IP-valvontakameroiden tietoturvallisuus

Taneli Syrjälä

2021 Laurea

Laurea-ammattikorkeakoulu

IP-valvontakameroiden tietoturvallisuus

Taneli Syrjälä
Turvallisuusala
Opinnäytetyö
Tammikuu 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusala

Turvallisuusala, tradenomi (AMK)

Taneli Syrjälä

IP-valvontakameroiden tietoturvallisuus

Vuosi 2021 Sivumäärä 34

Opinnäytetyön tarkoitus oli selvittää IP-valvontakameroihin kohdistuvan tietoturvauhan yleisyyttä, laajuutta, ominaispiirteitä sekä hyviä käytänteitä tietoturvan kehittämiseksi. Tavoitteena oli tuottaa tietoa IP-valvontakameroihin liittyvästä tietoturvauhasta toimeksiantajayrityksen hyödynnettäväksi.

Opinnäytetyön teoreettinen viitekehys muodostui IP-valvontakamerajärjestelmien toiminnasta, käyttötarkoituksesta sekä tietoturvallisuudesta ja sen merkityksestä organisaation toiminnalle. Merkittävimpinä lähteinä teoriapohjan luomisessa olivat kirjallisuusmateriaalit sekä erilaiset artikkelit ja julkaisut.

Tutkimuksessa käytettyjä tutkimusmenetelmiä olivat kirjallisuuskatsaus sekä teemahaastattelu. Kirjallisuuskatsauksessa käsiteltiin aiempia tutkimuksia aiheesta sekä esiteltiin tunnetuimpia IP-valvontakameroihin kohdistuneita kyberhyökkäyksiä. Teemahaastatteluita suoritettiin kolme kappaletta. Haastateltavista kaksi työskenteli tietoturvakonsulttina yksityisellä sektorilla ja yksi tietoturvapäällikkönä suuressa julkisen sektorin organisaatiossa. Haastattelut toteutettiin ennalta laadittua teemahaastattelurunkoa hyödyntäen maaliskuun 2020 aikana. Haastatteluiden teemat olivat IP-valvontakameroihin kohdistuvan tietoturvauhan yleisyys ja laajuus, tietoturvauhan ominaispiirteet ja tietoturvan parantaminen.

Tutkimuksen tuloksena ilmeni, että IP-valvontakamerat ovat kyberhyökkääjiä kiinnostavia kohteita, kuten muutkin verkkoon kytketyt laitteet. Merkittäviä haittavaikutuksia aiheuttaneita kyberhyökkäyksiä on raportoitu useita ympäri maailman. IP-valvontakameroiden tietoturvan parantamisessa keskeisiksi toiminnoiksi havaittiin tietoturvalliset salasanat, ylimääräisten porttien sulkeminen sekä erilaiset tekniset toiminnot kuten 802.1X-tekniikka.

Asiasanat: IP-valvontakamera, kyberuhka, tietoturvallisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Bachelor's Thesis

Taneli Syrjälä

Information Security of IP Surveillance Cameras

Year 2021 Pages 34

The purpose of this thesis was to research the prevalence, magnitude and quality of information security threats relating to IP surveillance cameras and to establish best practices to develop the information security of IP surveillance cameras. The objective was to produce useful information about information security threats of IP cameras for the commissioner of this thesis.

The theoretical framework of this thesis convers the functioning of IP surveillance camera systems, the purpose of the use and information security and its significance in the daily operations of an organization. The most prominent information sources in the theoretical framework were literature, articles and scientific publications.

The research methods used in this thesis were literature review and theme interview. The literature review adressed previous studies about the topic and introduced the most well-known cyber attacks on IP surveillance cameras. Three theme interviews were conducted. Two interviewees work as information security consultants and one as an information security chief in a major public sector organization. The interviews were conducted in March 2020 using a theme interview frame. Themes in the interview were prevalence and magnitude of information security threats to IP surveillance cameras, characteristics of a threat and improvement of information security.

The results indicate that IP surveillance cameras are attracting targets to cyber attackers as well as other devices connected to a network. There have been several verified attacks on IP surveillance cameras that have caused significant adverse effects around the world. Key functions in improving information security of IP surveillance cameras discovered are using stong passwords, closing additional ports and various technical functions, such as 802.1X technology.

Keywords: information security, IP surveillance camera, cyberthreat

Sisällys

1 Johdanto

Opinnäytetyön aiheena on IP-valvontakameroiden tietoturvallisuus. IP on lyhenne englanninkielisestä termistä Internet Protocol. Kyseessä on protokolla, joka siirtää tietoa Internet-verkossa. IP-valvontakamerat eroavat tavallisista valvontakameroista siten, että ne on mahdollista kytkeä internet-verkkoon. Internet-verkon välityksellä on mahdollista katsella valvontakameran kuvaa ja muuttaa kameran asetuksia. Tässä työssä käsitellään IP-valvontakameroita niiden verkko-ominaisuuksien aiheuttaman tietoturvariskin vuoksi.

Opinnäytetyön aiheen valinnan taustalla oli IP-valvontakameroiden eli verkossa toimivien valvontakameroiden tunnistetut uhkat tieto- ja kyberturvallisuuteen liittyen. IP-valvontakameroihin kohdistuvien tietoverkkohyökkäysten määrän on raportoitu kasvaneen lähivuosien aikana. Tämän lisäksi IP-valvontakameroiden tietoturvan toteutuksessa on havaittu puutteita, jotka altistavat hyökkäyksille. Huonosti suojattujen kameroiden kautta on mahdollista murtautua yritysten verkkoihin, joka aiheuttaa merkittävän riskin yritysten tietoturvallisuudelle.

Työn toimeksiantajana toimi IP-valvontakameroita valmistavan yrityksen maahantuoja Suomessa ja työn tavoitteena oli tuottaa toimeksiantajalle tietoa IP-valvontakameroiden tietoturvallisuuteen liittyen. Opinnäytetyön tarkoituksena oli vastata kysymyksiin: ”Kuinka yleisiä IP-valvontakameroihin kohdistuvat tietoverkko- ja kyberhyökkäykset, tai niiden yritykset ovat?”, ”Mitkä ovat mahdolliset seuraukset hyökkäyksistä?” ja ”Millä keinoin IP-valvontakameroiden tietoturva voidaan toteuttaa asianmukaisesti hyökkäyksiltä suojautumiseksi?”

Opinnäytetyön tarkoituksena oli kartoittaa tutkimusten, selvitysten sekä asiantuntija-arvioiden pohjalta IP-valvontakameroihin kohdistuvan tietoturvauhan yleisyyttä, laajuutta, ominaispiirteitä sekä käytänteitä tietoturvan parantamiseksi. Tarkoituksena oli selvittää, kuinka yleisiä kohteita IP-valvontakamerat ovat tietoverkkohyökkäyksille, minkä tyyppisiä tietoverkkohyökkäyksiä kameravalvontajärjestelmiin kohdistuu sekä mitkä ovat tietoverkkohyökkäysten mahdolliset seuraukset yritysten liiketoiminnan sekä tietoturvallisuuden näkökulmasta. Opinnäytetyö on tutkielmatyyppinen ja aihe rajattiin koskemaan ainoastaan IP-valvontakameroiden tietoturvallisuutta, jättäen kameravalvontaan liittyvän henkilötietojen käsittelyn ja henkilöiden tietosuojan työn rajauksen ulkopuolelle.

2 Teoreettinen viitekehys

Opinnäytetyön teoriapohja muodostui pitkälti IP-valvontakamerajärjestelmien toiminnasta, käyttötarkoituksesta sekä tietoturvallisuudesta ja sen merkityksestä organisaation

toiminnalle. Keskeisimpiä käsitteitä tässä opinnäytetyössä ovat IoT, kyberturvallisuus, kyberuhka, tietoturvallisuus, tietoturvauhka, IP-valvontakamera, tietoverkkohyökkäys ja kyberhyökkäys.

Merkittävimpinä lähteinä teoriapohjan luomisessa oli tässä työssä IP-valvontakamerajärjestelmiin, tietoturvallisuuteen ja tietoturvauhkiin liittyvät kirjallisuusmateriaalit sekä erilaiset artikkelit ja julkaisut. Näiden pohjalta pyrittiin luomaan mahdollisimman kattava teoriapohja opinnäytetyölle.

2.1 Keskeiset käsitteet

IP-valvontakamera on tietoverkkoa kuvansiirrossa hyödyntävä valvontakäyttöön tarkoitettu kamera. IP-valvontakamera muuttaa kameran tuottaman digitaaliseksi bittivirraksi, jota hyödyntäen kuva voidaan siirtää tietoverkkoa pitkin nollina ja ykkösinä kuvan tallentamiseen käytettävälle tallenninlaitteelle. (Sallinen 2011, 20.)

IoT on lyhenne englanninkielisestä termistä Internet Of Things, suomennettuna Esineiden Internet. Termiä käytetään silloin kun internetiä käytetään esineiden ja laitteiden tiedonvälityskeinona. IP-valvontakamerat kuuluvat esineiden internetiin kytkettävissä oleviin laitteisiin. Esineiden internetiin liitettävissä olevalla laitteella tarkoitetaan laitetta, jonka voi liittää internetiin tietokoneena toimivan komponentin avulla, jolla on oma IP-osoite eli verkkosovittimien yksilöimiseen käytettävä numerosarja. Komponenttina voidaan käyttää muun muassa anturia ja RFID- tai WLAN-sirua. Esineiden internetin määritelmä täyttyy myös silloin kun esineellä on yksilöllinen tunniste kuten postipaketin lähetystunnus, jonka avulla se on tunnistettavissa internetissä, vaikkei se olisikaan suoraan kytkeytynyt internetiin. (Sanastokeskus TSK 2020.)

Kyberhyökkäyksellä puolestaan viitataan tietoverkkohyökkäystä kattavampaan käsitteeseen, koska se on mahdollista implementoida myös muita keinoja hyödyntäen kuin tietoverkkoa (Turvallisuuskomitea 2018, 30). Kyberhyökkäyksestä puhuttaessa hyökkäys kohdistuu yhteiskunnalle tärkeisiin toimintoihin kuten ydinvoimalaan, liikenteen ohjausjärjestelmään tai pankkijärjestelmään, jolloin hyökkäyksen seuraukset yhteiskunnan toiminnan kannalta voivat olla merkittäviä (Sanastokeskus TSK 2020).

Kyberturvallisuus on turvallisuuskomitean (2018) mukaan tavoitetila, jossa kybertoimintaympäristö on luotettava ja jossa sen toiminta kyetään turvaamaan. Kyberturvallisuus käsitteenä kattaa toimenpiteet, joiden avulla pyritään proaktiivisesti hallita ja tarvittaessa suorittaa vastatoimenpiteitä kyberuhkia vastaan. (Turvallisuuskomitea 2018, 22.)

Kyberuhka viittaa haitalliseen tapahtumaan tai kehityskulkuun, jolla on mahdollisuus toteutua. Toteutuessaan kyberuhka altistaa siitä riippuvaisen toiminnon haitallisille seurauksille.

Kyberuhkia aiheuttavat tyypillisesti toteutuneiden tietoturvauhkien lisäksi yhteiskunnan turvallisuutta vaarantavat toimet, jotka toteutetaan digitaalisessa viestintäympäristössä. Kyberuhat kohdistuvat tyypillisesti yhteiskunnalle tärkeisiin toimintoihin ja kriittiseen infrastruktuuriin. (Turvallisuuskomitea 2018, 25.)

Tietoturvallisuudella tarkoitetaan suoritettuja toimenpiteitä, joiden avulla yritetään varmistaa tiedon saatavuus, eheys ja luottamuksellisuus. Tietoturva kattaa muun muassa tietoaineistojen, laitteistojen, ohjelmistojen turvaamisen. Tiedon saatavuudella pyritään siihen, että tieto on hyödynnettävissä silloin kun sitä tarvitaan. Eheydellä tarkoitetaan sitä, että tieto on alkuperäistä, eikä sitä olla päästy muuttamaan. Tiedon luottamuksellisuudella tarkoitetaan sitä, että tieto on saatavilla vain niille, joille se on tarkoitettu. (Turvallisuuskomitea 2018, 15.)

