavuuteen. Kun haavoittuvuuden korjaava ohjelmistopäivitys on julkaistu ja viety tuotantoon, kannattaa organisaation tekemiä haavoittuvuuden hyväksikäyttöä rajaavia toimenpiteitä tarkastella kriittisesti ja tarvittaessa palauttaa ne tilaan, jossa palvelu toimii jälleen normaalisti, mikäli korjaavan ohjelmistopäivityksen asentamisen jälkeen tehdyt muutokset voidaan kumota (Calder 2023).

5.3 Haavoittuvuuksien priorisointi ja vakavuuden arviointi

Haavoittuvuustietoja tulisi arvioida ja analysoida kohdeympäristöön perustuen. Magnussonin mukaan haavoittuvuusskannerin tuottama raportti saattaa suuressa ympäristössä löytää valtavan määrän erilaisia haavoittuvuuksia, mutta tärkeiden haavoittuvuuksien erottaminen vähemmän tärkeistä voi olla vaikeaa. Järjestelmässä olevia haavoittuvuuksia voi lähteä arvioimaan esimerkiksi hyväksikäytettävyyden, kriittisyyden tai julkaistujen hyväksikäyttömenetelmien perusteella. Mikäli haavoittuvuus täyttää arvioinnin kriteerit kannattaa sen korjaaminen suorittaa mahdollisimman pian, mutta mikäli haavoittuvuus ei aiheuta merkittävää vaaraa ympäristölle, voi sen korjaamisen priorisoida matalammaksi (Magnusson 2020).

Magnusson toteaa, että mikäli järjestelmästä löytyy paljon haavoittuvuuksia, niiden pisteyttäminen ja listaaminen kriittisyysjärjestykseen on myös hyvä keino priorisoida korjaavia toimenpiteitä. Kriittisyyttä voidaan arvioida esimerkiksi vaikutuksilla luottamuksellisuuteen, eheyteen ja saatavuuteen tai pisteyttämällä ne käyttäen hyväksi ulkoista pisteytysmenetelmää, kuten CVSS-laskuria. Myös järjestelmän toiminnan kannalta kriittisistä kohteista löydettyjä haavoittuvuuksia voidaan priorisoida korkeammalle, kuin haavoittuvuuksia, jotka eivät vaaranna järjestelmän toimintaa. Eniten kriittisten haavoittuvuuksien löytämisen jälkeen voidaan vähemmän kriittiset haavoittuvuudet arvioida ja päättää niiden kanssa menettelystä (Magnusson 2020).

5.3.1 Julkinen vs. suljettu ympäristö

Uhkatoimijat pyrkivät monesti hyödyntämään hyökkäyksissään julkiseen verkkoon kytkettyjä palveluita tai järjestelmiä. Tällaiseen kohteeseen hyökkääminen ei välttämättä vaadi fyysistä pääsyä

laitteelle tai laajempaa ymmärrystä sen takana olevasta ympäristöstä, yksikin etäkäytettävä haavoittuvuus saattaa riittää järjestelmään murtautumiseen. Yleisesti tavoitteena on käyttää tällaista palvelua tai järjestelmää hyökkäyksen ensimmäisen jalansijan saamiseksi, jonka jälkeen hyökkääjä voi jatkaa etenemistään edelleen muihin kohteisiin.

MITRE:n mukaan uhriksi päätyvät kohteet ovat yleensä verkkosivuja tai -palvelimia, mutta joukossa saattaa olla muitakin kohteita, kuten tietokantoja tai ylläpitoon käytettäviä sovelluksia tai protokollia. Myös pilvipalvelussa tai konttiteknologian päällä toimivaan sovellukseen hyökkääminen on mahdollista ja saattaa johtaa tilanteeseen, jossa hyökkääjä kykenee sen avulla murtautumaan alustaan tai konttiin, jossa sovellus isännöidään. Julkisessa verkossa olevia haavoittuvia kohteita voidaan myös kartoittaa käyttämällä siihen tarkoitettuja työkaluja tai palveluita. Julkisesta verkosta löytyvään haavoittuvaan kohteeseen hyökkääminen ei välttämättä ole myöskään aina kohdennettua, vaan kohde saattaa valikoitua haavoittuvuuksien hyväksikäytettävyyden helppouden perusteella (Exploit Public-Facing Application 2023).

Uhkatoimijat voivat myös käyttää järjestelmiin murtautumiseen etäkäyttöpalveluita, kuten VPN-sovelluksia tai alustoja, joista palveluita tarjotaan. Varastetuilla tai muuta kautta haltuun saaduilla käyttäjätunnuksilla hyökkääjä voi mahdollistaa itselleen pääsyn muodostamalla yhteyden palveluita tarjoavaan verkkoon tai alustaan. Myös etäkäyttöpalvelussa olevan haavoittuvuuden hyväksikäyttö saattaa johtaa järjestelmään murtautumiseen. Esimerkiksi monet yritykset tai oppilaitokset saattavat mahdollistaa työntekijöilleen tai opiskelijoilleen mahdollisuuden käyttää sisäisiä palveluitaan etänä hyödyntäen VPN-ratkaisua. Lisäksi järjestelmiin pääsy on mahdollista muodostaa esimerkiksi tietojenkalastelusähköpostin kautta levitettävällä tai verkosta ladattavalla haittaohjelmalla (External Remote Services 2023).

Mikäli hyökkääjä kykenee murtautumaan organisaation sisäiseen verkkoon hyväksikäyttämällä etäkäyttöpalvelua, haavoittuvuutta tai julkiseen verkkoon kytkettyä kohdetta, hyökkääjän todennäköisenä seuraavana tavoitteena on tunkeutuminen syvemmälle järjestelmään. Hyökkääjän toisena todennäköisenä tavoitteena on myös yhteyden muodostaminen etänä olevaan komentopalvelimeen tai kohteeseen. Murtautumisen jälkeisien toimenpiteiden toteuttaminen, kuten datan

kuljettaminen ulos järjestelmästä tai kiristyshaittaohjelman asentaminen saattaa vaatia vielä sivuttaissiirtymistä järjestelmän sisällä tai käyttöoikeuksien korottamista vaadittujen toimenpiteiden suorittamiseksi (Exploitation of Remote Services 2022).

On myös olemassa suljettuja järjestelmiä, joihin ei ole lähtökohtaisesti mahdollista päästä käsiksi julkisesta verkosta tai etäyhteyssovelluksen kautta. Tällaiseen suljettuun järjestelmään hyökkääminen on hankalaa, mutta mahdollista. Lähes poikkeuksetta kaikkiin järjestelmiin tuodaan jotain tietoa ulkopuolelta kuten kuvia, dokumentteja, päivityksiä ja ohjelmistoja. Myös ulkoisia muistivälineitä saatetaan käyttää normaalin järjestelmän käytön yhteydessä. Edellä mainitut tavat mahdollistavat järjestelmiin vaikuttamisen esimerkiksi toimitusketjun tai haitallista koodia sisältävän tiedoston kautta. Haittaohjelman vieminen suljettuun järjestelmään on myös mahdollista matkapuhelimen tai muun mobiililaitteen kautta, mikäli laite kytketään järjestelmään tai työasemaan kiinni USB-kaapelilla (Replication Through Removable Media 2023).

5.4 Korjaavat toimenpiteet ja päätöksenteko

Tilanteessa, jossa organisaation ympäristössä havaitaan kriittinen nopeita toimenpiteitä vaativa haavoittuvuus, joka koskettaa monia kohdeympäristön komponentteja tulee helposti vastaan tilanne, jossa yksittäisen ylläpitäjän tai järjestelmävastaavan mandaatti ei riitä päättämään järjestelmien pikaisesta päivittämisestä. Joissain tapauksissa isojen tuotantoympäristöjen päivittäminen saattaa viedä valtavasti aikaa ja aiheuttaa isoja kustannuksia, jos järjestelmät ajetaan alas päivittämisen ajaksi.

Kappaleessa perehdytään korjaavista- sekä muutoksenhallinnan toimenpiteistä päättämiseen ja niistä mahdollisesti aiheutuviin taloudellisiin haittoihin sekä päätöksenteon prosessiin. Kappaleen tarkoituksena on tunnistaa päätöksenteon roolit sekä tilanteet, joissa nopealla aikataululla toteutettavan hätämuutoksen käskeminen on järkevin vaihtoehto järjestelmien turvaamiseksi tavallisen päivityssyklin sijaan.

5.4.1 Jatkuva prosessi vai hätämuutos?

ITIL määrittelee palvelunhallinnan organisaatiollisiksi kyvykkyyksiksi, joilla tuotetaan asiakkaalle arvoa palveluiden muodossa. Puolestaan organisaation tarkoituksena on tuoda arvoa sidosryhmille. Mikäli organisaation asiakkaalle tai sidosryhmälle tuottamat palvelut ovat alhaalla, siitä saattaa aiheutua taloudellista tai maineellista haittaa. Organisaation tulisi kaikissa tilanteissa kyetä tarjoamaan jatkuvia sekä turvallisia palveluita asiakkailleen, jotta toiminta pysyy kannattavana. Lisäksi ITIL kertoo, että tietoturvakontrollien ei myöskään pidä olla liian tiukalla, jotteivat ne haittaa merkittävästi työn tuloksellisuutta. Organisaation järjestelmien turvaamisen ja innovaation välille tulisikin löytää järkevä balanssi (ITIL foundation : ITIL 4 edition 2019).

Mikäli julkaistu haavoittuvuus aiheuttaa merkittävää ja akuuttia vaaraa organisaation palveluille, voidaan ongelman korjaamiseksi joutua suorittamaan hätämuutos, jolla haavoittuvat palvelut päivitetään tai suojataan välittömästi haavoittuvuuden hyväksikäyttöä rajoittavilla toimenpiteillä. Suoritettaviin toimenpiteisiin liittyy aina riskejä, mikäli ne tehdään hätämuutoksena suoraan tuotantoympäristöön. Joissain tapauksissa haavoittuvuuden korjaamiseksi vaadittavat toimenpiteet, kuten päivittäminen tai konfiguraatiomuutos saattavat aiheuttaa aleneman tuotettavissa palveluissa (ITIL foundation : ITIL 4 edition 2019).

5.5 Päätöksenteon roolit ja prosessi

Organisaation toiminnan jatkuvuuden kannalta päivityksien tuotantoon viemiselle tulisi olla toimiva prosessi. Prosessissa tulisi olla huomioituna normaalin päivityksien hallinnan lisäksi optio hätämuutoksen suorittamiselle ja sen vaiheille. Hätämuutoksen tekeminen vaatii myös aina päätöksentekoa organisaation sisällä, joten päätöksistä vastaava taho kannattaa olla määriteltynä prosessissa (ITIL foundation : ITIL 4 edition 2019).

5.5.1 Muutosvastaava ja muutoskomitea

Muutosvastaavalla henkilöllä (eng. Change Manager) on vastuullaan palveluiden ja järjestelmien muutoksista päättäminen. Muutokset tulee Wattsin mukaan suunnitella siten, että niistä aiheutuu mahdollisimman pieni katkos tuotettavaan IT-palveluun. Muutoksien elinkaaren hallinta kuuluu myös muutosvastaavalle, koska hän toimii tyypillisesti muutoskomitean (eng. Change Advisory Board) johtajana. Muutoskomitean tehtävänä on tuottaa tarvittavat tiedot muutosvastaavalle,

jotta hän kykenee priorisoimaan, aikatauluttamaan ja määrittelemään tehtävät muutokset (Watts 2019).