Tietoturvauhalla viitataan ulkoiseen tai sisäiseen tietoturvalle haitalliseen tapahtumaan. Sisäinen tietoturvauhka käsittää organisaation oman henkilökunnan aiheuttaman tietoturvauhan, kuten esimerkiksi tahattoman tietojen luovuttamisen väärälle henkilölle. Ulkoisella tietoturvauhalla tarkoitetaan organisaation ulkopuolelta aiheutuvaa uhkaa, esimerkiksi virusta. (Sanastokeskus TSK 2004.)

Tietoverkkohyökkäys on Turvallisuuskomitean (2018, 30) määritelmän mukaan teko tai toiminta, jonka tavoitteena on tietoverkkoa hyödyntäen vahingoittaa tai väärinkäyttää tietojärjestelmää, tietoverkkoa, dataa tai laitetta. Tietoverkkohyökkäyksen toteutustapoja ovat esimerkiksi palvelinestohyökkäys tai haittaohjelma.

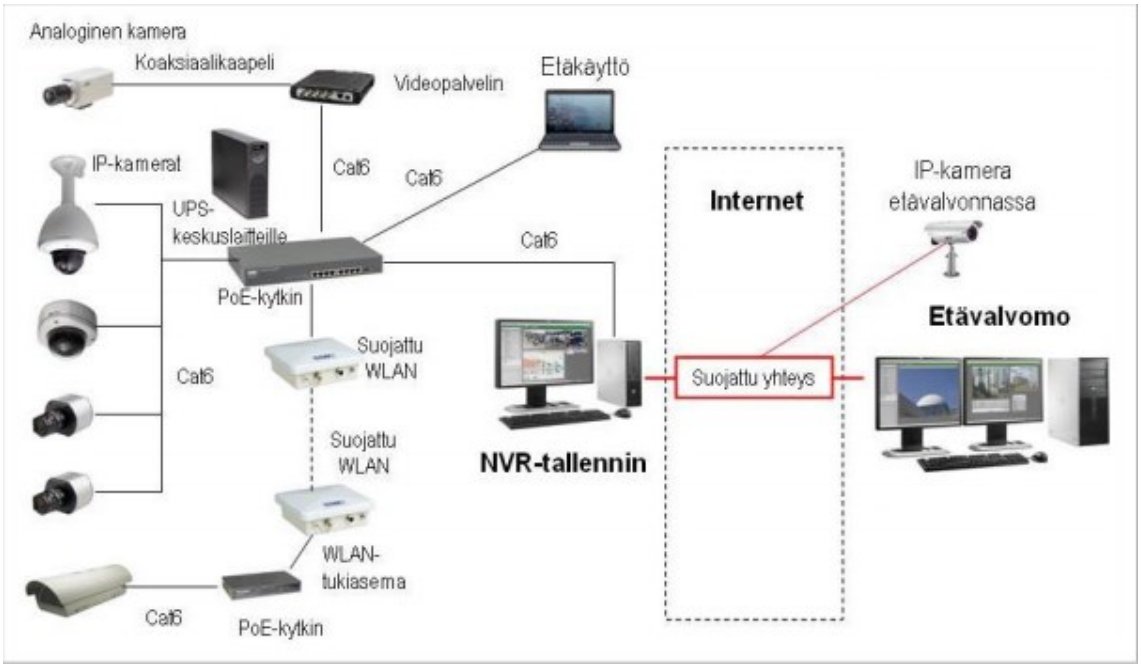
2.2 IP-Kameravalvontajärjestelmä

Kameravalvontajärjestelmä koostuu kaapeloinnista, kameroista, keskuslaitteesta, kuvantallentimesta, paikallisista monitoreista ja mahdollisesta kuvansiirrosta ulkopuoliseen valvontapisteeseen, kuten esimerkiksi vartiointiliikkeen hälytyskeskukseen. (Sähköala 2020.)

IP-kamera eli Internet Protocol- kamera on valvontakäyttöön soveltuva kamera, jonka ominaisuudet mahdollistavat sen liittämisen verkkoon ja kommunikoinnin verkossa. Etuna perinteiseen analogiseen valvontakameraan on IP-kameran käyttöönoton helppous sekä mahdollisuus etäkäyttöön ja -hallintaan. Analogiset valvontakamerat vaativat omat kaapelit ja laitteet valvontakameroille, sillä ne käyttävät analogista verkkoa. IP-kameran käyttöönottoa edesauttaa se, että useimmista moderneista kiinteistöistä löytyy Ethernet-verkkoa varten toteutetut CAT-kaapeloinnit, joihin IP-kamerat saadaan kytkettyä. (Tilavahti 2020.)

IP-kameran kuvansiirtotapa ja formaatti eroaa analogisesta kamerasta. Analoginen kamera siirtää kuvan analogisena videovirtana koaksiaalikaapelia pitkin tallenninlaitteelle tai tarkkailumonitorille. IP-kamera puolestaan muuttaa kuvainformaation digitaaliseksi bittivirraksi ja

näin ollen kuva siirtyy tietoverkkoa hyödyntäen nollina ja ykkösinä verkkotallentimelle. Kuvan digitalisoinnin mahdollistaa IP-kameran mikroprosessori, keskusmuisti sekä kuvanpakkaus- ja katseluohjelmat. (Sallinen 2011, 20.) Kuviossa 1 on esitetty verkkopohjaisen valvontakamerajärjestelmään kuuluvia komponentteja ja niiden yhteyttä toisiinsa. Kuvassa on esitettynä verkkopohjaisen kameravalvontajärjestelmän keskeisimmät komponentit. IP-kamerat saavat virran PoE-kytkimistä ja siirtävät kuvan NVR-tallentimelle koaksiaalikaapelia pitkin. Tallentimelta voidaan katsoa kameran tallentamaa kuvaa etänä suojatun WLAN-yhteyden avulla. Järjestelmän tukena voidaan tarvittaessa käyttää UPS-laitetta, joka toimii varavirtalähteenä, mikäli virransyöttö katkeaa. (Sallinen 2011, 25.)



Kuvio 1 IP-valvontakamerajärjestelmän komponentit (Sallinen 2011, 25).

IP-valvontakameraa voidaan kutsua tietokoneen ja kameran kombinaatioksi. Sen ominaisuudet mahdollistavat kuvan lähettämisen suoraan internet-verkon yli hyödyntämällä tiedonsiirrossa IP-paketteja. Verkko-ominaisuudet mahdollistavat IP-kameran kuvan katselun, hallinnan sekä kuvan tallentamisen myös etänä verkkoyhteyttä hyödyntäen. IP-kameralla on oma IP-osoite, jonka avulla laite kykenee kommunikoimaan verkossa ja näin ollen se voidaan sijoittaa mihin tahansa, missä on IP-protokollaa noudattava verkkoyhteys. (Nilsson 2017, 9.)

IP-valvontakameroiden virransyötössä voidaan hyödyntää Power over Ethernet eli PoE- tekniikkaa, joka mahdollistaa kameroiden virransyötön samasta parikaapelista, jolla kamera yhdistetään verkkoon. Näin ollen kamerat saavat sekä virran, että verkkoyhteyden yhdestä ja samasta kaapelista, mikä säästää kaapelointikustannuksia merkittävästi sekä helpottaa kameroiden fyysisten sijoituspisteiden muuttamista tarpeen vaatiessa. PoE- tekniikkaa

hyödyntämällä voidaan myös parantaa kameravalvontajärjestelmän toimintavarmuutta häiriötilanteissa käyttämällä lisäksi erillistä UPS- varavirtalähdettä, joka kytketään PoE- kytkimeen, josta kamerat saavat virtansa. Näin ollen kameravalvontajärjestelmä kykenee toimimaan myös tietyn aikaa sähkökatkoksen aikana. (Nilsson 2017, 165-166.)

2.3 Kameravalvontajärjestelmän käyttö ja tarkoitus

Kameravalvonta on menetelmä, jonka tarkoituksena on muodostaa jatkuvaa kuvallista informaatiota kiinteistön alueella tai tilassa esiintyvästä kohteesta. Kameravalvontajärjestelmän yleisin tarkoitus on rikosten ja vahingontekojen ennaltaehkäisy sekä yrityksiin kohdistuvien vahingontekojen selvittäminen jälkeenpäin hyödyntämällä kameravalvontajärjestelmän tuottamia tallenteita tapahtumista. Kameravalvontajärjestelmä viestii ympäristölle, että yritykseen kohdistuvat vahingonteot eivät jää selvittämättä, mikä pienentää vahingontekojen kohteeksi joutumisen riskiä. Rikoksentorjuntaan liittyvien tavoitteiden lisäksi valvontakameroita voidaan käyttää esimerkiksi teollisuuden ja sairaaloiden prosessien valvonnassa sekä tukemassa henkilö- ja ajoneuvoliikenteen kulunohjausta (Sallinen 2011, 6). Tulevaisuudessa kameroiden kehittyvien videoanalytiikkaominaisuuksien hyödyntäminen yleistyy muun muassa asiakasvirtojen laskennassa sekä ruuhkaselvityksissä (Nilsson 2017, 275).

Kameravalvontaa toteutetaan tyypillisesti joko reaaliaikaisesti tapahtuvana kuvan tarkkailuna esimerkiksi myymälätarkkailussa vartioiden toimesta tai passiivisena kuvamateriaalin analysointina. Reaaliaikaisesti tapahtuva tarkkailu pyrkii havaitsemaan mahdolliset rikokset välittömästi. Myymälässä toteutetussa reaaliaikaisessa tarkkailussa kameroita valvova henkilö on useimmiten radioyhteydessä myymälässä oleviin vartijoihin ja on näin ollen kykenevä ohjeistamaan heitä mahdollisiin väärinkäytöksiin puututtaessa. (Sallinen 2011, 7.)

Passiivinen kuvamateriaalin analysointi toteutetaan jälkikäteen tallenteita tutkimalla. Tarkoituksena tällöin on saada jälkikäteen selvyys kameroiden tuottaman tallennemateriaalin avulla tapahtumien kulusta. Tallenteita voidaan hyödyntää esimerkiksi onnettomuuksien tai rikoksen tutkinnassa jälkikäteen. Niiden avulla pyritään tunnistamaan rikoksen tekoon liittyviä henkilöitä, teko-olosuhteita ja helpotetaan rikoksentekijän tunnistamista. Materiaali myös auttaa tuomioistuinta saamaan kokonaiskuvan tapahtuneesta. (Sallinen 2011, 7.)

2.4 Kameravalvontajärjestelmien älykkäät ominaisuudet

Moderneissa kameravalvontajärjestelmissä on paljon älykkäitä ominaisuuksia, joita voidaan hyödyntää valvonnan tehostamisessa. Yksi tunnetuimmista ja yleisimmin käytössä olevista ominaisuuksista on liikkeentunnistus, joka mahdollistaa valvontakameroiden tallentamisen ainoastaan silloin kun ne havaitsevat liikettä. Näin ollen säästetään merkittävästi tallennustilaa, kun valvontakamerat tallentavat kuvaa ainoastaan havaitessaan liikettä. Liiketunnistus mahdollistaa myös tietyn alueen rajaamisen kuva-alueesta, josta halutaan tunnistaa liikettä.

Liiketunnistuksen avulla voidaan asettaa kamera antamaan hälytyksen tietynlaisesta toiminnasta, kuten henkilön liikkumisesta kielletyllä alueella (Nilsson 2017, 277-278.)

Toinen yleistyvä kameravalvontajärjestelmän älykäs ominaisuus on rekisterikilven tunnistus, jota käytetään muun muassa parkkihallien kulunvalvonnassa. Rekisterikilven tunnistamisen avulla on mahdollista rajata sisäänpääsy parkkihalliin ajoneuvon rekisterinumeron perusteella. Käytännössä tämä toimii siten, että kuljettajan ajaessa halliin sisään ja sieltä ulos parkkihallin puomi nousee automaattisen rekisterinumeron tunnistamisen perusteella. Toimintoa voidaan myös hyödyntää pysäköinnin valvontaan tarkastelemalla sitä, kuinka kauan ajoneuvo on pysäköitynä. (Nilsson 2017, 292.)

Muita kameravalvontajärjestelmissä hyödynnettäviä älykkäitä ominaisuuksia ovat kasvojentunnistus, henkilölaskenta, äänentunnistus sekä tulen ja savun tunnistaminen (Nilsson 2017, 275-295). Caputo (2010, 203) toteaa kameravalvontajärjestelmien älykkäiden ominaisuuksien merkittävästi valvontaa helpottavana ja tehostavana tekijänä, sillä suuren kameramäärän valvominen vaatisi perinteisesti toteutettuna paljon työntekijöitä. Älykkäiden toimintojen avulla valvontaa voidaan tehostaa ja näin ollen henkilöstön työmäärää vähentää. Kun henkilöstöllä on paljon kameroita katseltavana, on hyvin epätodennäköistä havaita tapahtumia juuri sillä hetkellä katseltavassa kamerassa. Tässä asiassa kameroiden älykkäistä ominaisuuksista on paljon hyötyä, sillä kun valvontakamera havaitsee jotain poikkeavaa toimintaa, se hälyttää, mikä edesauttaa kameravalvonnan suorittamista tehokkaasti.

2.5 Tietoturvallisuus

Elinkeinoelämän keskusliiton (2016) mukaan tietoturvallisuus on yritysturvallisuuden yksi osaalue ja sen tärkeimmät suojattavat arvot ovat tietojen eheys, saatavuus ja luottamuksellisuus. Eheydellä tarkoitetaan tiedon muuttumattomana pysymistä tiedonkäsittelyn eri vaiheissa, saatavuudella tiedon käytettävyyden varmistamista ja luottamuksellisuudella sitä, ettei suojattava tieto päädy ulkopuolisten saataville (Helsingin kaupunki 2020).

Kuvio 2 Tiedon luottamuksellisuus, eheys ja saatavuus muodostavat tietoturvallisuuden kokonaisuuden (Maskulin 2018, 9.)

Termejä tietoturvallisuus ja kyberturvallisuus käytetään usein ristiin. Molemmissa termeissä kyse on pitkälti samasta asiasta, joka on datan suojaaminen sekä tietojärjestelmien asianmukaisen toiminnan varmistaminen. Eron näiden kahden termin välille tekee toiminnan tavoitteet. Tietoturvallisuudella pyritään tietojen, tiedostojen ja yksittäisten tietokoneiden suojaamiseen. Tietoturvallisuudesta on siis kyse silloin kun esimerkiksi varmuuskopioidaan tiedostoja, asennetaan päivityksiä ja asetetaan salasanoja. Kyberturvallisuudesta on kyse silloin kun tietoturva linkittyy yhteiskunnan peruspalveluihin kuten sähkön ja veden jakeluun sekä tietoliikenneyhteyksien toimintaan yhteiskunnallisella tasolla. Termiin kyberturvallisuus liittyy siis vahvasti yhteiskunnallisilta vaikutuksiltaan merkittävät uhkakuvat kuten verkkopankin kaatuminen, kun taas tietoturvallisuus kattaa pienemmän mittakaavan uhkakuvat kuten yksittäisen tiedoston katoamisen tai salasanojen urkinnan. (Järvinen 2018, 14-15.)

2.6 Hallinnollinen tietoturvallisuus

Organisaation tietoturvallisuuden perustana pidetään usein hallinnollista tietoturvallisuutta, jolla pyritään luomaan organisaatiolle toimintatavat, jotka tukevat tietoturvallisuuden asianmukaista toteuttamista. Hallinnon tehtävä organisaatiossa on määritellä tietoturvallisuuden pääperiaatteet laajemmassa mittakaavassa ja määrittää toimenpiteet, jotka tehdään tietoturvallisuuden edistämiseksi. Hallinnollisen tietoturvallisuuden perustana toimivat erilaiset standardit, suositukset, toimintatavat sekä hyväksytyt käytänteet. Näiden avulla on mahdollista varmistaa tietoturvallisuuden kehittäminen ja johtaminen luomalla edellytykset

yrityksen tietoturvallisen toiminnan ylläpitämiselle ja ihmisten johtamiselle. (Hakala, Vainio & Vuorinen 2006, 10-11.)

Tietoturvallisuuden organisoinnissa keskeistä on, että se tukee organisaation perustehtävää ja strategian määrittelemien tavoitteiden saavuttamista. Tietoturvallisuuden toteutuksessa keskeistä on myös kustannustehokkuus ja se, että tietoturvallisuus on osa organisaation käytännön toimintaa sekä kokonaisvaltaista riskienhallintaa muodostaen perustan jatkuvuussuunnittelulle ja toimintavarmuudelle. Keskeisessä roolissa tietoturvallisuuden hallinnassa on organisaation johto, jolla on merkittävä rooli tietoturvallisuuden suunnittelussa, ylläpidossa ja kehittämisessä. Johdon vastuulla on myös huolehtia riittävistä resursseista tietoturvallisuuden toteuttamiseen. (Andreasson & Koivisto 2013, 32-33.)

Organisaation johdon lisäksi keskeinen rooli tietoturvallisuuden toteutumisessa on tietoa käsittelevillä ihmisillä, joiden toiminta on erittäin keskeistä tiedon suojaamisessa. Organisaatiossa on erittäin tärkeää kouluttaa tietoa käsitteleviä ihmisiä tiedon asianmukaiseen käsittelemiseen liittyen, sillä tiedon vuotaminen väärille tahoille saattaa aiheuttaa vahinkoa yritykselle, josta tieto on peräisin. Kun organisaatiossa työskentelevät ihmiset on koulutettu toimimaan käsittelemään tietoa oikein, on yrityksellä mahdollisuus vedota tahalliseen toimintaan tietovuodon sattuessa. (Leppänen 2006, 263-265.)

2.7 Tekninen tietoturvallisuus

Tekninen tietoturvallisuus on jaettu Puolustusministeriön (2015) mukaisesti tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuteen. Tietoliikenneturvallisuus viittaa yrityksen tietoverkon rakenteellisiin ja verkkoliikenteeseen liittyviin turvallisuusvaatimuksiin kuten verkkoyhteyksien toteuttamiseen. Tietojärjestelmäturvallisuus sisältää muun muassa järjestelmien pääsyoikeuksien hallinnan, haittaohjelmasuojauksen ja käyttäjätilien todentamisen. Tietoaineistoturvallisuudella tarkoitetaan yrityksen tietojen siirtämistä, tietojen tulostamista, kopiointia ja hävittämistä. Käyttöturvallisuus pyrkii puolestaan varmistamaan, että yrityksen tietoaineistojen käyttö on riittävän turvallista koko niiden elinkaaren ajan.

Tekniseen tietoturvallisuuteen kuuluvia tekijöitä on syytä huomioida esimerkiksi verkon suunnitteluvaiheessa. Verkon suunnittelussa olennaista on tietää tarkasti, mitä laitteita verkkoon aiotaan liittää ja minkälaista on tieto, jota verkossa siirretään. Oleellista teknisen tietoturvallisuuden toteutuksessa on myös verkon suojaaminen sisältäen muun muassa asianmukaisen palomuurin verkon osien erittelyyn sekä verkon suojaamisen hyödyntämällä porttikohtaista autentikointia, jolla estetään ulkopuolisen henkilön kytkeytyminen organisaation verkkoon omalla laitteellaan. (Andreasson & Koivisto 2013, 70-75.)

3 Tutkimusmenetelmät

Tämä opinnäytetyö on tutkielmatyyppinen ja opinnäytetyössä hyödynnettäväksi menetelmäksi valikoitui kvalitatiivinen tutkimus, joka soveltui ominaispiirteidensä vuoksi hyvin tavoitteeseeni selvittää IP-valvontakameroihin kohdistuvan tietoturvauhan yleisyyttä, ominaispiirteitä sekä vaikuttavuutta. Pääasialliseksi menetelmäksi aineiston hankkimiseen käytettiin teemahaastattelua, joka eteni ennalta valittujen teemojen mukaisesti.

Opinnäytetyössä käytettävä laadullinen eli kvalitatiivinen tutkimus on tarkoituksenmukainen tutkimusmenetelmä siinä tapauksessa, kun tutkittavaa ilmiötä ei entuudestaan tunneta kovin hyvin. Kun tutkittava ilmiö on tuntematon, ei ole myöskään olemassa teorioita, jotka selittäisivät, mistä ilmiössä on kysymys. (Kananen 2017, 16–17.)

3.1 Laadullinen tutkimus

Laadullisen tutkimuksen pääasiallisena tarkoituksena on pyrkiä kuvaamaan ja ymmärtämään tutkittavaa ilmiötä syvällisemmin sekä laajemmin verrattuna määrälliseen, eli kvantitatiiviseen tutkimukseen, joka pohjautuu pitkälti määriin eli lukuihin (Kananen 2017, 35). Laadullinen tutkimus ei ole kuitenkaan täysin päinvastainen määrällisen eli kvantitatiivisen tutkimuksen kanssa. Kvalitatiivinen ja kvantitatiivinen tutkimustyyli ovat lähestymistapoja, joilla on toisiaan täydentävät suuntauksensa (Hirsjärvi, Remes ja Sajavaara 1997, 127).

Laadullisissa tutkimuksissa tulosten analysointi ja tutkittavan aihealueen ymmärtäminen on merkittävässä roolissa. Tutkittavan aiheen ymmärrystä on laadullisessa tutkimuksessa syytä pyrkiä tuomaan ilmi jo tutkimuksen aikana eikä ainoastaan sen lopussa. (Kananen 2017, 35.)

3.1.1 Laadullisen tutkimuksen eettisyys

Tutkimuseettisten ongelmien voidaan nähdä jakaantuvan kahteen luokkaan. Tiedonhankinta ja tutkittavien suoja sekä tutkijan vastuu tutkimustulosten sovelluksista. (Mäkelä 1987, 180.) Tässä opinnäytetyössä ei tutkita yksilöitä vaan ilmiötä. Tästä huolimatta opinnäytetyön tietoperustan rakentamiseen kerätään tietoa yksilöiltä muun muassa haastatteluiden muodossa. Haastateltavilta ei kuitenkaan kerätä yksilöiden henkilökohtaisia tietoja, vaan ainoastaan näkemyksiä tutkittavaan aiheeseen. Haastateltavien nimiä ei myöskään julkaista valmiissa opinnäytetyössä.

Tietoa hankitaan enimmäkseen julkisista lähteistä kuten standardeista, kirjallisuudesta ja tutkimuksista. Toimeksiantajayrityksen opinnäytetyön tekemisen tueksi luovuttamat sisäiset dokumentit ovat luottamuksellisia eikä niiden sisältöä julkaista valmiissa opinnäytetyössä. Merkittävä osa opinnäytetyön tutkimustuloksista on kuitenkin julkista tietoa, joka on kaikkien saatavilla eikä näin ollen ole salassa pidettävää tietoa.

3.1.2 Laadullisen tutkimuksen luotettavuus

Koko tutkimusprosessiajan on tärkeää arvioida tutkimuksen tasoa, johtopäätöksen pätevyyttä sekä tutkimuksen luotettavuutta. Tutkimuksen luotettavuudessa voidaan käyttää erilaisia aineistotyyppejä, näkökulmia analyysimenetelmiä sekä teorioita. Kun näitä kaikkia käytetään samanaikaisesti, on kyse tällöin triangulaatiosta (Tutkimuksen toteuttaminen. 9.3.2010).