Muutosvastaavalla on mandaatti antaa lupa suunnitellun muutostyön aloittamiselle. Watts toteaa, että prosessi kokonaisuudessaan muutoksien hallitsemisessa ja muutosehdotuksien hyväksymisessä vie paljon aikaa, sillä kaikki tarvittava tieto tulee kerätä ja analysoida, jotta muutos voidaan toteuttaa. Prosessin toteutumista tulee myös seurata tarkasti, jotta muutoksesta aiheutuu mahdollisimman vähän keskeytystä järjestelmän toiminnalle. Mahdollisimman lyhyellä keskeytysajalla myös muutoksesta aiheutuvat kustannukset pienenevät ja jatkuvat liiketoiminnat (Watts 2019).

Normaalit ja suunnitellut muutokset kyetään toteuttamaan edellä kuvatun mukaisesti, mutta joissain tapauksissa hätämuutos on ainoa vaihtoehto, jotta maksimaalinen suorituskyky voidaan saavuttaa. Hätämuutoksista päättämiseen muodostetaan hätämuutoskomitea (eng. Emergency Change Advisory Board), joka on muutoskomitean alaryhmä. Hätämuutoskomitean on toimittava paljon tiukemmissa aikamääreissä, kuin muutoskomitean. Hätämuutoskomiteassa tehdyt päätökset perustuvat riskien minimoimiseen ja riskiarvion tekemiseen mahdollisimman lyhyessä ajassa. Muutoksen luonteen ja tärkeyden määritteleminen on ensimmäinen tehtävä päätettäessä, eskaloidaanko muutoksesta päättäminen hätämuutoskomitealle. Mikäli muutosta ei tarvitse suorittaa hätämuutoksena, siirretään sen käsittely suoraan muutoskomitealle (Watts 2019).

Kun muutos päätetään tehdä hätämuutoksena, työt täytyy aloittaa välittömästi päätöksenteon jälkeen. Tarvittaessa muutokset voidaan testata ennen tuotantoon vientiä hätätilanteessakin, mikäli sille on aikaa. Päätöksenteon rooli korostuu päätettäessä hätämuutoksien etenemisestä, hätämuutoskomitea ja muutosvastaava tekevät päätöksen muutostöiden etenemisestä parhaaksi katsomallaan tavalla. Hätämuutoksen epäonnistuessa tulee toimenpiteet aloittaa alusta, mutta onnistuessaan hätämuutos voidaan merkitä suoritetuksi, mikäli juurisyy saadaan korjattua. Prosessi hätämuutoksen suorittamiselle voidaan parhaillaan viedä läpi tunneissa, mutta päätöksentekoon liittyvä aika- ja suorituspaine voivat vaihdella tilanteen mukaan (Watts 2019).

Onnistuneen hätämuutoksen tärkeimpiä elementtejä on ajanhallinta. Hätämuutoskomitean tulee tehdä nopeat johtopäätökset tilanteesta ja määritellä aikaikkuna, jossa muutos on suoritettava.

Hätämuutoskomitean tehtävänä on minimoida riskejä ja estää tapahtumaa aiheuttamasta ylimääräistä haittaa kohdejärjestelmälle. Liian hätäiset päätökset tai lyhyet aikaikkunat voivat kuitenkin johtaa suurempaan tuhoon tai ylimääräisen ajan tuhlaamiseen muutoksen epäonnistuessa. Toisaalta muutoksen siirtäminen myöhemmäksi saattaa aiheuttaa palvelunaleneman tai jättää järjestelmän haavoittuvaksi liian pitkäksi aikaa (Watts 2019).

5.5.2 Tietoturvajohtaja ja tietohallintojohtaja

Tietoturvajohtaja (eng. CISO) on yleisesti käytössä oleva titteli kokeneelle johtohenkilölle, jonka toimenkuvaan kuuluu organisaation tietoturvallisuuden hallinta ja varmistaminen. Tyypillisiin tietoturvajohtajan tehtäviin kuuluu uusien ja käytettävien tietoturvateknologioiden implementointi sekä määritteleminen. Tietoturvajohtajan vastuulla on monesti myös fyysisen sekä loogisen pääsynhallinnan toteutus niin työntekijöiden ja urakoitsijoiden, kuin vieraidenkin osalta. Tietoturvajohtajan rooli pitää sisällään paljon vastuuta, sillä roolissa työskentelevä henkilö usein vastaa organisaation datan tietoturvallisesta hallinnasta ja sen turvallisuuden varmistamisesta (Kouns & Kouns 2023).

Tietoturvajohtaja työskentelee usein osana erilaisia työryhmiä, kuten muutoskomitea, hätämuutoskomitea tai tekninen johtoryhmä. Työryhmissä tietoturvajohtajan tehtävänä on tuoda esiin tietoturvallisuuden näkökulmaa ja arvioida muutoksen tai päivityksen aiheuttamaa riskiä tietoturvalle. Muutoksien tietoturvallisuuden varmistamisesta huolimatta järjestelmien täytyy säilyä käytettävinä ja saatavilla ja suunnitellut turvallisuustoimenpiteet eivät saa aiheuttaa merkittävää haittaa kohdejärjestelmälle (Kouns & Kouns 2023).

Tietoturvajohtaja on yleisesti raportointivelvollinen tietohallintojohtajalle (eng. CIO), jonka tehtäviin kuuluu yleisesti koko IT-infrastruktuurista vastaaminen ja sen hankkiminen sekä ylläpitämisen ja kehittämisen suunnittelu. Tietohallintojohtaja vastaa myös monesti organisaation tieto- ja viestintätekniikan strategioista sekä resurssien hallinnasta sekä valvoo IT-järjestelmien turvallisen käytön toteutumista. Tietohallintojohtaja kuuluu myös monesti organisaation johtoryhmään ja vastaa suoraan joko pääjohtajalle tai talousjohtajalle ja tehtävään liittyy paljon taloudellista vastuuta, koska tietohallintojohtaja vastaa myös järjestelmien käytettävyydestä ja saatavuudesta (Kouns & Kouns 2023).

5.6 Haavoittuvuuksien hyväksikäytön havaitseminen

Tässä kappaleessa tarkastellaan haavoittuvuuksien hyväksikäyttämistä ja sitä, kuinka julkisista lähteistä on saatavilla tietoa maailmalla hyväksikäytettyjen haavoittuvuuksien osalta. Maailmalla vallitsevien trendien ja ilmiöiden seuraaminen liittyen erilaisten haavoittuvuuksien hyväksikäyttöön on hyödyllistä tietoa oman organisaation haavoittuvuuden hallinnan tilannekuvan kannalta. Aiemmin organisaatiossa matalalle prioriteetille luokiteltu haavoittuvuus saattaakin muodostua kriittiseksi uhaksi, mikäli siihen liittyen julkaistaan uutta tietoa tai uusia tapoja sen hyväksikäyttämiseen.

5.6.1 Haavoittuvuuksien aktiivinen hyväksikäyttö ja julkaistut hyväksikäyttömenetelmät

Hyväksikäytettävyydellä tarkoitetaan haavoittuvuuden kannalta sitä, kuinka helposti hyökkääjän on mahdollista käyttää julkaistua haavoittuvuutta hyökkäyksissään. Määrittelyyn vaikuttavia asioita ovat esimerkiksi julkisen hyväksikäyttömenetelmän saatavuus, järjestelmän saavutettavuus julkisen verkon yli, mahdollisuus päästä sisään järjestelmään ilman lupaa ja yleinen taitotaso, jota haavoittuvuuden hyväksikäyttö vaatii. Yhdysvaltain kyberturvallisuusviranomaisen CISA:n mukaan aktiiviseksi hyväksikäytöksi määritellään tapahtuma, jossa on näyttöä siitä, että haitallista koodia on suoritettu järjestelmässä ilman omistajan lupaa. (Reducing the Significant Risk of Known Exploited Vulnerabilities 2024).

Hyväksikäyttömenetelmällä (PoC) puolestaan tarkoitetaan koodia, jonka suorittamalla haavoittuvuuden hyväksikäyttäminen todistetusti onnistuu. Hyväksikäyttöön tarkoitettua koodia voidaan myös käyttää tutkijoiden ja toimittajien apuna haavoittuvuuden korjaamiseen sekä oman organisaation asiantuntijoiden työn tukena poikkeavien tapahtumien havaitsemiseen. Mikäli hyväksikäyttömenetelmä päätyy julkiseen jakoon, johtaa se erittäin todennäköisesti kyseisen haavoittuvuuden hyväksikäyttöjen määrän lisääntymiseen maailmalla. Julkaistu hyväksikäyttömenetelmä ei myöskään ole tae sille, että haavoittuvuutta tullaan hyväksikäyttämään tai on jo hyväksikäytetty (Reducing the Significant Risk of Known Exploited Vulnerabilities 2024).

CISA ylläpitää yhtenä tuotteenaan KEV-katalogia, jossa se raportoi tiedossa olevista maailmalla aktiivisesti hyväksikäytetyistä haavoittuvuuksista. CISA:n mukaan katalogin tarkoituksena on lähettää

selkeä viesti kaikille organisaatioille haavoittuvuuksia korjaavien liikkeiden tekemiseksi. Jotta haavoittuvuus lisätään katalogiin, täytyy sen täyttää vaaditut kriteerit, joita ovat olemassa oleva haavoittuvuuden CVE-tunniste, haavoittuvuuden aktiivinen hyväksikäyttö maailmalla ja selkeät ohjeet korjaustoimenpiteistä. KEV-katalogin tapauksessa aktiiviseksi hyväksikäytöksi lasketaan haavoittuvuuden hyväksikäytön todennetut yritykset tai haavoittuvuuden onnistuneet hyväksikäytöt (Reducing the Significant Risk of Known Exploited Vulnerabilities 2024).

5.6.2 Hyväksikäytön havaitseminen uhka- ja hyökkäystunnisteiden avulla

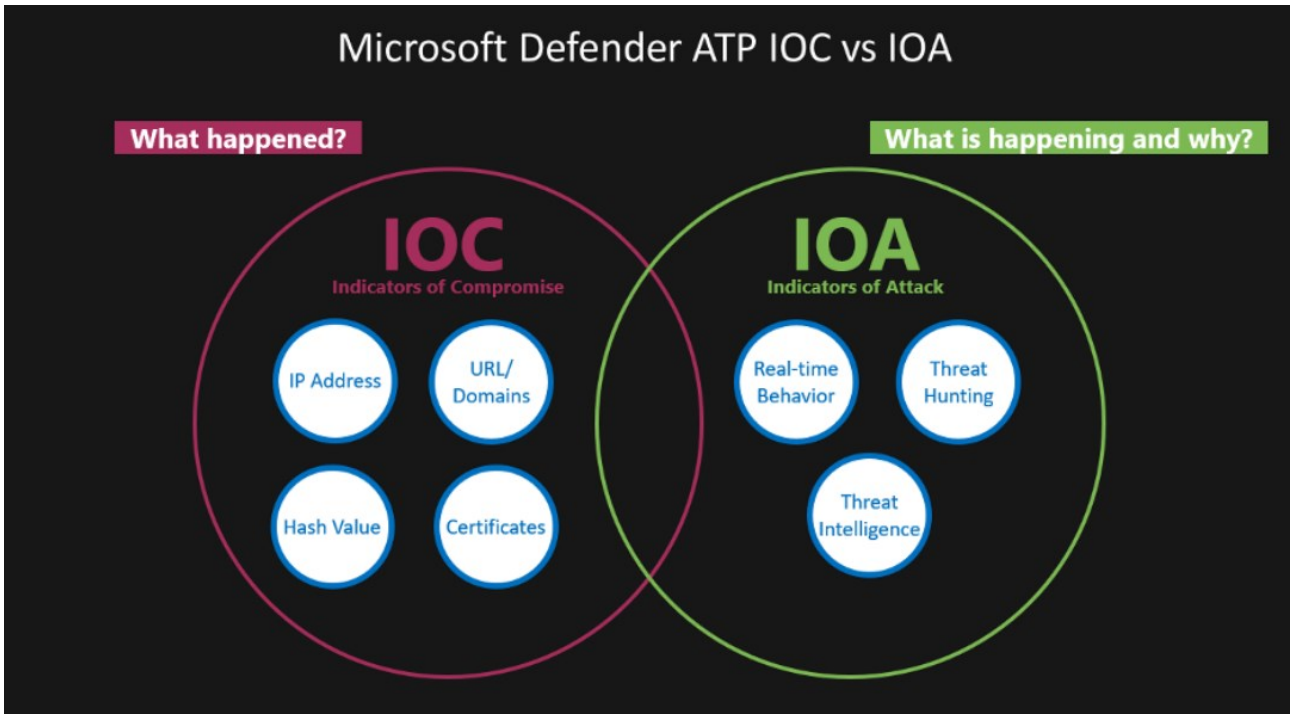
Termillä uhkatunniste (IOC) tarkoitetaan Onyegbulan mukaan merkkejä tai tunnistetietoja toiminnasta, jotka viittaavat tietomurtoon, kyberhyökkäykseen tai järjestelmään tunkeutumiseen. Uhkatunnisteet voidaan jakaa useisiin eri kategorioihin. Esimerkkejä suosituista kategorioista Onyegbulan (2023) mukaan ovat verkkoliikenteeseen, tiedostoihin ja käyttäytymiseen perustuvat uhkatunnisteet. Hasayan toteaa, että uhkatunnisteilla voidaan evästää olemassa olevia tietoturvatyökaluja, jotta niiden avulla päästäisiin tehokkaammin jyvälle uusista haitallisista tapahtumista. Uhkatunnisteiksi voidaan Hasayanin mukaan laskea esimerkiksi haitalliseksi tunnistetut IP-osoitteet, tiivistesummat sekä tiedostojen nimet, kuten myös luvun lopussa olevasta kuviosta havaitaan. (Hasayan 2022).