Tutkimuksen onnistumisen kannalta merkittävää on sen luotettavuuden arviointi. Laadullisessa tutkimuksessa ei pystytä määrittämään suoranaisesti reliabiliteettia eikä validiteettia, kuten määrällisessä tutkimuksessa. Reliabiliteetti tarkoittaa lyhyesti tuloksien toistettavuutta. Tässä tutkimuksessa hyödynnettiin menetelmänä ihmisten haastatteluita, eivätkä nämä ole toistettavissa. Validiteetti tarkoittaa puolestaan sitä, että tutkimukseen on valittu juuri siihen sopiva tutkimusmenetelmä. Luotettavuuden mittarina laadullisessa tutkimuksessa käytetään yleisesti sitä, kuinka tarkasti ja läpinäkyvästi tulokset ja tutkimuksen kulku ovat kerrottuna. Haastatteluiden mahdollisista häiriötekijöistä tai virhetulkinnoista on syytä viestiä avoimesti. (Hirsjärvi ym. 2014, 232-233.)

3.2 Kirjallisuuskatsaus

Kirjallisuuskatsauksella tarkoitetaan metodia ja tutkimus etikkaa, joka tutkii aikaisemmin tehtyä tutkimusta aiheeseen liittyen. Kirjallisuuskatsauksen avulla pyritään tekemään niin sanotusti ”tutkimus tutkimuksesta”, mikä tarkoittaa sitä, että kootaan yhteen aikaisemmin tehtyjen tutkimusten tuloksia ja näin ollen luodaan pohja uudelle tutkimukselle ja sen tuloksille. Kirjallisuuskatsaukset on mahdollista jakaa kolmeen pääluokkaan, jotka ovat kuvaileva, systemaattinen ja meta-analyysi. (Salminen 2011, 4-6.)

Kirjallisuuskatsausta hyödyntäen pyritään ymmärtämään opinnäytetyön aihepiirin kokonaisuutta. Sitä hyödyntämällä saadaan tietoa siitä, miten paljon tutkimustietoa on olemassa, millaisesta näkökulmasta aihetta on tutkittu ja millaisin menetelmin. Teoreettinen viitekehys perustuu systemaattiseen tiedonhakuun. Tämä teoreettinen viitekehys on kirjallisuuskatsaus (eli tutkimuskatsaus), jossa kuvataan opinnäytetyön käsitteellistä taustaa ja miten tekeillä oleva työ liittyy jo olemassa oleviin tutkimuksiin (Hirsjärvi ym. 2014, 121). Tässä opinnäytetyössä teoreettinen viitekehys ja kirjallisuuskatsaus on käsitelty eri osioissa. Teoreettisessa viitekehyksessä käsitellään aihealueita ja keskeisiä käsitteitä, joista opinnäytetyön teoriapohja muodostuu. Kirjallisuuskatsauksessa puolestaan käsitellään aikaisempia tutkimuksia ja esimerkkitapauksia IP-valvontakameroihin kohdistuneista tietoverkkohyökkäyksistä.

3.3 Teemahaastattelu

Teemahaastattelu kuuluu keskeisiin laadullisessa tutkimuksessa käytettäviin aineistonkeruumenetelmiin. Teemahaastattelun avulla pyritään erittelemään tutkimusongelmista keskeiset

asiat tai teemat, joista halutaan kerätä tietoa vastauksien saamiseksi (Vilkka 2005, 101). Teemahaastattelussa keskeistä on myös huolellisesti suunniteltu aihepiiri, mutta haastattelukysymyksiä ei ole muotoiltu tarkasti (Hirsjärvi ym., 1997, 208).

Teemahaastattelussa valikoidut teemat ovat aiheita haastattelijan ja haastateltavan väliseen keskusteluun, jossa tarkoitus on saada pitkiä ja kattavia vastauksia haastateltavalta. Ominaista teemahaastattelulle on, että haastattelun aikana syntyy aihealueeseen liittyviä uusia kysymyksiä, joita ei ole ennalta suunniteltu kysyttäviksi. Tämän haastattelumuodon tarkoituksena on syventää ja laajentaa ymmärrystä tutkittavasta ilmiöstä uusien asioiden avulla, jotka haastattelussa ilmenevät. (Kananen, 2013, 93- 94.)

Teemahaastattelua toteuttaessa keskeistä on, että haastattelu on jatkuvasti haastattelijan ohjauksessa, eikä haastateltava pääse liiaksi johdattelemaan keskustelua. Riskinä teemahaastattelua käyttäessä tutkimuksessa onkin se, että haastateltava johdattelee haastattelun kulkua, jolloin haastattelusta saatava tutkimusaineisto ei vastaa täysin haastattelijan ennalta määrittelemää teemaa. Näin ollen haastattelut saattavat erota toisistaan niin paljon, ettei ole mahdollista saada tarpeeksi samankaltaista aineistoa. Tämän takia tutkijan on erittäin haastavaa muodostaa pirstaleisesta ja toisistaan eroavista aineistoista yhtenevää kokonaiskuvaa tutkittavasta ilmiöstä. (KvaliMOTV 2013.)

Teemahaastattelua toteutettaessa valmistautuminen alkaa kohderyhmän määrittelemisellä, jonka jälkeen voidaan miettiä haastattelussa hyödynnettävät teemat. Kohderyhmän määrittelyn, teemojen valitsemisen ja keskustelutyyppisen haastattelutilanteen jälkeinen toteutusvaihe on haastattelusta saadun tiedot käsitteleminen ja analysointi. (KvaliMOTV 2013.)

3.4 Tiedon analysointi

Kerätyn tiedon analysointiin valittiin menetelmäksi sisällönanalyysi. Sisällönanalyysi on menetelmä, jota hyödyntäen on mahdollista analysoida kirjalliseen muotoon saatettua materiaalia, kuten esimerkiksi kirjoja, haastatteluja sekä raportteja (Tuomi & Sarajärvi 2002, 105). Sisällönanalyysi arvioitiin soveltuvaksi menetelmäksi tähän opinnäytetyöhön, sillä sen avulla pyritään Tuomen & Sarajärven (2002,105) mukaan tuottamaan kuvaus tutkittavasta ilmiöstä tiivistetyssä ja yleisessä muodossa.

Sisällönanalyysi ei ole Tuomen & Sarajärven (2002, 105) mukaan kuitenkaan itsessään riittävä menetelmä johtopäätösten tekemiseen aineistosta. Sen avulla pyritään ensisijaisesti vain kerättyä aineisto järjestetyksi, jotta sen pohjalta voitaisiin tehdä varsinaiset johtopäätökset. Useita sisällönanalyysilla suoritettuja tutkimuksia on kritisoitu siitä, ettei tutkimuksesta ole tehty varsinaisia johtopäätöksiä kattavasti, vaan on ainoastaan esitelty sisällönanalyysillä järjestetty aineisto tutkimuksen lopputuloksena.

Sisällönanalyysiä hyödynnettiin tässä opinnäytetyössä tarkastelemalla aikeisempia tutkimuksia, selvityksiä sekä artikkeleita IP-valvontakameroiden tieto- ja kyberturvallisuuteen liittyen. Tietoa on kerätty useista eri lähteistä ja sisällönanalyysiä hyödyntäen pyritty kerätyn tiedon pohjalta muodostamaan selkeää ja kattavaa kokonaiskuvaa tutkittavasta ilmiöstä. Myös opinnäytetyötä varten haastateltujen asiantuntijoiden haastattelut kirjattiin kirjalliseen muotoon ja kerätty tieto analysoitiin sisällönanalyysia hyödyntäen. Analysoidun tiedon pohjalta pyrittiin löytämään mahdollisimmat yksiselitteiset, kattavat ja yksityiskohtaiset vastaukset tutkimuskysymyksiin sekä muodostamaan johtopäätökset tutkimuksen tuloksista. Sisällönanalyysin merkitys johtopäätösten muodostamisessa oli se, että sillä saatiin kerätty aineisto selkeästi järjestellyksi, jonka jälkeen johtopäätösten tekeminen tutkimuksen tuloksista oli huomattavasti helpompaa.

4 Kirjallisuuskatsaus IP-valvontakameroihin kohdistuvasta tietoturvauhkasta

IP-pohjainen kameravalvontajärjestelmä toimii verkossa, jolloin sen tietoturvallisuuteen on syytä kiinnittää huomiota. Kartano (2019) korostaa artikkelissaan valvontakameroiden tietoturvan laiminlyönnin haitallisuutta. Hän toteaa, että mikäli valvontakameraan kohdistuvan tietoverkkohyökkäyksen tekijä pääsee murtautumaan kameravalvontajärjestelmään, on tekijällä mahdollisuus luoda väärää dataa, manipuloida kuvasisältöjä, kuunnella ääntä valvontakameran mikrofonia hyödyntäen tai varastaa järjestelmässä olevia salasanoja. Nämä toimet vaarantavat valvontakameroiden keräämän datan eheyden ja on näin ollen merkittävä tietoturvauhka. Verkossa toimiva kameravalvontajärjestelmä on sen verkko-ominaisuuksien takia myös laajempi uhka organisaation tietoturvallisuudelle, sillä haavoittuvaa laitetta on mahdollista käyttää eräänlaisena porttina, jonka kautta organisaation luottamukselliseen tietoon voi päästä käsiksi vaarantaen täten organisaation tiedon eheyden, luottamuksellisuuden ja saatavuuden (Ndichu 2019).

Japanilaisyritys Trend Micro on raportoinut estäneensä yli 5 miljoonaa IP-valvontakameroihin kohdistuvaa kyberhyökkäystä ainoastaan viiden kuukauden ajanjaksolla. Tunnistetuista hyökkäyksistä yli 75 prosenttia oli väsytyshyökkäyksiä, jotka pyrkivät salasanojen selvittämiseen. Yritys toteaakin, että IP-pohjaisiin valvontalaitteisiin kohdistuva tietoturvauhka on kasvamaan päin ja IP-valvontakamerat ovat haavoittuvia kyberhyökkäyksille. IP-valvontakameroiden tietoturvan haavoittuvuutta lisää valmistajien haluttomuus kiinnittää huomioita valmistamiensa valvontakameroiden tietoturvallisuuteen. (Cybersecurity Insiders 2020.)

Eräs merkittävä raportoitu haavoittuvuus valvontakameroiden tietoturvaan liittyen on oletussalasanat ja -käyttäjätunnukset, jotka ovat helposti selvitettävissä. Oletussalasanojen ja -käyttäjätunnusten avulla hyökkääjä pääsee helposti kirjautumaan kameran hallintapaneeliin internet-yhteyttä hyödyntäen. Tätä haavoittuvuutta hyödynnettiin esimerkiksi tunnetussa

Mirai botnet -palvelunestohyökkäyksessä vuonna 2016. Tähän ongelmaan on kuitenkin havahduttu, ja nykyisin suurin osa IP-valvontakameroiden valmistajista pakottaa käyttäjän asettamaan salasanan käyttöönoton yhteydessä, jolloin kamerassa ei voi olla oletussalasanaa käyttöönoton jälkeen. (IoT World Today 2019).

Oletussalasanojen ja -käyttäjätunnusten lisäksi IP-valvontakameroihin kohdistuu samanlaisia tietoturvauhkia kuin tavallisiin tietokoneisiin, sillä IP-pohjaiset valvontakamerat ovat käytännössä tietokoneen ja valvontakameran yhdistelmä. Adams (2018) raportoi artikkelissaan, että vuonna 2017 Yhdysvaltain Presidentin virkaanastujaisissa 65 prosenttia Washingtonin kaupungin ulkokameroista onnistuttiin saamaan toimintakyvyttömiksi kyberhyökkäyksellä. Tiedossa ei ole tarkalleen miten hyökkäys toteutettiin, mutta todennäköisimpänä vaihtoehtona pidetään tavallisiin tietokoneisiin tyypillisesti kohdistettuja verkkohyökkäystyyppejä kuten saastunutta USB-tikkua, väärennettyä internet-sivustoa ja tiedonkalasteluhyökkäystä.

4.1 IP-valvontakameroiden tietoturvauhan ominaispiirteet

Huolimatta siitä, että IP-pohjaisissa valvontakameroissa on paljon samankaltaista tekniikkaa, eroavat ne joiltain osin muista verkkoon kytkettävistä laitteista kuten tietokoneista ja muista esineiden internet- kategoriaan kuuluvista laitteista tieto- ja kyberturvallisuuteen liittyvien tekijöiden osalta. Tämä johtuu siitä, että IP-valvontakamerajärjestelmät ovat kyber-fyysisiä järjestelmiä, tarkoittaen sitä, että ne virtuaalisesti tukevat ja vahvistavat fyysistä turvallisuutta. Mikäli valvontakamerat onnistutaan tekemään toimintakyvyttömiksi kyberhyökkäyksellä, on se tällöin riski myös rakennuksen fyysiselle turvallisuudelle esimerkiksi kotona tai työpaikalla. Valvontakameroihin kohdistuva tietoturvauhka eroaa muista verkkoon kytkettävistä laitteista teknologisten tekijöiden lisäksi myös tietoturvanuhan aiheuttajien ja kyberhyökkäysten tekijöiden motivaation puolesta (Kalbo, Mirsky, Shabtai & Elovici 2019, 1). Myös Costin (2016, 3) raportoi IP-valvontakameroiden erovan muista verkkoon liitettävissä olevista laitteista kyber- ja tietoturvallisuuden näkökulmasta. Hän toteaa, että kameravalvontajärjestelmissä on visuaalinen ulottuvuus, joka erottaa sen muista internetiin kytkettävissä olevista laitteista. Visuaalisella ulottuvuudella hän tarkoittaa kyberhyökkäyksen tekijän mahdollisuutta valvontakameroiden kuvamateriaalin väärinkäyttöön kuten steganografiaan eli tiedon piilottamiseen kuvamateriaaliin. Steganografialla pyritään piilottamaan salaiset viestit tavalliseen informaatioon kuten esimerkiksi IP-valvontakameroiden tuottamaan kuvaan.

IP-valvontakameroihin liittyvän tietoturvauhan aiheuttajat ovat tyypillisesti hyökkääjiä, joilla on aikomuksena hyödyntää valvontakameroiden muista IoT-laitteista ja tietokoneista eroavia ominaisuuksia, jotka liittyvät pääosin kuvan tallentamiseen. Tekijät voivat tyypillisesti olla esimerkiksi varkaita, joilla on aikomuksena hyödyntää valvontakameroita maantieteelliseen tiedusteluun tai rikollisia, jotka pyrkivät kiristämään uhria kameroiden tallentamalla kuvamateriaalilla. Hyökkääjien motivaatio puolestaan liittyy tyypillisesti taloudellisen hyödyn

tavoitteluun esimerkiksi kiristyksen avulla tai vakoiluun esimerkiksi sotilaallisen tai poliittisten syiden vuoksi. Myös valvontakameroiden toiminnan häirintä rikoksen teon helpottamiseksi muun muassa palvelunestohyökkäystä hyödyntäen on yksi motivaatiotekijöistä. (Kalbo ym. 2019, 1-2.)

Myös teknologisten tietoturvaan liittyvien tekijöissä on eroa muihin verkkoon kytkettäviin laitteisiin verrattuna. Kalbo ym. (2019, 2) toteavat raportissaan, että valvontakamerajärjestelmien palvelimet pyrkivät usein olemaan avoimia järjestelmäalustoja ja yhteensopivia mahdollisimman monen kameramallin kanssa. Tästä syystä kameravalvontajärjestelmien palvelimet käyttävät usein vanhentuneita salaustekniikoita mikä altistaa hyökkäyksille. Modernit IP-valvontakamerat hyödyntävä koneoppimista kohteiden ja ihmisten jäljittämiseen sekä tunnistamiseen. Nämä tekoälymallit ovat helposti hyödynnettävissä niiden tietoturva-aukkojen takia.

4.2 Esimerkkitapauksia ja niiden seurauksia

Tässä kappaleessa esitellään tunnetuimpia raportoituja IP-valvontakameroihin kohdistuneita kyber- ja tietoverkkohyökkäyksiä. Kappaleessa käsitellään kolme tunnettua IP-valvontakameroihin liittyvää kyber-/ tietoverkkohyökkäystä ja näiden perusteella pyritään muodostamaan käsitystä siitä, että millaisia tietoturva- ja kyberuhkia IP-valvontakameroihin kohdistuu. Esimerkkitapauksissa käsitellään haavoittuvuuksia ja muita tekijöitä, jotka ovat olleet keskeisessä roolissa hyökkäyksessä. Tämän lisäksi kappaleessa kerrotaan toteutuneiden tietoverkko- ja kyberhyökkäysten seurauksista ja vaikutuksista.

4.2.1 Mirai Botnet

Lokakuussa 2016 arviolta 600 000 verkkoon kytkettyyn valvontakameraan, tallentimeen, reitittimeen ja muihin IoT- laitteisiin murtauduttiin ja niitä käytettiin bottiverkkona, eli kaapatuista laitteista muodostuvana verkkona, jonka haltija kykenee hyödyntämään sitä laittoman toiminnan kuten palvelunestohyökkäyksen tekemisessä (Adams 2018). Mirai on haittaohjelma, joka päästessään IoT- laitteen prosessoriin muuttaa laitteen osaksi etäältä hallittavaa bottiverkkoa. Se kykenee murtautumaan laitteisiin, jossa on ARC-prosessori sekä Linux-käyttöjärjestelmä. Jotta Mirai kykenee murtautumaan laitteeseen, täytyy laitteessa olla myös käytössä oletussalasana ja -käyttäjätunnus (Cloudflare 2020).

Hyökkäyksen onnistumisen mahdollisti myös tässä tapauksessa yleisesti tunnettu verkkoon kytkettyjen laitteiden haavoittuvuus eli käytössä olevat oletussalasanat ja -käyttäjätunnukset. Mirai Botnet toteutettiin siten, että hyökkääjät kehittivät ohjelmiston, joka haravoi internetverkkoa etsien sieltä laitteita, jotka ovat haavoittuvia hyökkäykselle. Löydettyjä haavoittuvia laitteita hyökkääjät hyödynsivät ottamalla ne hallintaansa ja käyttämällä niitä palvelunestohyökkäyksen toteuttamiseen (Cloudfare 2020). Merkittävä määrä Mirai Botnet -hyökkäyksessä käytetyistä kaapatuista laitteista oli IP-valvontakameroita. Tässä tapauksessa hyökkäykselle

haavoittuvia laitteita olivat ne, joissa oli käytössä Linux-järjestelmä, ARC-prosessori sekä oletussalasana ja -käyttäjätunnus. Seurauksena tästä kyberhyökkäyksestä oli monen palveluntarjoajan kotisivujen hetkellinen kaatuminen. Hyökkäyksen kohteeksi joutuneiden palveluntarjoajien joukossa oli myös suuria ja tunnettuja toimijoita kuten Twitter, Amazon ja Netflix (Cloudfare 2020).

4.2.2 Salakuuntelu

Vuonna 2019 raportoitiin suuresta haavoittuvuudesta useissa yhden maailman merkittävimmän valvontakameroiden valmistajan kameramalleissa. Kyseessä oli haavoittuvuus, joka mahdollisti sen, että valvontakameroiden mikrofonien nauhoittamaa ääntä oli mahdollista salakuunnella. Haavoittuvuus löydettiin useasta kyseisen valmistajan kameramalleista tarkoittaen sitä, että miljoonat valvontakamerat olivat sisältäneet haavoittuvuuden, joka altistaa kameran äänen kuuntelulle ilman pääsyoikeuksia myös silloin kun valvontakameran äänitoiminto on kytketty pois käytöstä. (Doffman 2019.)

Haavoittuvuus mahdollisti kameran äänitallenteiden kuuntelemisen ilman asianmukaista pääsyoikeutta. Äänitallenteisiin todettiin olevan mahdollista murtautua kolmella eri tavalla. Yksi tapa murtautua äänitallenteisiin todettiin olevan pääsyoikeudettoman yhteyden muodostaminen tietyllä komentosarjalla päätepisteeseen eli tässä tapauksessa valvontakameraan IP-osoitetta hyödyntäen. Toinen tapa oli hyödyntää VLC media player -ohjelmaa suoran verkkolähetyksen avaamiseen. Havaittiin, että VLC -ohjelma ei toista ääntä, mutta käyttämällä lisäksi erillistä pakettianalysaattoria verkkolähetys saatiin näkyviin ja tätä kautta päästiin kuuntelemaan kameran nauhoittamaa ääntä. Kolmas tapa oli ottaa selaimella suoraan yhteys valvontakameraan IP-osoitteen kautta ja lisätä siihen ”/videotalk” -pääte, jolloin oli mahdollista ladata äänitiedosto kamerasta (Honovich & Scanian). Tässä tapauksessa keskeinen osa haavoittuvuutta oli se, että nämä toiminnot kyettiin tekemään ilman tunnistautumista, sillä käyttäjätunnusta ja salasanaa ei vaadittu näiden toimintojen suorittamiseen. Kyseessä oli täten sisäänrakennettu haavoittuvuus kamerassa eli käyttäjä ei ollut kykenevä asettamaan tunnistautumista vaadittavaksi tälle toiminnolle. Myöhemmin haavoittuvuus paikattiin laiteohjelmistopäivityksellä. Laiteohjelmistopäivityksen jälkeen käyttäjätunnusta ja salasanaa vaaditaan aina kun päätepisteeseen eli valvontakameraan otetaan yhteys verkon välityksellä.

Kyseisellä tietoturvaan liittyvällä haavoittuvuudella oli suuret vaikutukset, kun se tuli julkisuuteen. Doffman (2019) kirjoittaa artikkelissaan, että valmistaja, jonka valvontakameroista haavoittuvuus löydettiin, kärsi mittavia haittoja. Yhdysvaltain hallitus kielsi kyseisen valmistajan sopimukset ja sovellukset, joiden katsottiin sisältävän kansallisen turvallisuuden rajoituksia.

4.2.3 Washingtonin ulkokameroiden hakkerointi

Tammikuussa 2017 Yhdysvaltain ennen presidentin virkaanastujaisia romanialaiset hakkerit tunkeutuivat merkittävään osaan Washingtonin valvontakameroista. Washingtonin alueella oli tuolloin 187 poliisin käytössä olevaa verkkoon kytkettyä ulkokameraa, joista 123 joutui hyökkäyksen kohteeksi. Hyökkäyksen seurauksena kamerat olivat hetkellisesti kykenemättömiä tallentamaan kuvaa. Hakkerit onnistuivat myös saamaan valvontakameroita hallinnoivat tietokoneet haltuunsa ja lähettivät sähköpostin 180 000 sähköpostiosoitteeseen, jossa uhattiin lukita valvontakameroiden hallintaan käytettävät tietokoneet siihen asti kunnes hakkerit saavat tietyn summan rahaa. Viranomaiset onnistuivat kuitenkin saamaan hakkeroinnin kohteeksi joutuneet valvontakamerat takaisin täyteen toimintakykyyn ilman maksun suorittamista hakkereille asettamalla kamerat offline-tilaan, jonka jälkeen ne puhdistettiin ja käynnistettiin uudelleen. (Dier 2017.)

4.3 Käytänteitä kameroiden tietoturvallisuuden parantamiseksi

IP-valvontakameroiden tietoturvallisuutta voidaan parantaa useilla erilaisilla menetelmillä. Asianmukaiset toimenpiteet tietoturvallisuuden edistämiseksi ennaltaehkäisevät valvontakameroiden kyber- ja tietoverkkohyökkäyksen kohteeksi joutumista. Tässä kappaleessa esitellään asiantuntija-arvioihin pohjustaen parhaimmat käytänteet IP-valvontakameroiden tietoturvallisuuden toteuttamisen tueksi.