Sekä Onyegbula (2023) että Hasayan (2022) väittävät, että tunnistetietojen ilmaantuminen viittaa aina johonkin haavoittuvuuteen järjestelmässä. Toisaalta täysin suojattuunkin järjestelmään on mahdollista yrittää hyökätä käyttäen samoja tekniikoita tai haittaohjelmia, joilla on onnistuttu murtautumaan johonkin toiseen järjestelmään. Tällöin epäonnistuneeseenkin kyberhyökkäykseen viittaavia tunnistetietoja voidaan havaita lokitiedoista. Myös tunnetussa tietojenkalastelusähköpostista oleva haitallinen linkki voi olla uhkatunniste, mutta se ei tarkoita onnistunutta tietomurtoa, jollei sitä aktivoida. Uhkatunnisteita voidaan käyttää sekä järjestelmässä olemassa olevien toimijoiden tai uhkien etsimiseen että uusien hyökkäysten tai epänormaalien tapahtumien havaitsemiseen (Onyegbula 2023).

Meneillään olevien kyberhyökkäysten tunnisteista käytetään Onyegbulan (2023) mukaan termiä IOA (Indicator of Attack). Tunnisteiden avulla tunnistetaan tekniikoita, taktiikoita ja työkaluja, joita hyökkäyksessä käytetään ja voidaan tehdä arvioita siitä, mihin hyökkääjä toimillaan pyrkii. Puoles-

taan Hasayanin mukaan IOA-tunnisteilla vastataan kysymykseen: ”Mitä tapahtuu ja miksi?”. Aiemmin tässä luvussa ollut esimerkki tietojenkalastelusähköpostista, joka sisältää haitallisen linkin sisältää uhkatunnisteita, jotka viittaavat teknisin yksityiskohtiin, kuten linkkiin itsessään. Puolestaan, jos käyttäjä aktivoi haitallisen linkin, joka tarjoaa hyökkääjälle mahdollisuuden tunkeutua järjestelmään ja aktiivinen kyberhyökkäys alkaa, määritellään hyökkäyksen aikana havaitut tunnisteet IOA-tunnisteiksi. Hyökkääjän toimiin viittaavia tunnisteita voivat olla esimerkiksi jalansijan ylläpitäminen järjestelmässä, yhteyden muodostaminen ulkoiseen komentopalvelimeen tai datan siirtäminen ulos järjestelmästä (Hasayan 2022).

Myös todennetuista haavoittuvuuksien hyväksikäytöistä julkaistaan havainnon tekijän toimesta monesti uhkatunnisteita, joiden perusteella organisaatio voi etsiä järjestelmästään merkkejä onnistuneesta hyväksikäytöstä tai. Menetelmästä käytetään termiä uhkanmetsästys (eng. threat hunting), joka myös yleisesti tarkoittaa jo olemassa olevien uhkien etsimistä järjestelmistä. Julkaistuja uhkatunnisteita voidaan myös käyttää järjestelmässä tunnistettujen haavoittuvuuksien hyväksikäytön havaitsemiseen (Hasayan 2022).



Kuvio 8: IOC vs IOA (Hasayan 2022).

Parhaita tapoja havaita järjestelmään kohdistuvia haavoittuvuuksien hyväksikäytön yrityksiä tai kyberhyökkäyksiä uhkatunnisteiden avulla on suorittaa reaaliaikaista kybervalvontaa ja ylläpitää ajantasaisia tietoturvakontrolleja, kuten virustorjuntaa. Calder toteaa, että tapahtuvasta tietoturvaloukkauksesta tulisi saada hälytys mahdollisimman pian ja kaikkea, mitä IT-järjestelmässä tapahtuu, tulisi kyetä valvomaan (Calder 2023).

Valvontaan ja tapahtumien käsittelyyn kannattaa Calderin mukaan valita työkalut, joilla anomaliat havaitaan mahdollisimman pian ja automatisoidusti. Monissa pienemmissä, kuin suuremmissakin organisaatioissa reaaliaikaisen ja ympärivuorokautisen kybervalvonnan toteuttaminen voi olla haastavaa, jolloin se kannattaa myös pyrkiä automatisoimaan mahdollisimman pitkälle. Myös oman organisaation havaitsemista poikkeamista kannattaa kerätä mahdolliset tunnisteet, joita sen osalta on saatavilla (Calder 2023).

Joskus järjestelmään saattaa jäädä haavoittuvuuksia, joita ei kyetä korjaamaan tai niiden korjaaminen on vielä prosessissa. Mikäli haavoittuvan komponentin onnistunutta hyväksikäyttöä tai hyväksikäytön yrityksiä havaitaan kriittisessä järjestelmässä, on poikkeamaan vastaamiseen liittyvät toimenpiteet syytä käynnistää viipymättä. Tapahtumien reaaliaikainen valvonta ja löytäminen järjestelmästä kyetään toteuttamaan käyttämällä siihen tarkoitettuja automatisoituja työvälineitä, mutta toimenpiteiden käynnistämisestä ja merkittävän poikkeaman käsittelystä tulisi ihmisen Calderin mukaan olla aina vastuussa. Myös automaation havaitsema poikkeama tulisi aina tarkastaa asiantuntevan ihmisen toimesta sen arvioimiseksi ja tarvittaessa eskaloimiseksi (Calder 2023).

5.7 Haavoittuvuuden onnistuneen hyväksikäytön jälkeiset tapahtumat

Bhatt toteaa, että monissa tapauksissa haavoittuvuuksia hyväksikäytetään sisäänpääsyn luomiseksi järjestelmiin. Sisäänpääsyn jälkeen hyökkääjällä on yleensä monia eri tavoitetta. Tavoitteita voivat olla esimerkiksi järjestelmään sisäänpääsyn ylläpitäminen, joka onnistuu luomalla järjestelmään uusia käyttäjiä, asentamalla takaovia ja peittelemällä hyökkääjän tekemiä toimenpiteitä, jotta toiminta ei paljastu. Toisena tavoitteena on yleisesti käyttöoikeuksien korottaminen järjestelmässä, jotta haluttuja toimenpiteitä on helpompi suorittaa ja enemmän käytettävissä. Yksi tavoite on Bhattin mukaan myös datan siirtäminen ulos järjestelmästä (Bhatt, 2023).

Järjestelmään murtautumisen jälkeen edistyneillä uhkatoimijoilla on tapana pyrkiä liikkumaan lateraalisesti ja etsiä uusia kohteita kohdeympäristöstä. Myös toimenpiteistä aiheutuvien jälkien peitteleminen havaitsemisen vaikeuttamiseksi on yleinen toimenpide. Koska hyökkääjän tavoitteisiin kuuluu järjestelmään murtautumisen lisäksi erittäin todennäköisesti jotain edellä mainituista, on tärkeää, että haavoittuvuuksien korjaamisen jälkeen järjestelmää tarkastellaan myös muun haitallisen toiminnan kannalta. Tarkastelussa voidaan hyödyntää esimerkiksi jatkuvaa kybervalvontaa, päätelaitteita suojaavia ohjelmistoja ja yleisesti organisaatioiden kyberpoikkeamiin liittyvää käsittelyprosessia (Bhatt, 2023).

5.8 Raportointi, dokumentointi ja työnohjaus

Microsoftin haavoittuvuuden hallinnan mallin elinkaaren mukaan tilanneymmärryksen muodostamisen yksi osa on raportointi. Tehtyjen havaintojen, toimenpiteiden ja vaikutusten mahdollisimman tarkka sekä ajantasainen dokumentoiminen mahdollistaa reaaliaikaisen tilannekuvan ylläpitämisen. Mallin mukaan raportoinnilla pyritään määrittelemään järjestelmistä tunnistetut haavoittuvuudet sekä järjestelmän turvaaminen niiden osalta (What is vulnerability management? N.d.).

Kun haavoittuvuuksia tunnistetaan ja käsitellään, on syytä dokumentoida kaikki tehdyt toimenpiteet ja merkittävät organisaation järjestelmiä koskevat haavoittuvuudet. Korjaavien toimenpiteiden ja havaintojen ylläpitäminen esimerkiksi työnohjausjärjestelmässä auttaa organisaatiota hahmottamaan, mitä kunkin tunnistetun haavoittuvuuden osalta on tehty ja mikä tämän hetken tilanne on. Dokumentoinnin pohjalta organisaation asiantuntijat voivat luoda tilannekuvaa, jota voidaan käyttää tukena haavoittuvuuksien hallinnan prosessissa ja päätösten tekemisessä (What is vulnerability management? N.d.).

Organisaatioon kohdistuneesta kyberhyökkäyksestä tai haavoittuvuuden hyväksikäytöstä muodostuneesta poikkeamasta on aina hyvä ilmoittaa myös tarvittaessa kansalliselle viranomaiselle sekä mahdollisille asiakkaille, joihin poikkeama saattaa vaikuttaa. Havaintojen perusteella kyetään kansallisella sekä kansainvälisellä tasolla luomaan isompaa tilanneymmärrystä julkaistujen haavoittuvuuksien sekä niiden hyväksikäyttöjen jälkeisten toimenpiteiden osalta (What is vulnerability management? N.d.).

Laaja raportointi puolestaan parantaa yhteistä tilanneymmärryksen luomista ja auttaa myös muita organisaatioita kartoittamaan kyseisiä haavoittuvuuksia sekä niiden hyväksikäyttöä omista ympäristöistään, jos haavoittuvuuden hyväksikäyttöön liittyviä uhka- tai hyökkäystunnisteita saadaan kerättyä ja jaettua esimerkiksi viranomaisen kautta yleiseen jakoon muille organisaatioille. Tiedon jakamista voidaan myös rajoittaa, mikäli se sisältää organisaation salassa pidettävää dataa tai jaettavan tiedon luotettavuutta ei ole kyetty todentamaan tai varmistamaan (What is vulnerability management? N.d.).