4.3.1 Käyttäjätunnus ja salasana

Käyttäjätunnus ja salasana on yleisesti käytössä oleva tunnistamis- ja todentamismenetelmä, jotka pyrkivät rajaamaan pääsyä eri tietojärjestelmiin ja näin ollen suojaamaan tietoa (Kyberturvallisuuskeskus 2020). Nykyisin suurin osa IP-valvontakameroiden valmistajista pakottaa käyttäjän asettamaan salasanan käyttöönoton yhteydessä, jolloin kamerassa ei voi olla oletussalasanaa käyttöönoton jälkeen.

Salasanan valinnassa on syytä kiinnittää huomiota sen laatuun. Salasanan valinnassa sen pituus on yksi merkittävimmistä tekijöistä, joita tulee ottaa huomioon. Kyberturvallisuuskeskuksen (2020) mukaan pituus varjelee salasanaa sekä sosiaalisilta että teknisiltä huijauksilta, koska pitkän salasanan arvaaminen ja toistaminen on vaikeaa, vaikka sen syöttämisen näkisi. Myös tekninen selvittäminen vaikeutuu, kun salasana on riittävän pitkä. Riittäväksi pituudeksi Kyberturvallisuuskeskus arvioi noin 15 merkkiä. Pituuden lisäksi useiden erilaisten merkkien käyttö salasanassa vaikeuttaa sen murtamista.

4.3.2 802.1X-tekniikka

Yksi IP-valvontakameroihin liittyvä tietoturvariski on ulkopuolisen henkilön kytkeytyminen organisaation verkkoon irrottamalla valvontakamerassa olevan verkkokaapelin ja kytkemällä sen

omaan laitteeseensa. Tältä tietoturvariskiltä voidaan suojautua hyödyntämällä 802.1X-tekniikkaa eli porttikohtaista todentamista. Sen tarkoituksena on estää luvattoman laitteen kommunikointi lähiverkon liitäntäpisteen kautta. Sen avulla voidaan ohjata organisaation omaksi tunnistetut laitteet haluttuun verkon osaan ja tunnistamattomat laitteet esimerkiksi vierailijaverkkoon. Laitteiden pääsy voidaan myös kokonaan estää, jolloin estetään tuntemattoman laitteen pääsy organisaation omaan verkkoon ja vierailijaverkkoon. (Adreasson & Koivisto 2013, 75-76.)

802.1X-tekniikka on maailmanlaajuisesti yksi yleisimmistä käytössä olevista suojausmenetelmistä IP-valvontakameroissa. Kyseisen tekniikan merkitys korostuu erityisesti silloin, kun valvontakameran fyysinen sijainti on julkisella paikalla. 802.1X vaatii toimiakseen kolme komponenttia. Ensimmäinen on laite, esimerkiksi IP-kamera, joka pyytää pääsyä lähiverkkoon. Toinen on komponentti, joka laitteen tunnistaessaan myöntää laitteen pääsyn verkkoon, yleisimmin kytkin tai langattoman verkon tukiasema. Kolmas on palvelin, joka ohjaa verkkoon pyrkivän laitteen tunnistautumisprosessia. Mikäli verkkoon pyrkivää laitetta ei tunnisteta, se ei pääse liittymään verkkoon.

4.3.3 Laiteohjelmiston päivitys

Laiteohjelmiston päivitys tietoturvan näkökulmasta on tärkeää, sillä havaitut tietoturva-aukot yleensä paikataan päivityksillä. Esimerkiksi aiemmin opinnäytetyössä esitellyn valvontakameroiden salakuuntelun mahdollistanut haavoittuvuus paikattiin laiteohjelmistopäivityksellä. Vuonna 2019 tehty tutkimus viittasi siihen, että yli puolet IP-kameroista, joissa laiteohjelmisto ei ole ajan tasalla, sisältää tunnistetun tietoturvallisuuteen liittyvän haavoittuvuuden. Tutkimuksessa mukana ollut asiantuntija korostaa laiteohjelmiston päivityksen merkitystä ennaltaehkäisevänä toimintana tietoturvallisuuden parantamiseksi toteamalla, että yksikin vanhentuneen laiteohjelmiston omaava IP-kamera voi vaarantaa koko yrityksen tietoverkon turvallisuuden (SDM 2019).

4.3.4 Tiedonsiirron salaus HTTPS- menetelmällä

HTTPS on lyhenne sanoista Hypertext Transfer Protocol Secure ja se on verkkoviestintäprotokolla, jota käytetään tiedon salaamiseen. Erona tavalliseen selainten ja WWW-palvelimien tiedosiirrossa käytettävään HTTP-protokollaan on se, että HTTPS käyttää tiedon salaamiseen Transfer Layer Security (TLS)-protokollaa. TLS mahdollistaa tietojen salaamisen luvattomilta käyttäjiltä, jolloin verkkosivua selatessa kukaan ei pääse seuraamaan käyttäjän toimintoja verkkosivulla tai varastamaan tietoja. Tietoja ei pääse myöskään muokkaamaan tai vahingoittamaan tiedonsiirron aikana. Useissa IP-valvontakameroissa on sisäänrakennettu tuki HTTPS-yhteydelle, joka mahdollistaa kuvan katsomisen turvallisesti verkkoyhteyden avulla. (Nilsson 2017, 205.)

4.3.5 IP-osoitteen suodattaminen

Monissa IP-kameroissa on mahdollista kytkeä päälle IP-osoitteen suodattaminen (IP-filtering), joka mahdollistaa sen, että kameraan saadaan yhteys vain yhdestä tai useammasta erikseen määritellystä IP-osoitteesta. Tämän toiminnon ollessa päällä kameraan pääsee kirjautumaan verkon kautta ainoastaan tietyn IP-osoitteen omaavilla laitteilla (Nilsson 2017, 203-204.) IP-osoitteen suodattamisen tarkoituksena on rajata laitteelle pääsy ainoastaan erikseen sallituilta IP-osoitteilta, mikä estää laitteelle pääsyn tuntemattomasta IP-osoitteesta ja näin ollen vähentää tietomurron riskiä.

5 Teemahaastattelun toteutus

Opinnäytetyön keskeisenä tiedonhankinamenetelmänä oli asiantuntijoiden haastattelu aiheeseen liittyen. Haastattelu toteutettiin teemahaastatteluna ja haastateltavia oli yhteensä kolme kappaletta. Teemahaastattelu menetelmänä valikoitui siksi, että haastattelukysymyksiä oli mahdollista muokata keskustelun edetessä ja haastattelun aikana oli mahdollista johdatella haastattelua toivottuun suuntaan. Näin ollen aiheesta saatiin mahdollisimman laajasti näkemyksiä haastateltavilta.

Haastateltavista olivat kaikki useamman vuoden työkokemuksen omaavia kyber- ja tietoturvallisuuden asiantuntijoita. Haastateltavista kaksi työskenteli tietoturvakonsulttina yksityisellä sektorilla ja yksi tietoturvapäällikkönä suuressa julkisen sektorin organisaatiossa. Haastattelut suoritettiin etäyhteyden välityksellä maaliskuun 2020 aikana ja ne toteutettiin teemahaastattelurungon (liite 1) pohjalta.

Haastattelut etenivät ennalta suunniteltujen teemojen mukaisesti, jotta tutkittavasta aiheesta saataisiin mahdollisimman kattavasti näkemyksiä ja tietoa. Haastattelut nauhoitettiin ja litteroitiin, jonka jälkeen haastateltavien vastauksista pyrittiin poimimaan ranskalaisilla viivoilla keskeiset näkökulmat ja huomiot. Haastattelusta saatujen tietojen analysointiin käytettiin sisällönanalyysia, jotta haastatteluista saatua tietoa pystyttiin tiivistämään.

Haastateltavien näkemykset eivät merkittävästi poikenneet toisistaan ja esiin tulleet huomiot ja näkemykset IP-valvontakameroiden tietoturvallisuuteen liittyen olivat pitkälti samankaltaisia. Asiantuntijoiden haastatteluista ilmenneet keskeiset huomiot ja näkemykset on käsitelty opinnäytetyön tulokset ja johtopäätökset -osiossa yhdessä kirjallisuuskatsauksen tulosten kanssa.

6 Tulokset ja johtopäätökset

Tässä luvussa esitetään opinnäytetyön tulokset ja näin ollen pyritään vastaamaan opinnäytetyön tutkimuskysymyksiin. Tulokset pohjautuvat opinnäytetyön kirjallisuuskatsauksessa sekä asiantuntijoiden haastatteluissa kerättyyn lähdemateriaaliin IP-valvontakameroihin kohdistuvista tietoturvauhkista, aikaisemmista IP-kameroihin kohdistuneista tietoturvahyökkäyksistä sekä käytänteistä kameran tietoturvan parantamiseksi. Tulosten pohjalta muodostuu tutkijan itsensä tekemät johtopäätökset, joiden avulla pyritään muodostamaan mahdollisimman selkeä ja kattava kuva tutkittavasta ilmiöstä.

6.1 IP-valvontakameroihin kohdistuvien tietoverkko- ja kyberhyökkäysten yleisyys, ominaispiirteet ja seuraukset

Opinnäytetyön tutkimuskysymyksiin kuului ”Kuinka yleisiä IP-valvontakameroihin kohdistuvat tietoverkko- ja kyberhyökkäykset, tai niiden yritykset ovat?” ja ”Mitkä ovat mahdolliset seuraukset hyökkäyksistä?”

IP-kameroihin kohdistuvia tietoverkko- ja kyberhyökkäyksiä voidaan pitää melko yleisenä. Kirjallisuuskatsauksessa ilmeni, että japanilainen tietoturva-alan yritys raportoi estäneensä yli 5 miljoonaa IP-valvontakameroihin kohdistuvaa kyberhyökkäystä viidessä kuukaudessa. Näistä hyökkäyksistä merkittävä osa oli väsytyshyökkäyksiä, joilla pyrittiin selvittämään IP-kameran salasana ja tällä tavoin päästä hallinnoimaan kameraa. Kirjallisuuskatsauksessa käsiteltiin myös tunnettuja kyberhyökkäyksiä ja tietoturva-aukkoja, jotka liittyvät jollakin tavalla IP-kameroihin.

Yhtenä merkittävimpänä riskinä haastatteluiden pohjalta ilmeni yrityksen toimistoverkkoon murtautuminen IP-kameran kautta vaarantaen yrityksen verkon sisältämän tiedon luottamuksellisuuden, eheyden ja saatavuuden. Yhdeksi riskin aiheuttajaksi asiantuntijoiden haastatteluiden pohjalta tunnistettiin se, että IP-kameroissa on fyysinen USB-portti, jonka kautta hyökkääjän on mahdollista syöttää haittaohjelma kameraan, jolloin on tärkeää suojata kamera myös fyysisesti niin, ettei siihen pääse helposti käsiksi. Turvallisuusjärjestelmät – kuten kameravalvontajärjestelmät – ovat usein eri verkossa kuin toimistoverkko, missä on usein salassa pidettävää tietoa. Tästä huolimatta kameravalvontajärjestelmän verkon kautta voi olla mahdollista päästä yrityksen toimistoverkkoon, mikäli toimistoverkko on huonosti suunniteltu. Pahimmillaan hyökkääjä voi siis päästä murtautumaan IP-kameran kautta aina yrityksen verkon pääkäyttäjäksi, jolloin hyökkääjällä on pääsy käytännössä kaikkiin yrityksen verkossa oleviin tietoihin. Organisaation toimistoverkkoon murtautuminen kameravalvontajärjestelmän kautta on siis merkittävä IP-valvontakamerajärjestelmän tietoturvallisuuteen liittyvä riski organisaatiolle seurausten vakavuuden vuoksi. Todennäköisyys riskin toteutumiselle on kuitenkin hyvin

pieni ja toteutuakseen se vaatii puutteellisen kameravalvontajärjestelmän tietoturvallisuuden lisäksi myös heikosti suunnitellun toimistoverkon.

Yleisenä IP-kameroihin kohdistuvana tietoturvauhkana kirjallisuuskatsauksen sekä haastatteluiden pohjalta selvisi se, että IP-kameroihin murtaudutaan ja niitä käytetään apuvälineenä palvelunestohyökkäyksessä. Tämän tyyppisestä hyökkäyksestä esimerkkitapauksena on kirjallisuuskatsauksessa käsitelty Mirai botnet-hyökkäys vuonna 2016, jossa useita verkossa olevia IP-kameroita sekä muita IoT-laitteita käytettiin suuressa palvelunestohyökkäyksessä, joka johti usein merkittävän palveluntarjoajan kuten Netflixin ja Twitterin hetkelliseen kaatumiseen. Palvelunestohyökkäyksestä ei välttämättä seuraa merkittäviä haittoja kaapatulle IP-kameralle vaan haitta tapahtuu lähinnä hyökkäyksen kohteessa. Laite usein toimii normaalisti, vaikka sitä käytettäisiinkin palvelunestohyökkäykseen. Asiantuntijoiden haastatteluissa kävi kuitenkin ilmi, että kun kaapatun kameran kapasiteettiä käytetään palvelunestohyökkäykseen, on mahdollista, että se alkaa jossain vaiheessa aiheuttaa toimintahäiriöitä myös itse kamerassa. IP-kameraan murtautuminen mahdollistaa myös kameran toiminnan tarkoituksellisen pysäyttämisen, jolloin se ei täytä sen perustehtävää eli kuvamateriaalin tuottoa ja sen tallennusta. IP-valvontakameraan murtautuminen ja sen käyttö apuvälineenä palvelunestohyökkäyksessä on tutkimuksen perusteella riskin todennäköisyyden näkökulmasta merkittävä riski, sillä aikaisempia tapauksia on todettu useita. Riskin seuraukset IP-valvontakameroita käyttävälle taholle ovat kuitenkin melko pienet, sillä merkittävin haitta tapahtuu palvelunestohyökkäyksen kohteessa.

Tutkimuksesta selvisi myös, että IP-valvontakameroita on mahdollista käyttää salakuuntelulaitteena. Vuonna 2019 raportoitiin haavoittuvuus, joka mahdollisti pääsyn kameran äänitallenteisiin ilman pääsyoikeuksia. Haavoittuvuus paikattiin sen tultua ilmi laiteohjelmistopäivityksellä. Tapaus levisi kuitenkin laajasti julkisuuteen aiheuttaen merkittävän mainehaitan kyseiselle valmistajalle, jonka kameroista haavoittuvuus löydettiin. Seurauksena tämän haavoittuvuuden ilmi tulemisesta Yhdysvaltain hallitus hyllytti määräajaksi osan kyseisen valmistajan sopimuksista ja sovelluksista. Myös teemahaastatteluissa kävi ilmi kameroiden äänitallenteisiin liittyvä tietoturvauhka. Haastateltava asiantuntija totesi, että IP-kameraan murtautuvalla hyökkääjällä voi olla ainoana tavoitteena käyttää laitetta etäkuuntelulaitteena.

Opinnäytetyön teoriaosuudessa nousi esille IP-valvontakamerajärjestelmiin liittyvä kyber-fyysinen näkökulma, sillä järjestelmät tukevat ja vahvistavat fyysistä turvallisuutta virtuaalisesti. Tästä syystä yksi IP-valvontakameroihin kohdistuvan kyberuhan ominaispiirteistä on hyökkäyksen aiheuttama riski kiinteistön fyysiselle turvallisuudelle. Teoriaosuudessa esitelty esimerkkitapaus Washingtonissa tapahtuneesta valvontakameroihin kohdistuneesta kyberhyökkäyksestä on yksi tunnettu tapaus, jossa valvontakameroiden toimintakyvyttömäksi saattaminen kyberhyökkäyksellä on aiheuttanut merkittävän riskin rakennuksen fyysisen turvallisuuden näkökulmasta. Asiantuntijoiden haastatteluista ilmeni myös valvontakameroiden tietoturvan

linkittyminen fyysiseen turvallisuuteen myös siten, että hyökkäys on mahdollista toteuttaa tunkeutumalla kameraan fyysisesti paikan päällä, eikä etäyhteyden välityksellä, kuten useissa esimerkkitapauksissa. Mikäli käytössä oleva valvontakamera on sijainniltaan sellaisessa paikassa, että laitteeseen pääsee helposti käsiksi, on hyökkääjän mahdollista ujuttaa hyökkäysohjelma USB-tikulla kameraan.

6.2 Tietoturvan asianmukainen toteutus

Yhtenä tutkimuskysymyksenä opinnäytetyössä oli ”Millä keinoin IP-valvontakameroiden tietoturva voidaan toteuttaa asianmukaisesti hyökkäyksiltä suojautumiseksi?”. Tähän tutkimuskysymykseen pyrittiin löytämään vastauksia aikaisempien tutkimusten ja raporttien pohjalta sekä tietoturvallisuuden asiantuntijoiden haastatteluilla, jotka toteutettiin teemahaastatteluina. Haastateltavia oli kolme kappaletta ja heistä jokainen omasi mittavan kokemuksen tieto- ja kyberturvallisuuden parissa työskentelemisestä.

Yhdeksi keskeisimmistä IP-valvontakameroihin liittyvistä tietoturvauhista ilmeni hyökkääjän mahdollisuus käyttää kameraa etävakoilulaitteena. Hyökkääjän päästessä käsiksi kameran hallintapaneeliin on sillä kuvatallenteiden katsomisen lisäksi mahdollisuus kuunnella kameran tallentamaa ääntä äänitallenteista. Parhaiksi käytänteiksi kyseiseen tietoturvauhkaan ilmeni haastatteluiden pohjalta ylimääräisten porttien sulkeminen, tietoturvallisen salasanan asettaminen kameralle. Näillä toimenpiteillä pyritään estämään mahdollisimman tehokkaasti hyökkääjän pääsy kameran hallintatoimintoihin. Tietoturvallisen salasanan valinnassa huomio tulee kiinnittää erityisesti sen pituuteen, sillä pitkän salasanan arvaaminen ja toistaminen on erittäin haastavaa. Kirjallisuuskatsauksessa selvisi, että jopa 75 prosenttia IP-kameroihin kohdistuvista tietoturvahyökkäyksistä on väsytyshyökkäyksiä, joissa pyritään murtamaan salasana. Näiltä hyökkäyksiltä suojautumisessa salasanan pituudella on erittäin suuri merkitys. Riittävä pituudeksi salasanalle on arvioitu noin 15 merkkiä Kyberturvallisuuskeskuksen (2020) toimesta.

Vahvan salasanan lisäksi keskeisimmiksi keinoiksi IP-kameroiden tietoturvallisuuden parantamiseksi havaittiin erilaiset tekniset toiminnot, joista yhdeksi keskeisimmistä tunnistettiin 802.1X-tekniikka eli porttikohtainen todentaminen. Kyseisellä toiminnolla voidaan hallinnoida laitteita, jotka voidaan liittää organisaation verkkoon ja täten estämään luvattoman laitteen kommunikointi lähiverkossa olevan liitäntäpisteen kautta. Porttikohtaisen todentamisen merkitys tietoturvallisuuden näkökulmasta korostuu erityisesti tilanteissa, joissa valvontakamera sijaitsee fyysisesti paikassa, johon on helppo päästä käsiksi. Porttikohtainen todentaminen pyrkii siis estämään riskin siitä, että organisaation verkkoon päästäisiin käsiksi irrottamalla valvontakamerassa oleva verkkokaapeli ja liittämällä se omaan laitteeseen.

Teknisistä toiminnoista IP-valvontakameroiden tietoturvan parantamisen ja ylläpitämisen näkökulmasta merkittäväksi toiminnoksi tunnistettiin laiteohjelmiston päivitys. Kameroiden

valmistajat paikkaavat havaittuja tietoturva-aukkoja laiteohjelmistopäivityksillä, joten käyttäjän näkökulmasta on tärkeää pitää päivitykset ajan tasalla. Opinnäytetyön kirjallisuuskatsauksessa esiteltiin tutkimus vuodelta 2019, jossa ilmeni, että jopa yli puolet IP-kameroista, jossa ei ole asennettuna uusinta laiteohjelmistopäivitystä sisältää tunnistetun tietoturvallisuuteen liittyvän haavoittuvuuden. Asiantuntijoiden haastatteluissa ilmeni, että vaikka yrityksen tietoverkko on usein erillään kameravalvontajärjestelmän verkosta, on joissain tapauksissa mahdollista päästä kameravalvontajärjestelmän verkon kautta yrityksen sisäverkkoon ja sieltä tärkeisiin tietoihin käsiksi. Päivittämätön IP-valvontakamera voi siis pahimmillaan vaarantaa koko yrityksen verkon tietoturvallisuuden.

Muut opinnäytetyössä tunnistetut IP-kameroiden tietoturvaa parantavat tekniset ratkaisut olivat IP-osoitteen suodattaminen sekä tiedonsiirron salaus. IP-osoitteen suodattaminen selvisi hyväksi ja keskeiseksi toiminnoksi erityisesti kameroiden verkon suojaamiseen, sillä se rajaa IP-avaruutta, josta IP-kameran toimintoja voidaan suorittaa. Kyseinen toiminto mahdollistaa sen, että kameraan saadaan yhteys vain yhdestä tai useammasta erikseen määritellystä IP-osoitteesta. IP-kameroiden tiedonsiirron salaaminen on myös yksi keino parantaa niiden tietoturvallisuutta. Yleisin tiedon salauksessa käytetty verkkoviestintäprotokolla on HTTPS (Hypertext Transfer Protocol Secure), joka hyödyntää tiedonsalauksessa TLS-protokollaa. Käyttämällä tiedonsiirrossa HTTPS-verkkoviestintäprotokollaa, voidaan salata tiedot luvattomilta käyttäjiltä, jolloin verkkosivua selatessa kukaan ei pääse seuraamaan käyttäjän toimintoja verkkosivulla eikä myöskään varastamaan, muokkaamaan tai vahingoittamaan tietoja tiedonsiirron aikana.

6.3 Yhteenveto

Opinnäytetyön keskeisimpänä tarkoituksena oli saada mahdollisimman kattava käsitys IP-valvontakameroiden tietoturvauhkista sekä käytänteistä, joilla tietoturvaa voidaan parantaa. Tutkimuksen perusteella voidaan todeta, että IP-valvontakamerat ovat kyberhyökkääjiä kiinnostavia kohteita, kuten muutkin verkkoon kytketyt laitteet. Todennettuja hyökkäyksiä IP-valvontakameroihin, joista on aiheutunut merkittäviä haittavaikutuksia, on raportoitu useita ympäri maailman. Tunnetuimpana hyökkäyksenä voidaan pitää Mirai botnet -hyökkäystä, jossa arviolta 600 000 verkkoon kytkettyyn valvontakameraan, tallentimeen, reitittimeen ja muihin IoT- laitteisiin murtauduttiin käyttäen niitä bottiverkkona palvelunestohyökkäyksessä, joka aiheutti usean tunnetun palveluntarjoajan verkkosivujen kaatumisen. Palvelunestohyökkäyksissä merkittävin haitta tapahtuu muualla kuin itse kamerassa, mutta kaapatussa kamerassa saattaa esiintyä toimintahäiriöitä, jotka haittaavat kameran merkittävimmän toiminnon toteutumista eli kuvan tuottoa ja tallennusta.

Hyökkäysten yleisyyden ja mahdollisten seurausten vakavuuden pohjalta on syytä todeta, että IP-valvontakameroiden tietoturvaan on syytä suhtautua vakavasti, sillä pahimmillaan niiden kautta on mahdollista murtautua yrityksen sisäverkkoon, jossa säilytetään merkittävä määrä organisaatiolle arkaluontoista tietoa. Todennäköisyys yrityksen sisäverkkoon pääsyyn IP-kameran kautta on kuitenkin hyvin pieni ja se vaatii sen, että sisäverkko on huonosti suunniteltu.