6 Tapausesimerkit

Kappaleessa tarkastellaan haavoittuvuuden hallintaan ja haavoittuvuuksien hyväksikäyttämiseen liittyviä kokonaisuuksia ajankohtaisien tapausesimerkkien kautta. Tapausesimerkeiksi valittiin kolme toisistaan eroavaa tapausta, joita tarkastellaan erilaisista näkökulmista hyödyntäen aiemmissa kappaleissa esille tuotuja haavoittuvuuden hallinnan tilanneymmärryksen luomista helpottavia kokonaisuuksia sekä menetelmiä.

Ensimmäisessä tapausesimerkissä tarkastellaan turvallisen etäyhteyden muodostamiseen liittyviin ratkaisuihin tarkoitetuissa sovelluksissa julkaistuihin haavoittuvuuksiin sekä Internetin reunalla oleviin muihin haavoittuviin verkkolaitteisiin. Yksi tarkastelun kohteena oleva tapaus on yhdysvaltalainen tietoturvallisuuden ohjelmisto- ja laitetoimittaja Ivanti, jonka tuotteisiin julkaistiin useita kriittisiä haavoittuvuuksia. Julkaistuja haavoittuvuuksia käytettiin maailmalla merkittäviin kyberhyökkäyksiin ja haavoittuvuuksien hyväksikäytön jälkeisiä toimenpiteitä seurattiin viranomaisten ja tietoturvayhtiöiden toimesta aktiivisesti. Lisäksi tapausesimerkissä käsitellään toista tapausta, jossa eri laitevalmistajien VPN-tuotteisiin kohdistettiin lukuisia väsytyshyökkäyksiä, joilla autentikaatiomenetelmiä pyrittiin murtamaan järjestelmiin pääsyn saamiseksi (Known Exploited Vulnerabilities 2024).

Toisessa tapausesimerkissä käsitellään jatkuvaa prosessia, jossa tietoturvapäivityksiä julkaistaan, tasaisin väliajoin ja ne suositellaan asennettavaksi mahdollisimman nopeasti julkaisun jälkeen, jotta ympäristöt pysyvät turvallisina. Tapausesimerkin kautta pyritään tuomaan esiin sitä, että jatkuvalla prosessilla päivityksien vieminen tuotantoon helpottaa ympäristöjen ylläpitäjien työtä ja kouluttaa organisaatiota prosessin noudattamiseen.

Viimeisessä tapausesimerkissä tarkastellaan uhkatoimijoiden mahdollisuuksia vaikuttaa alustojen ja sovelluksien toimitusketjuun. Esitellyssä esimerkissä perehdytään tapahtumaan, jossa uhkatoimija sai sisällytettyä Linux-pohjaisien käyttöjärjestelmien jakelun mukana tulevaan tiedostojen pakkaustyökaluun haitallista koodia, jonka myötä tietyillä reunaehdoilla käyttöjärjestelmään avautui takaovi. Takaovea hyödyntämällä uhkatoimijalla oli mahdollisuus muodostaa yhteys julkisessa verkossa kiinni olevaan ympäristöön, joihin se oli päivityksien mukana päätynyt.

6.1 Verkon reunalla olevien tuotteiden hyödyntäminen hyökkäyksissä

Monien valmistajien verkkolaitteisiin sekä VPN-tuotteisiin on julkaistu vuosien 2023 lopussa ja 2024 alussa useita kriittisiä haavoittuvuuksia, joita on hyväksikäytetty laajasti maailmalla. Hyväksikäyttäen Internetin reunalla olevia haavoittuvia verkkolaitteita ja VPN-tuotteita, hyökkääjät ovat onnistuneet suorittamaan lukuisia merkittäviä kyberhyökkäyksiä, joissa on päästy käsiksi ratkaisun takana olevaan järjestelmään. Hyvänä esimerkkinä tällaisista haavoittuvuuksista toimivat CVE-2024-21887 ja CVE-2023-46805, jotka koskevat Ivantin Connect Secure ja Policy Secure -tuotteita Ivanti tarjoaa palveluita ja tuotteita esimerkiksi päätelaitteiden hallintaan ja niiden turvallisuuden varmistamiseen.

Haavoittuvuudet julkaistiin 0-päivähaavoittuvuuksina, joihin ei julkaisuhetkellä ollut virallista korjaavaa päivitystä saatavilla. Yhdysvaltain kyberturvallisuusviranomainen, CISA julkaisi myös useita varoituksia ja ohjeistuksia vuoden 2024 alussa kyseisien haavoittuvuuksien hyväksikäytön ehkäisemiseksi ja havaitsemiseksi. Lisäksi tuotteisiin julkaistiin useita muita haavoittuvuuksia, joiden avulla tuotteisiin kyettiin hyökkäämään (Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways 2024)

6.1.1 Case: Haavoittuvan Ivantin Connect Secure tai Policy Secure -tuotteen hyväksikäytön jälkeiset toimenpiteet

Edellisessä luvussa mainittujen haavoittuvuuksien hyväksikäyttäminen antaa hyökkääjälle mahdollisuuden päästä käsiksi etänä järjestelmään sekä mahdollisuuden ohittaa käyttäjätunnistautuminen. Tämän jälkeen hyökkääjä voi suorittaa pahimmassa tapauksessa järjestelmänvalvojan oikeuksilla mielivaltaisia komentoja palvelimella ja saada osia koko verkosta haltuunsa. Mikäli kyseisiä haavoittuvia tuotteita on saavutettavissa Internetistä, on todennäköistä, että niihin on yritetty vaikuttaa. Tässä tapausesimerkissä tarkastellaan mahdollisia toimenpiteitä, joita tietty uhkatoimija on

tunnetusti suorittanut haavoittuvuuden hyväksikäytön jälkeen järjestelmissä (Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways 2024).

Mandiantin julkaiseman artikkelin mukaan esimerkiksi toistaiseksi tuntematon uhkatoimija, jonka tiedetään hyväksikäyttävän edellisessä luvussa mainittuja Ivantin haavoittuvuuksia, on useassa eri tapauksessa asentanut järjestelmiin haittaohjelmia, jotka naamioituvat luotettaviksi tiedostoiksi. Kyseinen uhkatoimija on myös toteuttanut muita toimenpiteitä, joilla se on saanut ylläpidettyä jalansijaansa järjestelmissä ja mahdollistaakseen haavoittuvuuksien hyväksikäytön jälkeiset toimenpiteet. Haavoittuvuuksien hyväksikäytön jälkeiset toimenpiteet voivat olla esimerkiksi käyttäjätunnusten, tietojen ja tiedostojen varastamista järjestelmästä (McLellan, Wolfram, Roncone, Lin, Wallace & Andonov 2024).

Haittaohjelmien ja haavoittuvuuden hyväksikäytön jälkeisten toimenpiteiden tunnistamiseksi oli julkaistu myös tunnisteita ja tunnistussääntöjä, joilla haitallista toimintaa voitiin etsiä järjestelmästä. Haavoittuvuuksiin ei ollut julkaisuhetkellä tarjolla korjaavaa ohjelmistopäivitystä, vaan Ivanti julkaisi keinon rajoittaa haavoittuvuuksien hyväksikäyttömahdollisuuksia, tämä rajoituskeino kuitenkin kyettiin myöhemmin todistetusti ohittamaan. Korjaava ohjelmistopäivitys julkaistiin vasta viikkojen kuluttua haavoittuvuuden julkaisemisesta (McLellan, Wolfram, Roncone, Lin, Wallace & Andonov 2024).

Haavoittuvuuksien hyväksikäyttömahdollisuuksiin julkaistun korjaavan toimenpiteen ohittamisen mahdollisuuden tultua julkisuuteen uhkatoimijat alkoivat kehittää tapoja, joilla järjestelmiin kyettiin luomaan takaovia. Takaovista havaittiin useaa eri variaatiota, joiden avulla järjestelmään kyettiin tekemään uhkatoimijan toiminnan mahdollistavia muutoksia. Haavoittuvuuksia kyettiin myös ketjuttamaan suuremman vaikutuksen aikaan saamiseksi. Joissain tapauksissa uhkatoimijat myös poistivat järjestelmästä lokitietoja peitelläkseen omia jälkiään (Lin, Wallace, Wolfram, Andonov & McLellan 2024).

Uhkatoimijoiden toimenpiteiden ja menetelmien tunnistamiseksi luotiin Ivantin toimesta työkaluja, joilla haavoittuvuuksiin yhdistettyjä toimenpiteitä voitiin havaita järjestelmästä. Ivanti julkaisi työkalut sekä ulkoisien, kuten asiakkaiden että organisaation sisäisien järjestelmien eheyden tar-

kastamiseksi. Lisäksi hyökkäyksien yhteydessä havaittuihin takaoviin, haittaohjelmiin ja muihin toimenpiteisiin julkaistiin tunnisteita ja sääntöjä, joilla haitallista toimintaa voidaan havainnoida järjestelmästä. Myös useat eri viranomaiset julkaisivat suosituksia siitä, kuinka organisaatioiden tulisi toimia, mikäli heillä on käytössä kyseisen valmistajan haavoittuvia tuotteita (Lin, Wallace, Larsen, Gandrud, Thompson, Pearson & Frazer 2024).

Organisaation tilanneymmärryksen muodostamiseksi haavoittuvuuksien osalta suositeltiin, että kaikkiin järjestelmiin, joissa tuotteita on käytössä, ajetaan Ivantin julkaisemat tarkastustyökalut uhkatoimijoiden mahdollisien toimenpiteiden varalta. Tarkastustyökaluja suositeltiin ajettavaksi siitä huolimatta, että useat viranomaiset olivat todenneet, että niiden tuloksiin ei voi täysin luottaa, sillä uhkatoimijat olivat keksineet keinoja tarkastustyökalun kiertämiseen. Myös kaikkia tuotteiden Internet-yhteyksiä kehotettiin rajoittamaan ja järjestelmät kehotettiin pitämään ajan tasalla päivityksien osalta. Yhtenä toimenpiteenä neuvottiin myös rajoittamaan sellaisien käyttäjien pääsyä VPN-palveluihin, joilla siihen ei ollut tarvetta (Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways 2024).

CISA suositteli, että kaikki järjestelmiin suoritettavat toimenpiteet tulisi suorittaa viipymättä ja tarvittaessa hätätoimenpiteinä. Myös kaikista mahdollisista havainnoista kehotettiin ilmoittamaan viipymättä viranomaiselle. Koska haavoittuvuuksien hyväksikäyttöä havaittiin maailmalla massoittain, CISA myös lisäsi haavoittuvuudet ylläpitämäänsä KEV-katalogiin tilannetiedon jakamiseksi. Lopulta CISA:n suosituksen mukaan kaikki Ivantin toimittamat tuotteet tulisi poistaa organisaatioiden käytöstä viipymättä (Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways 2024).

6.1.2 Case: Väsytyshyökkäys Internetissä kiinni olevaan VPN-tuotteeseen, hyökkäys vai hämäys?

Huhtikuussa 2024 Ciscon omistama tietoturvayhtiö Talos kertoi havainneensa globaalia kasvua väsytyshyökkäyksissä, jotka kohdistuvat julkisessa verkossa oleviin kirjautumissivustoihin ja SSH-palveluihin. Merkittävää kasvua tilastoissa havaittiin maaliskuun 2024 puolivälin jälkeen ja määrän odotetaan edelleen kasvavan. Suurin osa havaituista hyökkäyksistä vaikutti tulevan anonyymiin Internetin selaamiseen tarkoitetusta Tor-verkosta sekä muista liikennettä anonymisoivista ratkaisuista. Väsytyshyökkäykset ovat aiemmin kuvatun mukaisesti yksi yleisimmistä kyberhyökkäyksistä

ja ne ovat myös helposti havaittavissa, sillä hyökkäykset aiheuttavat normaalia suuremman määrän liikennettä kohteeseen sekä selkeää kasvua kirjautumis- ja autentikointisyrityksiin (Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials 2024).