IP-kameroiden tietoturvan asianmukaisen toteutuksen näkökulmasta keskeisimpiä asioita tutkimuksen pohjalta tietoturvalliset salasanat, ylimääräisten porttien sulkeminen sekä erilaiset tekniset toiminnot. Salasanan valinnassa merkittävin tekijä on sen pituus, sillä pitkän salasanan arvaaminen ja toistaminen on erittäin haastavaa. Teknisistä toiminnoista yksi keskeisimmistä on laiteohjelmiston päivitykset. IP-valvontakameroiden valmistajat paikkaavat havaittuja tietoturva-aukkoja laiteohjelmistopäivityksillä, joten sen ajan tasalla pitäminen edistää kameroiden tietoturvallisuutta merkittävästi. Muita keskeisiä teknisiä toimintoja tietoturvallisuuden edistämiseen ovat opinnäytetyön tulosten perusteella 802.1X-tekniikka eli porttikohtainen todentaminen, IP-osoitteen suodattaminen sekä tiedonsiirron salaaminen.

7 Pohdinta

Tutkimuksessa toteutettujen teemahaastatteluiden tulokset vahvistivat hyvin opinnäytetyön teoriapohjaa IP-valvontakameroiden kyber- ja tietoturvauhkiin liittyen. Teoriaosuuteen oli saatavilla melko kattavasti materiaalia erilaisten ennakkotapausten sekä aikaisempien aiheeseen liittyvien julkaisuiden muodossa. Täysin vastaavaa tutkimusta aiheesta ei kuitenkaan ole koskaan tehty. Materiaalin keruussa tärkeää oli kiinnittää huomiota lähteiden tasoon selvittämällä lähteen julkaisijan luotettavuutta ja asiantuntemusta tutkittavasta aiheesta.

Tutkimusta tehdessä eettiset näkökulmat otettiin huomioon ja hyvään tutkimusetiikkaa kyettiin noudattamaan. Tiedonhankinnassa kerättiin tietoa yksilöiltä haastattelun muodossa. Tiedot, joita kerättiin eivät olleet henkilökohtaisia tietoja vaan ainoastaan näkemyksiä tutkittavaan ilmiöön. Opinnäytetyön tutkimustulokset ovat julkista tietoa, eivätkä näin ollen pidä sisällään salassa pidettävää tietoa.

Haastatteluissa ilmenneet näkemykset vastasivat hyvin opinnäytetyön tutkimuskysymyksiin ja näin ollen edistivät kattavan kuvan saamista tutkittavasta ilmiöstä. Haastattelut etenivät teemahaastattelulle tyypillisesti keskustelumuodossa tutkittavaan aiheeseen liittyviä ajatuksia, näkemyksiä ja kokemuksia vaihtaen. Jokaiseen ennalta laadittuun kysymykseen saatiin kattava vastaus hyvien perusteluiden saattelemana. Haastateltavia oli kolme kappaletta, ja jokaisella heistä oli erittäin laaja tietämys ja näkemys tutkittavasta ilmiöstä. Haastateltavien näkemyksen aiheesta eivät poikenneet käytännössä millään tavalla toisistaan, joten

suuremmalle määrälle haastatteluja ei katsottu olevan tarvetta. Suurempi määrä haastatteluja olisi kuitenkin mahdollisesti lisännyt tutkimuksen luotettavuutta.

Tutkimuksen tulokset antavat riittävän selkeät ja kattavat vastaukset tutkimuskysymyksiin, jotta tuloksista voidaan muodostaa relevantit johtopäätökset. Tuloksien pohjalta pystyttiin muodostamaan riittävän kattava kuva tutkittavasta ilmiöstä. Tulokset edesauttavat ymmärtämään IP-valvontakameroiden kyberturvallisuuteen liittyviä uhkien tyyppejä, niiden yleisyyttä sekä keinoja, joilla IP-valvontakamerasta voidaan tehdä tietoturvallinen.

Tutkimusta tehdessä oma tietotaito aiheeseen liittyen on kehittynyt nopeasti. Ennen opinnäytetyötä en omannut kovin laajaa osaamista tieto- ja kyberturvallisuuteen liittyen, mutta työtä tehdessä se on kehittynyt valtavasti. Erityisesti alan asiantuntijoiden teemahaastattelut olivat opettavaisia kokemuksia. Mahdollisia aiheita jatkotutkimuksille voisi olla se, miten IP-valvontakameroiden ja muiden IoT-laitteiden tietoturvauhkia voitaisiin tuoda paremmin niiden loppukäyttäjien tietoon.

Lähteet

Painetut

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy

Caputo, A. 2010. Digital video surveillance and security. Burlington: Butterworth-Heinemann.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. Jyväskylä: Gummerus Kirjapaino Oy.

Hirsjärvi, S., Remes, P. & Sajavaara P. 2014. Tutki ja kirjoita. Helsinki: Tammi

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docendo Oy.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2017. Laadullinen tutkimus opinnäytetyönä. Helsinki: Suomen Yliopistopaino Oy.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Tietoturvallisuus. Jyväskylä: Gummerus.

Nilsson. 2017. Intelligent network video. Boca Raton: CRC Press.

Tuomi, J., & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.
Tikkanen, S., Aapio, L., Kaarnalehto, A., Kammonen, L., Laitinen, J., Mikkonen, J. & Pisto, M. 2008. Ammattina turvallisuus. Helsinki: WSOY.

Vilkka, H. 2005. Tutki ja kehitä. Helsinki: Tammi.

Sähköiset

Adams. 2017. Cyber Attacks On CCTV Systems: What Are The Risks? Viitattu 6.4.2020. https://securityelectronicsandnetworks.com/articles/2018/08/17/cyber-attacks-on-cctv-systems-what-are-the-risks/

Claudflare. 2020. What is Mirai? Viitattu 6.4.2020. https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Costin, A. 2016. Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. Viitattu 9.4.2020. https://dl.acm.org/doi/10.1145/2995289.2995290

Cybersecurity Insiders. 2020. Over 5 million Cyber Attacks on IP Cameras in just 5 months. Viitattu 2.4.2020. https://www.cybersecurity-insiders.com/over-5-million-cyber-attacks-on-ip-cameras-in-just-5-months/

Dier, A. 2017. 65% of DC Cameras Hacked Before Inauguration. Viitattu 7.4.2020. https://www.newser.com/story/253448/hackers-infiltrated-dc-camera-network-before-inauguration.html

Doffman, Z. 2019. Warning As Millions Of Chinese-Made Cameras Can Be Hacked To Spy On Users: Report. Viitattu 7.4.2020. https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/#4b03cb106bf2

Elinkeinoelämän keskusliitto. Yritysturvallisuusmalli. Viitattu 26.3.2020. https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

Helsingin kaupunki. 2020. Mitä on tietoturva? Viitattu 26.3.2020. https://kehmet.hel.fi/poikkileikkaavat-toiminnot/tietoturva-ja-tietosuoja/

Honovich, J. & Scania, J. 2019. Dahua wiretapping vulnerability. Viitattu 7.4.2020. https://ipvm.com/reports/dahua-audio?code=allow

IoT World Today. 2019. 5 Cybersecurity Lessons Related to IP Security Cameras. Viitattu 2.4.2020. https://www.iotworldtoday.com/2019/08/31/5-cybersecurity-lessons-related-to-ip-security-cameras/

Kalbo, N., Mirsky, Y., Shabtai, A. & Elovici 2019. The Security of IP-based Video Surveillance Systems. Viitattu. 8.4.2020. https://arxiv.org/pdf/1910.10749.pdf

Kartano, J. 2019. Onko turvakamerasi tietoturvariski? Viitattu 2.4.2020. https://www.kauko.com/ajankohtaista/onko-turvakamerasi-tietoturvariski

KvaliMOTV 2013. Kvalitatiivisten tutkimusmenetelmien oppimisympäristö. Viitattu 14.10.2013 http://www.fsd.uta.fi/menetelmaopetus/kvali/index.html

Kyberturvallisuuskeskus. 2020. Salasanat haltuun. Viitattu 25.4.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Maskulin, L. 2018. BYOD-laitteden tietoturva. Pro Gradu -tutkielma. Viitattu 30.3.2020. https://www.doria.fi/bitstream/handle/10024/160401/SM1258.pdf;jsessionid=31155D9627869D25F1C0462944FDAF8B?sequence=1

Ndichu, D. 2019. Cyber security and IP cameras: the threat is real. Viitattu 9.4.2020. https://www.networkmiddleeast.com/84958-cyber-security-and-ip-cameras-the-threat-is-real

Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 3.5.2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

SDM. 2019. Almost 4 in 10 Security Cameras Can Be at Risk of Cyber Attack Due to Outdated Firmware. Viitattu 23.4.2020. https://www.sdmmag.com/articles/97398-almost-4-in-10-security-cameras-can-be-at-risk-of-cyber-attack-due-to-outdated-firmware

Sähköala. 2020. Kameravalvonta. Viitattu 14.1.2020. http://www.sahkoala.fi/kiinteistoala/Turvallisuus/fi_FI/videovalvonta/

Tilavahti. 2020. Mikä ihmeen IP-kamera? Viitattu 14.1.2020. https://www.tilavahti.com/page/10/mika-on-ip-kamera

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Viitattu 10.3.2020. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Tutkimuksen toteuttaminen. 9.3.2010. Viitattu 30.11.2019. https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/tutkimuksen-toteuttaminen

Sallinen Pekka. 2011. Kameravalvontaopas. Viitattu 26.3.2020. http://www.turva-alanyrittajat.fi/doc/kameravalvonta/KAMERAVALVONTAOPAS_2010.pdf

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Viitattu 23.3.2015. http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Sanastokeskus TSK. 2004. Tiivis tietoturvasanasto. Viitattu 16.2.2020. http://www.tsk.fi/tiedostot/pdf/TiivisTietoturvasanasto.pdf

Sanastokeskus TSK. 2020. TEPA-termipankki. Viitattu 30.3.2020. http://www.tsk.fi/tepa/fi/haku/kyberhy%C3%B6kk%C3%A4ys

Kuviot

Liite 1: Teemahaastattelun runko

Teemahaastattelu IP-valvontakameroiden tietoturvallisuudesta

Tämä teemahaastattelu on yhtenä tiedonhankintamenetelmänä opinnäytetyössäni, jonka tavoitteena on selvittää IP-valvontakameroihin kohdistuvan tietoturvauhan yleisyyttä, laajuutta, ominaispiirteitä ja hyviä käytänteitä tietoturvan parantamiseksi. Haastateltavien nimiä ei julkaista valmiissa opinnäytetyössä, joten pysytte anonyymina. Vastausten analysoinnin helpottamiseksi haluaisin nauhoittaa haastattelun, sopiiko tämä teille?

Tietoturvauhan yleisyys ja laajuus

- Kuinka houkuttelevana kohteena näet IP-valvontakamerat kyberrikollisten näkökulmasta?
- Kuinka paljon tiedät tapauksia, joissa IP-valvontakameroihin on kohdistunut kyberhyökkäys tai sen yritys?
- Arveletko IP-valvontakameroihin kohdistuvien kyber- ja tietoverkkohyökkäysten kasvavan tulevaisuudessa?

Tietoturvauhan ominaispiirteet

- Minkä tyyppisiä tietoturvauhkia IP-valvontakameroihin liittyy? Yleisimmät haavoittuvuudet?
- Mitä erityispiirteitä teknisten valvontajärjestelmien tietoturvallisuuteen liittyy?
- Onko näköpiirissä uusia tietoturvaan liittyviä uhkia teknologian kehityksen myötä?

Tietoturvan parantaminen

- Kuinka hyväksi arvioit tämänhetkisen tietoturvallisuuden tason?
- Mitkä ovat keskeisimmät tekniset toiminnot IP-valvontakameroiden tietoturvallisuuden parantamiseksi?