Havaituissa hyökkäyksissä käytettiin usein geneerisiä sekä valideja organisaatioiden käyttäjätunnuksia. Hyökkäyksiä ei anonymisoinnin ja niiden satunnaisuuden takia voitu myöskään kohdentaa mihinkään tiettyyn toimialaan tai maantieteelliseen sijaintiin. Riippuen kohteesta, onnistunut väsytyshyökkäys voi johtaa käyttäjätunnuksien lukkiutumiseen tai palvelunestotilaan. Myös heikkojen tai vuodettujen käyttäjätunnuksien tapauksessa on mahdollista, että hyökkääjä saa väsytyshyökkäyksellä pääsyn kohteena olevaan järjestelmään (Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials 2024).

Väsytyshyökkäysten on havaittu kohdistuvan useiden eri suosittujen valmistajien tuotteisiin, joista osassa on myös julkaistu merkittäviä hyväksikäytettyjä haavoittuvuuksia sekä niitä on hyödynnetty onnistuneisiin julkisuuteen tulleisiin kyberhyökkäyksiin vuonna 2024. Organisaation tietoturvakontrollien ja hälytysnäkymien tukkiminen väsytyshyökkäyksellä on tehokas tapa viedä huomiota pois muulta järjestelmissä tapahtuvalta vaikuttamiselta sekä työllistää henkilöstöä käsittelemään niistä aiheutuvia vaikutuksia (Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials 2024).

Organisaatioiden, joihin vastaavaa toimintaa kohdistuu, kannattaisi myös erityisesti tarkkailla muuta epänormaalia toimintaa järjestelmissään, sillä väsytyshyökkäysten luoma liikennemäärä ja huomion kiinnittyminen muualle antavat loistavan suojan muulle hiljaisemmalle kybervaikuttamiselle kohdeympäristössä. Myös itse väsytyshyökkäyksiin kannattaa suhtautua vakavasti ja ohjeistaa henkilöstöä ylläpitämään vahvoja salasanoja sekä monivaiheista tunnistautumista, jotta järjestelmään murtautuminen olisi mahdollisimman vaikeaa (Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials 2024).

6.1.3 Case: ArcaneDoor

Jatkona edellisen luvun uutisoinnille väsytyshyökkäysten merkittävästä määrällisestä kasvusta Talos julkaisi artikkelin, jossa se esitteli uuden kampanjan nimeltä ArcaneDoor. Kampanja on hyvä esimerkki siitä, kuinka valtiollisen tasoiset kyberuhkatoimijat hyväksikäyttävät Internetin reunalla

olevia haavoittuvia verkkolaitteita järjestelmiin murtautumispisteenä ja vakoiluun keskittyvään kybervaikuttamiseen. Verkon reunalla olevat sovellukset ja laitteet, joista menee liikennettä sekä sisään ja ulos tarjoavat haltuun otettuna uhkatoimijalle mahdollisuuden muokata verkkoliikenteen reitityksiä, uudelleenohjata liikennettä haluamiinsa sijainteihin sekä monitoroida verkkoliikennettä. Kampanja myös kertoo uhkatoimijan pitkäjänteisestä toiminnasta ja yleisesti uhkatoimijoiden kyvyistä löytää uusia haavoittuvuuksia, jotka pysyvät poissa julkisuudesta eikä niistä ole tunnistettuja havaintoja tai hyväksikäyttömenetelmiä (ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices 2024).

Hyökkäyksissä käytettyä alkuperäistä hyökkäysvektoria ei kyetty löytämään kampanjan tunnistamisvaiheessa, mutta Cisco julkaisi tuotteissaan kaksi uutta haavoittuvuutta, jotka liittyivät vastaavaan toimintaan. Talos suositteli, että kaikkien vastaavien laitteiden lokit tulisi siirtää keskitettyyn turvalliseen paikkaan sekä niissä tulisi käyttää vahvaa ja monivaiheista autentikointia. Lisäksi useat eri toimijat julkaisivat kampanjan tunnistamisvaiheessa uhkatunnisteita, joita todennetuissa hyökkäyksissä oli käytetty. Talos suositteli artikkelissan myös, että mikäli kyseisiä tunnisteita havaitaan järjestelmässä, olisi kohteiden tarkempi tutkiminen välttämätöntä. Lisäksi haavoittuvuuksiin julkaistiin valmistajan toimesta korjaavia ohjelmistopäivityksiä, jotka suositeltiin asennettavaksi tuotantoon viivyttelemättä (ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices 2024).

Haavoittuvuuksien ja hyökkäyksien valmistelusta ja pitkäjänteisyydestä kertoo aikajana, jonka mukaan ensimmäisiä havaintoja uhkatoimijan löytämistä haavoittuvuuksista ja suorittamista testihyökkäyksistä löydettiin jo kesällä 2023. Vastaava toiminta oli jatkuvaa kampanjan julkaisuajankohtaan asti ja näytteitä ensimmäisistä onnistuneista hyökkäyksistä todettiin tammikuussa 2024. Pitkäjänteisyys ja uusien 0-päivähaavoittuvuuksien hyväksikäyttäminen viittaavat kehittyneeseen valtiollisen toimijan tasoiseen uhkatoimijaan, joka artikkelin mukaan on vielä toistaiseksi tunnistamaton. Lisäksi uhkatoimija loi kampanjaa varten kaksi uutta takaovea, joita se käytti haitallisen toiminnan suorittamiseen kohteeksi päätyneissä järjestelmissä (ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices 2024).

6.2 Jatkuvan päivitysprosessin edut

Noudattamalla jatkuvaa päivitysprosessia tapauksessa, jossa tuotteeseen julkaistaan, tasaisin väliajoin uusia tietoturvapäivityksiä ja ne toteutetaan normaalin muutoshallinnan mukaisesti, kyetään ympäristö pitämään lähtökohtaisesti turvallisena. Jatkuva automatisoitu ja toistuva päivitysprosessi ei kuitenkaan täysin poista muutoshallinnan ja ylläpidon vastuuta, vaan päivitykset tulee asentaa ajallaan julkaisun jälkeen, jotta järjestelmään ei jää tunnettuja haavoittuvuuksia. Myös erikseen julkaistavia kiireellisiä päivityksiä on syytä seurata, jotta ne tulee asennettua ajallaan, tarvittaessa hätämuutoksena (Morrissey 2023).

Tietoturvapäivityksien tuominen tuotantoon on Magnussonin mukaan yksi helpoimmista tavoista pitää ympäristö turvallisena, joskaan kaikissa tapauksissa se ei ole helppoa. Tasaisin väliajoin julkaistavat päivitykset, jotka voidaan viedä tuotantoon käyttäen esimerkiksi keskitettyyn päivityksien hallintaan tarkoitettuja työkaluja ovat kuitenkin täysin päinvastainen asia verrattuna järjestelmiin, joissa haavoittuvuuksien korjaaminen saattaa vaatia mittavia toimenpiteitä ja testaamista ilman automatisointia (Magnusson 2020).

Jatkuvan prosessin toteuttamisella ja harjoittelemisella voidaan kuitenkin valmentaa henkilöstöä myös vaativampiin tapauksiin, sillä päivitysprosessin tuntemus kasvaa sitä mukaa, kun prosessia toteuttaa. Myös oman toimintaympäristön tuntemus paranee toteutettaessa jatkuvia päivityksiä ja arvioitaessa niiden vaikutuksia ympäristön toimintaan, jolloin voidaan tehdä nopeampia arvioita siitä, milloin tuotteet on viimeksi päivitetty ja mikä versio niistä on kyseisellä ajanhetkellä käytössä. Jatkuvassa prosessissakin asennettujen päivityksien jälkeen tulee tehdä validointia, jolla todetaan, että päivitykset ovat asentuneet oikein ja ympäristön toiminnot toimivat (Magnusson 2020).

6.2.1 Case: Microsoftin kuukausittaiset tietoturvapäivitykset

Hyvänä esimerkkinä toistuvasti tietyin väliajoin julkaistavista päivityksistä toimivat Microsoftin kuukausittaiset tietoturvapäivitykset, jotka julkaistaan jokaisen kuukauden toisena tiistaina. Morrisseyn mukaan Microsoft käyttää kuukausittain julkaistavien päivien julkaisupäivästä nimeä ”Patch Tuesday”. Päivitykset korjaavat Microsoftin tuotteisiin julkaistuja haavoittuvuuksia, joista joissain tapauksissa osa saattaa olla myös luokiteltu 0-päivähaavoittuvuudeksi. Microsoft julkaisee

tarvittaessa myös päivityksiä julkaisuikkunan ulkopuolella, mikäli sen tuotteista löydetään tarpeeksi vakava laatu- tai tietoturvaongelma (Morrissey 2023).

Microsoftin päivitykset ovat kumulatiivisia, eli ne korjaavat myös aiemmin julkaistut tietoturvaongelmat ja -haavoittuvuudet. Päivitykset on määritelty asennettavaksi järjestelmiin pakollisesti, mutta ympäristöissä, joissa ei ole pääsyä Internettiin ne täytyy kuitenkin asentaa manuaalisesti. Tietyin ja tasaisin väliajoin julkaistavien päivityksien asentaminen kannattaisikin aina suunnitella tällaisissa tapauksissa toteutumaan mahdollisimman pian julkaisun jälkeen. Microsoft tarjoaa myös mahdollisuuden päivityksiensä validoimiseen ennen julkaisua, mutta validoivat päivitykset eivät sisällä kaikkia julkaistavia tietoturvaominaisuuksia (Morrissey 2023).

6.3 Toimitusketju uhkatoimijan aseena

Vaikka organisaation sisäisen tieto- ja kyberturvallisuuden taso olisi yleisesti hyvä ei se ole tae sille, että organisaatio on turvassa kybervaikuttamiselta. Lähes poikkeuksetta organisaatioissa on käytössä jonkin kaupallisen toimijan tuotteita, joita se itse täysin hallinnoi. Toimitusketjuun vaikuttaminen mahdollistaakin haitallisen koodin tai sisällön tuomisen organisaation järjestelmiin, jonka takia kaikki ulkoa tulevat asennettavat päivitykset ja tuotteet kannattaa tarkastaa huolellisesti ennen käyttöönottoa. Tässä kappaleessa tarkastellaan toimitusketjuhyökkäystä, jossa uhkatoimija onnistui saamaan haitallista koodia Linux-käyttöjärjestelmässä olevan työkalun jakeluun. Kappaleen tutkimus perustuu ensimmäisiin päiviin haavoittuvuustiedotteen julkaisun jälkeen (Calder 2023).

6.3.1 Case XZ Utils: Haitallista koodia pakkaustyökalun mukana

Maaliskuun lopussa 2024 julkaistiin haavoittuvuustiedote koskien haavoittuvuutta CVE-2024-3094, joka koski osaa Linux-käyttöjärjestelmän jakeluversioista. Haavoittuvuus sai pohjapisteikseen CVSS 3.1 -menetelmällä ensiarviona täyden 10.0, lisäksi Yhdysvaltain kyberturvallisuusviranomainen CISA (2024) julkaisi aiheesta erillisen varoituksen. Haavoittuvuus muodostui Linux-käyttöjärjestelmälle luotuun XZ Utils-pakkaustyökaluun, johon uhkatoimija onnistui sisällyttämään haitallista koodia, joka mahdollisti tiettyjen ehtojen täyttyessä takaoven muodostamisen ja haitallisen koodin suorittamisen SSH-yhteyden kautta liitteen 1 mukaisesti. Haavoittuvuutta hyväksikäyttämällä

hyökkääjällä olisi mahdollisuus päästä järjestelmään käsiksi ilman tunnistautumista (Bar, Cohen & Aminov 2024).

Haavoittuvuudesta myös poikkeuksellisen teki se, että uhkatoimija oli kyennyt luomaan tarpeeksi vahvan luottamussuhteen järjestelmän toimittajaan sisällyttääkseen viralliseen jakeluun haitallista koodia. Vastaavan luottamussuhteen luominen oli mahdollisesti vuosien työ ja vaatinut taitavaa kohteen sosiaalista manipulointia. Tietoturvayhtiö Akamain mukaan uhkatoimija oli aloittanut antamaan kontribuutiota työkalun kehitykseen jo kaksi vuotta ennen haavoittuvuuden julkaisua. Tapahtuma kuitenkin osoittaa sen, että myös luotettaviin jakeluihin on mahdollista toteuttaa toimitusketjuhyökkäyksiä tarpeeksi pitkän ja vahvan luottamussuhteen luomisen avulla (XZ Utils Backdoor — Everything You Need to Know, and What You Can Do 2024).

Barin, Cohenin ja Aminovin mukaan haitallinen koodi oli naamioitu ja peitelty tarkkaan sekä sisällytetty mukaan ainoastaan tiettyihin Linux-jakeluihin. Kun haitallinen koodi käynnistyi tarkasti se ensimmäisenä, että Linux-käyttöjärjestelmästä on tietty versio käytössä ja se on rakennettu tietyllä tavalla. Mikäli ehdot eivät täyttyneet, takaovea ei asennettu järjestelmään. Takaoven asentumisen jälkeen se sisälsi lisäksi useita ajon aikaisia vaatimuksia, jotta sitä kyettiin hyödyntämään (Bar, Cohen & Aminov 2024).

6.3.2 Julkaisun jälkeisen tilanneymmärryksen muodostaminen XZ Utils -haavoittuvuuden osalta

Haavoittuvuuden julkaisemisen jälkeen useat eri tahot mukaan lukien sovellustoimittajat julkaisivat ohjeita, kuinka haavoittuvuuden kanssa tulisi ensikädessä toimia. Haavoittuvuuden korjaamiseksi poikkeuksellisesti yleisin ohje oli aluksi asentaa vanhempi jakeluversio, jossa haavoittuvaa koodia ei ollut mukana. Myös joidenkin käyttöjärjestelmäjakeluiden käyttö kehotettiin lopettamaan välittömästi, kunnes ongelma on korjattu ja korjaava versio julkaistu. Joissain tapauksissa haavoittuvia versioita sisältävät ympäristöt myös kehotettiin luomaan uudelleen puhtaalla Linux-asennuksella korjaavan version julkaisun jälkeen (Bar, Cohen & Aminov 2024).

Teknisen tilanneymmärryksen muodostamiseksi haavoittuvuuden osalta organisaatioiden ja ylläpitäjien tulisi ensi tilassa selvittää, onko kyseinen haavoittuva versio käytössä. Mikäli haavoittuva versio olisi käytössä, tulisi sitä koskevat julkaistut toimenpiteet käynnistää välittömästi, varsinkin

jos järjestelmään on mahdollista ottaa yhteys julkisesta verkosta. Haavoittuvia versioita sisältäneet järjestelmät tai laitteet tulisi tutkia ja epänormaalia toimintaa ympäristössä pitäisi tarkkailla tai metsästää, jotta mahdollinen haavoittuvuuden hyväksikäytön jälkeinen toiminta saataisiin kiinni (Bar, Cohen & Aminov 2024).

Myös Traficom (2024) haavoittuvuustiedotteessaan toteaa, että pelkkä haavoittuvuuden korjaaminen ei välttämättä ole riittävä toimenpide, mikäli haavoittuvuutta on jo hyväksikäytetty. Tilanneymmärryksen tueksi organisaatioiden tulisi jatkaa aiheen uutisoinnin seurantaa ja tarkkailla mahdollisia päivityksiä tilanteeseen liittyen sekä pyrkiä löytämään todennettuja onnistuneesta hyökkäyksestä koituneita seurauksia ja uhkatunnisteita, joita mahdollisista hyökkäyksen kohteeksi päätyneistä organisaatioista jaetaan käytettäväksi.

Koska haavoittuvuuden toimitusketjuun vienyt toimija ei ole haavoittuvuuden julkaisuhetkellä tiedossa eikä mahdollisten onnistuneiden hyökkäysten seuraamuksista ole tietoa ei voida arvioida, mihin haavoittuvuutta hyväksikäyttävät tahot pyrkivät toiminnallaan. Akamain (2024) mukaan operaation pitkäjänteisyys viittaa valtiolliseen uhkatoimijaan, mutta haavoittuvuuden julkaisuhetkellä attribuutiota ei ollut saatavilla. Tarvittaessa tapahtumista ja havainnoista tulisi myös laatia poikkeamailmoitus kansalliselle viranomaiselle, kuten CISA (2024) kehottaa ja valmistautua raportoimaan erikseen tapauksen selvittämisestä omalle organisaatiolle.

7 Johtopäätökset

IT-järjestelmistä ja järjestelmäkomponenteista löydetään jatkuvasti uusia kriittisiä haavoittuvuuksia, pahimmillaan useita kymmeniä päivässä. Osa haavoittuvuuksista onnistutaan myös salaamaan uhkatoimijoiden toimesta pitkiäkin aikoja ennen niiden paljastumista ja korjaavien toimenpiteiden, kuten ohjelmistopäivityksien julkaisua. Tietoturvan osa-alueiden, luotettavuuden, eheyden ja saatavuuden varmistaminen organisaatioiden käytössä olevien järjestelmien ja niiden sisältämien tietojen ja toiminnallisuuksien osalta tarvitsee toteutuakseen tieto- ja kyberturvallisen ympäristön, jossa haavoittuvuuksiin ja tieto- sekä kyberturvallisuuden puutteisiin suhtaudutaan niihin vaadittavalla vakavuudella.

Organisaation tuottamat ja ylläpitämät järjestelmät tulisi rakentaa ja tarkastaa valitsemalla siihen soveltuva ohjelmisto- tai järjestelmäkehityksen toimintamalli ja tietoturvallisuuden standardi, joita

noudatetaan. Tieto- ja kyberturvallisuus tulisi huomioida jatkuvana prosessina heti järjestelmän suunnitteluvaiheesta asti, sillä niiden toteuttaminen tuotantoon viennin jälkeen voi olla haastavaa. Ketterään ohjelmisto- ja järjestelmäkehitykseen on luotu myös työskentelymalleja, joiden avulla luodaan parempi sekä tehokkaampi tapa projekteille tuottaa asiakkaan tarpeita palvelevia turvallisia tuotteita.

Haavoittuvuuksista on olemassa paljon erilaisia variaatioita, joilla ei välttämättä ole edes yleisiä tunnisteita tai vakavuusluokitteluja. Oman organisaation tai ylläpidettävän järjestelmän syvällinen tunteminen helpottaa haavoittuvuuksien arvioinnissa, johon on myös tarvittaessa saatavilla erilaisia laskureita tai arviointimenetelmiä. Haavoittuvuuksiin liittyen julkaistaan jatkuvasti valtava määrä uutta tietoa, jonka joukosta juuri omaa järjestelmää koskevat tiedotteet voi olla haastava löytää. Haavoittuvuustiedon keräämiseen ja kartoittamiseen on myös organisaatioita ja viranomaisia, jotka kokoavat globaalisti merkittäviä vaikutuksia aiheuttavia ja maailmalla laajasti hyväksikäytettyjä haavoittuvuuksia sivustojensa alle helpottaakseen asiantuntijoiden työtä tiedon keräämisessä.

Haavoittuvuuksia voidaan myös kartoittaa järjestelmistä siihen tarkoitetuilla työkaluilla, kuten haavoittuvuusskannereilla. Työkalujen tuottamien raporttien perusteella voidaan priorisoida suurimman uhan järjestelmälle aiheuttavia haavoittuvuuksia ja määritellä järjestys, jossa haavoittuvuuksia lähdetään korjaamaan. Järjestelmistä löytyviä haavoittuvuuksia kannattaa tarkastella tasaisin väliajoin käyttäen siihen tarkoitettuja työkaluja, mutta myös uusimpia tiedotteita ja uutisointia on syytä seurata, jotta tilanneymmärrys säilyy mahdollisimman ajantasaisena ja uudet julkaistut haavoittuvuudet voidaan priorisoida.

Yhtenä tärkeimpänä johtopäätöksenä teknisen tilanneymmärryksen muodostamisen osalta on, että ainoastaan haavoittuvuustiedon kerääminen ja tunnettujen haavoittuvuuksien korjaaminen asentamalla julkaistu päivitys tai rajoittamiskeino ei ole riittävä toimenpide toimivan haavoittuvuuden hallinnan osalta. Korkean riskin hyväksikäytölle muodostavat kohteet, kuten suoraan Internetiin kytköksissä olevat haavoittuvat järjestelmät tulisivat olla jatkuvassa keskitetyssä valvonnassa ja seurannassa, jotta niihin mahdollisesti kohdistuvat vaikuttamisyritykset ja niistä aiheutuvat vahingot voidaan havaita ja niihin kyetään reagoimaan ajoissa. Lisäksi valvonta ja lokien

säilöntä tulisi toteuttaa erillisessä järjestelmässä, jotta mahdollisella lokien tuhoamisella ei saada peitettyä hyökkäyksen jälkiä.

Tilanteeseen ja tilanneymmärrykseen vaikuttaa olennaisesti myös organisaation kyky tehdä päätöksiä. Joissain tapauksissa nopeat päätökset ja hätämuutoksen aloittaminen ovat välttämättömiä, mutta tapauksissa, joissa on enemmän aikaa käytössä, korostuu päätöksenteon tueksi tehty analyysi ja tilannekuva. Päätöksentekoa ei kannata myöskään turhaan viivyttää, sillä ympäristön tai järjestelmän jättäminen haavoittuvaksi saattaa aiheuttaa merkittäviä katkoksia organisaation kriittisille toiminnoille, mikäli haavoittuvuuksien avulla kyetään aiheuttamaan häiritsevää tai tuhoavaa kybervaikuttamista.

Päätöksentekokykyä tai päätöksenteon nopeutta voidaan parantaa esimerkiksi luomalla muutosvastaavan tueksi ryhmä, jonka tehtävä on tuottaa materiaalia ja analyysiä päätöksenteon helpottamiseksi. Hätämuutoksia ja niiden toteuttamista varten puolestaan voidaan perustaa oma ryhmänsä, joka kutsutaan koolle tarvittaessa arvioimaan hätämuutoksen tarpeellisuutta. Päätöksentekoa voidaan helpottaa ja aikaa säästää luomalla joidenkin päivityksien ja muutoksien ympärille jatkuva ja jopa automatisoitu prosessi, jossa käytössä olevat tuotteet päivitetään uusimpaan versioon mahdollisimman nopeasti julkaisun jälkeen.

Tapausesimerkit osoittavat, että toinen toistaan kehittyneemmillä kyberuhkatoimijoilla on kyky luoda menetelmiä, kuten uusia toistaiseksi julkisuudelta piilossa olevia haavoittuvuuksia tai haittaohjelmia, joiden avulla päästään haluttuun loppuasetelmaan. Varsinkin internetin reunalla olevat kohteet, joiden kautta on pääsy järjestelmään ja mahdollisuus edetä syvemmälle kohteessa muodostavat merkittävän uhan organisaatioille, jolleivat niiden turvallisuuteen liittyvät tekijät kuulu jatkuvan seurannan ja tarkkailun piiriin. Uusimpien tietoturvapäivityksiä sisältävien ohjelmistoversioiden vieminen tuotantoon olisikin hyvä toteuttaa joko automatisoituna tai jatkuvana prosessina, jolloin järjestelmän turvallisuus paranee merkittävästi.

Pelkästään viimeisimpien ohjelmistopäivityksien asentaminen ja verkon reunalla olevien kohteiden erityisseuranta ei kuitenkaan ole lähtökohtaisesti riittävä toimenpide haavoittuvuuden hallinnalle tai organisaation kyberturvallisuusstrategiaksi. Uusimpiin uhkiin tulisi varautua jatkuvasti ja oman

organisaation ympäristön valvontaa tulisi evästää vähintäänkin uhkatunnisteilla, jotka liittyvät uusien tunnettujen haavoittuvuuksien hyväksikäyttöön tai maailmalla laajasti meneillään oleviin kampanjoihin.

Myös toimitusketju muodostaa merkittävän vektorin järjestelmiin ja organisaatioihin kohdistuvalle kybervaikuttamiselle. Luotettujen toimittajien tuottama koodi tai ohjelmisto saattaa olla turvallinen, mutta mikäli se käyttää tukenaan esimerkiksi kirjastoja tai sovelluksia, joiden toimitusketjuun on kyetty vaikuttamaan tai niihin on saatu lisättyä uhkatoimijan toimesta jotain ylimääräistä, muodostuu organisaation järjestelmään mahdollinen tietoturvaongelma. Tuotantoon vietävät päivitykset ja toiminnallisuudet tulisikin aina testata ja varmentaa niiden asentamista, mutta tämä ei kuitenkaan täysin poista mahdollisuutta joutua toimitusketjuun kohdistuvan kybervaikuttamisen kohteeksi.

8 Pohdinta

8.1 Tutkimuksen tulokset

Tutkimuksen tuloksena syntyi raportti, jossa käsiteltiin haavoittuvuuden hallinnan ja tilanneymmärryksen muodostamisen kannalta olennaisia asiakokonaisuuksia. Raportin pohjalta voidaan todeta, että haavoittuvuuden hallinta sekä sen tilanneymmärrys on todella laaja kokonaisuus, johon käyttötarkoituksesta riippuen liittyy paljon huomioitavia asioita, kuten korjaavien toimenpiteiden aikakriittisyys, olennaisen haavoittuvuustiedon kerääminen ja analysointi sekä oikea-aikaisen päätöksenteon merkitys.

Käsiteltyjen asiakokonaisuuksien määrästä huolimatta tuloksena ei syntynyt haavoittuvuuden hallinnan kaikkiin osa-alueisiin kaiken kattavaa tutkimusta, mutta tutkimus sisältää olennaisia kokonaisuuksia, jotka liittyvät aiheeseen. Myös tilanneymmärryksen muodostamisen olennaiset aiheet esiteltiin tutkimuksessa niin tekniseltä, kuin operatiiviselta näkökannalta käyttäen hyväksi viimeisimpiä maailmalla julkaistuja tapausesimerkkejä. Tapausesimerkeiksi valikoitiin mahdollisimman erilaisia kokonaisuuksia, jotta tilanneymmärryksen muodostamista kyettiin tarkastelemaan monenlaisissa tilanteissa.

8.2 Tutkimuksen tuloksien hyödyntäminen ja jatkokehittäminen

Tutkimuksen tuloksia voidaan hyödyntää parantamaan eri organisaatioiden käsitystä IT-järjestelmien haavoittuvuuksista ja niihin liittyvän tilanneymmärryksen muodostamisesta sekä yleisesti haavoittuvuuksien muodostamaa uhkaa järjestelmille. Tutkimukseen kerättiin ajankohtaisia aihealueita ja haavoittuvuuden hallintaan liittyviä kokonaisuuksia, joita hyödyntämällä saadaan muodostettua yleinen käsitys siitä, mitä ovat haavoittuvuudet ja mitä kokonaisuuksia niiden käsittelyssä tulee huomioida. Työn tuloksena syntynyttä raporttia voidaan myös käyttää uusien henkilöiden perehdyttämiseksi haavoittuvuuden hallintaan ja tilanneymmärryksen muodostamiseen organisaatioissa. Kenttätestaaminen on mahdollista myös organisaatioiden haavoittuvuuden hallinnan prosessin näkökulmasta.

Haavoittuvuudet ja uudet haavoittuvuuden hyväksikäytön jälkeiset kybervaikuttamisen menetelmät kehittyvät jatkuvasti, mutta niiden ympärille luodut vastuualueet, roolit ja prosessit säilyvät lähtökohtaisesti pääpiirteittäin muuttumattomina tai välttyvät merkittäviltä toiminnallisilta muutoksilta. Uusia viitekehyksiä ja standardeja julkaistaan sekä olemassa olevia kehitetään viranomaisten ja organisaatioiden toimesta. Standardien pohjalta haavoittuvuuden hallinnan edelleen kehittämien on tulevaisuudessakin mahdollista.

Tutkimuksessa ei varsinaisesti esitelty yhtä ja tiettyä vaihtoehtoa haavoittuvuuden hallinnan sekä tilanneymmärryksen muodostamisen prosessiksi, joten jatkokehittämisen näkökulmasta esimerkiksi toimivan prosessikaavion tai toimintamallin perustan luominen olisi oma kokonaisuutensa. Myös organisaatioiden toiminnan jatkuva kehittäminen ja nykytilanteen tunnistaminen haavoittuvuuden hallinnan osalta on mahdollista tutkimuksen pohjalta. Lisäksi tutkimuksessa käsitellyt aiheet ovat todella laajoja, joten lähes jokaiseen käsiteltyyn aihealueeseen perehtyminen syvällisemmin on mahdollista.

8.3 Tutkimuksen luotettavuus ja pätevyys

Tutkimuksen lähteinä käytettiin viranomaisten julkaisemaa materiaalia, joka liittyy olennaisesti käsiteltyyn aihealueeseen. Lisäksi materiaalia ja lähdeaineistoa kerättiin suurien tietoturvatalojen ja alan ammattilaisten blogikirjoituksista ja artikkeleista. Myös akateemista aiheeseen liittyvää kirjal-

lisuutta käytettiin työn lähdemateriaalina. Materiaalia pyrittiin keräämään kuitenkin mahdollisimman monen eri viranomaisen ja julkaisijan lähteistä, jolloin tutkimukseen kyettiin muodostamaan mahdollisimman puolueeton näkökulma. Tapausesimerkeissä yhdisteltiin tutkimuksen tuottajan omaa analysointia ja pohdintaa sekä tietoturvatalojen ja blogikirjoittajien näkemystä aiheista laajemman kokonaiskuvan luomiseksi.

Tutkimuksessa ei tuotettu mielipidekyselyitä eikä tutkimuksen tueksi suoritettu virallisia asiantuntijahaastatteluja. Tutkimuksen tukena olisi voinut käyttää laadullisia mittareita, kuten toimeksiantajan kykyä tai vasteaikaa käsitellä julkaistavia haavoittuvuustiedotteita, tunnettuja haavoittuvuuksia tai jonkin toisen organisaation vastaavaa dataa. Kokonaisuutena minkä tahansa organisaation haavoittuvuuden hallinnan kehittäminen tai tarkastelu vaatisi oman tutkimuksensa tai opinnäytteensä.

Lähteet

Alvarenga, G. 2022. DevOps vs. DevSecOps: Understanding the Difference. Artikkeli tietoturvayhtiö Crowd Striken verkkosivuilla. 15.9.2022. Viitattu 16.2.2024. https://www.crowdstrike.com/cybersecurity-101/cloud-security/devops-vs-devsecops.

ArcaneDoor - New espionage-focused campaign found targeting perimeter network devices. 2024. Blogikirjoitus Cisco Talos:n verkkosivuilla. 24.4.2024. Viitattu 1.5.2024. https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices.

Bar, M., Cohen, A. & Aminov, D. 2024. Backdoor in XZ Utils allows RCE: everything you need to know. Blogikirjoitus tietoturvayhtiö Wiz:n sivuilla. 30.3.2024. Viitattu 3.4.2024. https://www.wiz.io/blog/cve-2024-3094-critical-rce-vulnerability-found-in-xz-utils.

Bhatt, P. 2023. Understanding Post-Exploitation: Cybersecurity. Blogikirjoitus Mediumin verkkosivuilla. 15.11.2023. Viitattu 20.4.2024. https://medium.com/@paritoshblogs/understanding-post-exploitation-cybersecurity-5c8d11b75812.

Calder, A. 2023. Cyber Resilience: Depth-In-Depth Principles. Cambridgeshire: IT Governance. Viitattu 9.3.2024. https://janet.finna.fi, Ellibslibrary.

Drogseth, D. N., Sturm, R. & Twing, D. 2015. CMDB systems: Making change work in the age of cloud and agile. Ensimmäinen painos. Amsterdam: Elsevier. https://janet.finna.fi, Ellibslibrary.

Dugas, M. & Sabett, R. 2024. NIST Unveils Cybersecurity Framework 2.0. Artikkeli Cooleyn verkkosivuilla. 28.2.2024. Viitattu 8.4.2024. https://cdp.cooley.com/nist-unveils-cybersecurity-framework-2-0.

Exploit Public-Facing Application. 2023. Tekniikka MITRE:n ATT&CK-matriisissa. 28.11.2023. Viitattu 15.4.2024. https://attack.mitre.org/techniques/T1190.

Exploitation of Remote Services. 2022. Tekniikka MITRE:n ATT&CK-matriisissa. 24.2.2022. Viitattu 15.4.2024. https://attack.mitre.org/techniques/T1210.

External Remote Services. 2023. Tekniikka MITRE:N ATT&CK-matriisissa. 30.3.2023. Viitattu 15.4.2024. https://attack.mitre.org/techniques/T1133.

Gamblin, J. 2024. 2023 CVE data review. Blogikirjoitus. 3.1.2024. Viitattu 20.4.2024. https://jerrygamblin.com/2024/01/03/2023-cve-data-review.

Haavoittuvuudet – miten niistä ilmoitetaan oikein. 2023. Artikkeli Traficomin Kyberturvallisuuskeskuksen verkkosivuilla. 23.3.2023. Viitattu 16.2.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein.

Hasayen, A. 2022. Microsoft Defender – Indicators of Compromise IOC. Blogikirjoitus tietoturva-asiantuntijan verkkosivuilla. 27.11.2022. Viitattu 24.3.2024. https://blog.ahasayen.com/microsoft-defender-indicator-of-compromise-ioc%EF%BF%BC.

ISO/IEC 27000 Tietoturvallisuuden standardisarja. 2023. Julkaisu SFS Suomen Standardit Ry:n verkkosivuilla. 28.3.2023. Viitattu 16.2.2024. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja.

ITIL foundation : ITIL 4 edition. 2019. Lontoo: TSO. Viitattu 26.3.2024. https://janet.finna.fi, Ellibslibrary.

Judd, D. 2020. The Confidentiality Integrity Availability (CIA) Triad Write-Up. Blogikirjoitus . 27.11.2020. Viitattu 11.3.2024. https://sites.wp.odu.edu/darcyjudd/2020/11/27/the-cia-triad-write-up/.

Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. 2020. Ulkoministeriö. Viitattu 15.2.2024. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.

Kouns, B. L. & Kouns, J. 2023. The CISO perspective: Understand the importance of the CISO in the cyber threat landscape. Ely, Cambridgeshire: IT Governance Publishing. Viitattu 29.4.2024. https://janet.finna.fi, Ellibslibrary.

Kriittinen haavoittuvuus Linux-jakeluissa XZ Utils -tiedonpakkausohjelmistossa. 2024. Haavoittuvuustiedote Kyberturvallisuuskeskuksen verkkosivuilla. 29.3.2024. Viitattu 3.4.2024. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_10/2024

L 917/2014. Laki sähköisen viestinnän palveluista. Viitattu 14.2.2024. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.

Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials. 2024. Blogikirjoitus Cisco Taloksen verkkosivuilla. 16.4.2024. Viitattu 21.4.2024. https://blog.talosintelligence.com/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials.

Lin, M., Wallace, R., Wolfram, J., Andonov, D. & McLellan, T. 2024. Cutting Edge, Part 2: Investigating Ivanti Connect Secure VPN Zero-Day Exploitation. Blogikirjoitus Mandiantin verkkosivuilla. 31.1.2024. Viitattu 16.4.2024. https://www.mandiant.com/resources/blog/investigating-ivanti-zero-day-exploitation.

Lin, M., Wallace, R., Larsen, A., Gandrud, R., Thompson, J., Pearson, A. & Frazer, A. 2024. Cutting Edge, Part 3: Investigating Ivanti Connect Secure VPN Exploitation and Persistence Attempts. Blogikirjoitus Mandiantin verkkosivuilla. 27.2.2024. Viitattu 19.4.2024. https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence.

Log4j-komponentin haavoittuvuus on aktiivisen hyväksikäytön kohteena - päivitä välittömästi!. 2021. Varoitus Traficomin Kyberturvallisuuskeskuksen verkkosivuilla. 10.12.2021. Viitattu 4.3.2024. https://www.kyberturvallisuuskeskus.fi/fi/varoitus_5/2021.

Magnusson, A. 2020. Practical vulnerability management: A strategic approach to managing cyber risk. San Francisco, CA: No Starch Press. Viitattu 5.4.2024. https://janet.finna.fi, Ellibslibrary.

McLellan, T., Wolfram, J., Roncone, G., Lin, M., Wallace, R. & Andonov, D. 2024. Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation. Blogikirjoitus Mandiantin verkkosivuilla. 12.1.2024. Viitattu 15.4.2024. https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day.

Morrissey, C. 2023. Windows monthly updates explained. Blogikirjoitus Microsoftin verkkosivuilla. 21.3.2023. Viitattu 22.4.2024. https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-monthly-updates-explained/ba-p/3773544.

Most Common Types of Cyber Vulnerabilities. 2022. Artikkeli Crowd Striken verkkosivuilla 14.2.2022. Viitattu 15.2.2024. https://www.crowdstrike.com/cybersecurity-101/types-of-cyber-vulnerabilities.

Onyegbula, B. 2023. Indicators of Compromise (IoCs): What Are They and How Do They Strengthen Cyber Defense? Blogikirjoitus Splunkin verkkosivuilla. 31.5.2023. Viitattu 24.3.2024. https://www.splunk.com/en_us/blog/learn/ioc-indicators-of-compromise.html.

Process. N.d. Artikkeli CVE:n verkkosivuilla. Viitattu 15.3.2024. https://www.cve.org/About/Process.

Puolustusvoimien johtamisjärjestelmäkeskus. N.d. Puolustusvoimien verkkosivut. Viitattu 20.2.2024. https://puolustusvoimat.fi/tietoa-meista/johtamisjarjestelmakeskus.

Reducing the Significant Risk of Known Exploited Vulnerabilities. 2024. Katalogi America’s Cyber Defence Agency CISA:n verkkosivuilla. Viitattu 18.2.2024. https://www.cisa.gov/known-exploited-vulnerabilities.

Replication Through Removable Media. 2023. Tekniikka MITRE:n ATT&CK-matriisissa. 17.10.2023. Viitattu 25.4.2024. https://attack.mitre.org/techniques/T1091.

Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094. 2024. Varoitus CISA:n verkkosivuilla. 29.3.2024. Viitattu 3.4.2024. https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, MA., Amir, A., Vuda, KV. & Sarwat, AI. 2023. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Artikkeli Yhdysvaltain kansallisen lääketieteellisen kirjaston sivuilla. https://janet.finna.fi, Ellibslibrary.

Sesto, V. 2022. Practical Ansible: Configuration Management from Start to Finish. Toinen, uudistettu painos. New York City: Apress. Viitattu 10.3.2024. https://janet.finna.fi, Ellibslibrary.

Steinberg, S. 2022. Cybersecurity For Dummies. Toinen, uudistettu painos. Hoboken, New Jersey: John Wiley & Sons. Viitattu 26.3.2024. https://janet.finna.fi, Ellibslibrary.

Stokel-Walker, C. 2023. The top 4 instances when a weak password led to a major hacking incident. Cybernews. 4.5.2023. Viitattu 17.2.2024. https://cybernews.com/security/cost-of-week-password-hacking.

Sutton, D. 2022. Cyber security: The complete guide to cyber threats and protection. 2nd ed. Lontoo: BCS Learning and Development Limited. Viitattu 16.4.2024. https://janet.finna.fi, Ellibslibrary.

The NIST Cybersecurity Framework (CSF) 2.0. 2024. Julkaisu NIST:n verkkosivuilla. 26.2.2024. Viitattu 18.4.2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways. 2024. Varoitus CISA:n verkkosivuilla. 29.2.2024. Viitattu 21.4.2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b.

Tietosuoja. 2024. Artikkeli Tietosuojavaltuutetun toimiston sivuilla. Viitattu 16.2.2024. https://tietosuoja.fi/tietosuoja.

Tietoturva. 2020. Artikkeli Traficomin Kyberturvallisuuskeskuksen verkkosivuilla. 9.7.2020. Viitattu 16.2.2024. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

Titterington, A. 2024. The principle of least privilege: what is it and why is it needed? Tietoturvayhtiö Kaspersky. 12.1.2024. Viitattu 17.2.2024. https://www.kaspersky.co.uk/blog/what-is-the-principle-of-least-privilege/27125.

Top 8 Cyber Security Vulnerabilities. 2023. Artikkeli Chek Point:n verkkosivuilla. 11.1.2023. Viitattu 15.2.2024. https://www.checkpoint.com/cyber-hub/cyber-security/top-8-cyber-security-vulnerabilities.

Understanding vulnerabilities. 2015. Artikkeli NCSC UK:n verkkosivuilla 13.10.2015. Viitattu 15.2.2024. https://www.ncsc.gov.uk/information/understanding-vulnerabilities.

Viegas, V. & Kuyucu, O. 2022. IT security controls: A guide to corporate standards and frameworks. New York City: Apress. https://janet.finna.fi, Ellibslibrary.

VMware Security Advisories. 2024. Katalogi VMwaren verkkosivuilla. Viitattu 18.3.2024. https://www.vmware.com/security/advisories.html.

Vulnerability Metrics. 2023. Artikkeli US Department of Commerce:n National Institute of Standards and Technology verkkosivuilla. 6.11.2023. Viitattu 17.2.2024. https://nvd.nist.gov/vuln-metrics/cvss.

Watts, S. 2019. Introduction to ECAB: Emergency Change Advisory Board. Blogikirjoitus BMC:n verkkosivuilla. 23.10.2019. Viitattu 23.4.2024. https://www.bmc.com/blogs/ecab-emergency-change-advisory-board.

What are CVSS Scores. 2022. Artikkeli tietoturvayhtiö Balbixin verkkosivuilla. 4.8.2022. Viitattu 19.3.2024. https://www.balbix.com/insights/understanding-cvss-scores.

What is DevOps? 2023. Artikkeli Microsoftin verkkosivuilla. 25.1.2023. Viitattu 16.2.2024. https://learn.microsoft.com/en-us/devops/what-is-devops.

What Is a Zero-Day Vulnerability Exploit? 2022. Artikkeli Microsoftin verkkosivuilla. 25.11.2022. Viitattu 16.2.2024. https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/zero-day-vulnerability-exploit.

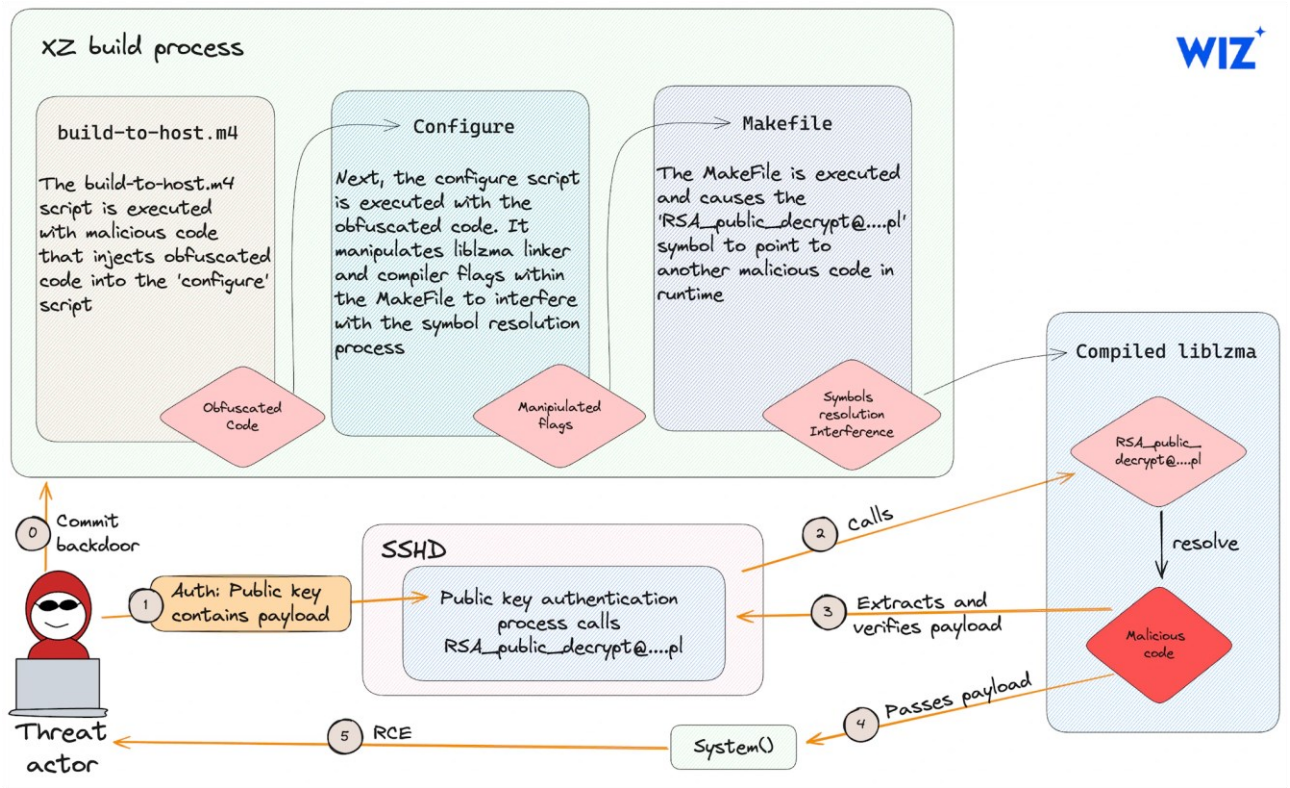
What is vulnerability management? N.d. Artikkeli Microsoftin verkkosivuilla. Viitattu 16.4.2024. https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management.

XZ Utils Backdoor — Everything You Need to Know, and What You Can Do. 2024. Blogikirjoitus tietoturvayhtiö Akamain verkkosivuilla. 1.4.2024. Viitattu 3.4.2024. https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know.

Zero-Day. 2022. Artikkeli ENISA:n verkkosivuilla. 29.11.2022. Viitattu 16.2.2024. https://www.enisa.europa.eu/topics/incident-response/glossary/zero-day?v2=1.

Liitteet

Liite 1. Kuvaus XZ Utils -haavoittuvuuden teknisestä toteutuksesta



Kuvio 9: XZ Utils (Bar, Cohen & Aminov 2024).