TURUN YLIOPISTO

Verkkoon liitettyjen valvontakameroiden tekniset haavoittuvuudet

Tietotekniikan
TkK-tutkielma

Laatija:
Sami Saarinen

17.6.2025
Turku

Kandidaatintutkielma

Tutkinto-ohjelma, oppiaine: Tietotekniikka
Tekijä(t): Sami Saarinen
Otsikko: Verkkoon liitettyjen valvontakameroiden tekniset haavoittuvuudet
Ohjaaja(t): Antti Hakkala
Sivumäärä: 23 sivua
Päivämäärä: 17.6.2025

Verkkoon liitettyjen valvontakameroiden käyttö on kasvanut merkittävästi kodeissa, yrityksissä sekä julkisissa tiloissa. Niitä käytetään moneen tarkoitukseen, kuten perinteisesti tilojen turvallisuuden varmistamiseen, mutta myös prosessien valvontaan sekä kaupunkiliikenteen analysointiin. Laitteiden liittäminen tietoverkkoihin aiheuttaa merkittäviä kyberturvallisuusriskejä, sillä niiden suuri määrä ja heikko suojaus tekevät niistä houkuttelevan kohteen rikollisille. Järjestelmien luottamuksellisuus, eheys sekä saatavuus ovat alttiita järjestelmien haavoittuvuuksien takia.

Tämä tutkielma selvittää verkkoon liitettyjen valvontakameroiden keskeisiä teknisiä ratkaisuja, tunnistaa niihin liittyviä haavoittuvuuksia sekä esittää keinoja niistä aiheutuvien riskien minimoiseksi. Tutkielma on kirjallisuuskatsaus, johon on kerätty aineistoa akateemisista lähteistä, alan luotettavilta verkkosivustoilta sekä viranomaislähteistä.

Valvontakamerajärjestelmien arkkitehtuurit vaihtelevat hyvin paikallisista järjestelmistä hajautettuihin ja pilvipohjaisiin ratkaisuihin. Järjestelmät hyödyntävät useita eri verkkoprotokollia, kuten HTTP:tä hallintaan sekä RTSP:tä videon välittämiseen. Yleisimpiä haavoittuvuuksia ovat heikot tai muuttamattomat oletussalasanat, laitteiden puutteellinen päivittäminen sekä suojaamattomat verkkopalvelut. Hyökkääjät käyttävät näitä sekä muita haavoittuvuuksia hyökätessään verkkoon liitettyihin valvontakameroihin saaden luvattoman pääsyn videokuvaan, kaapaten laitteen osaksi bottiverkkoja tai käyttäen laitetta väliportaana seuraavaan hyökkäykseen.

Tehokas riskien minimointi edellyttää suojautumista usealla kerroksella. Ensisijaisia suojautumistoimenpiteitä ovat vahva pääsynhallinta, eli salasanojen ja tunnistautumisen varmistaminen, ohjelmistojen säännöllinen päivittäminen, tarpeettomien palveluiden käytöstä poistaminen ja verkkoyhteyksien suojaus. Tekoäly, lohkoketjuteknologia sekä kvanttiturvalliset salausmenetelmät voivat parantaa tulevaisuudessa järjestelmien turvallisuutta.

Avainsanat: valvontakamera, haavoittuvuudet, riskit, minimointi, suojautuminen

Sisällysluettelo

1 Johdanto

Verkkoon liitettyjä valvontakameroita on yhä enenevissä määrin julkisissa tiloissa, yrityksissä, kodeissa ja teollisuudessa. Ne ovat oleellinen osa nykyaikaisia älykkäitä koteja ja kaupunkeja. Maailmassa arvioidaan vuonna 2021 olleen yli miljardi valvontakameraa [1]. Valvontakameroilla suojataan omaisuutta, varmistetaan tilojen turvallisuutta, seurataan prosesseja ja liikennettä, analysoidaan jopa leikkipuistojen käyttöastetta. Näiden järjestelmien käyttöön liittyy merkittäviä kybertuvallisuusriskejä, sillä yhä useammat kamerajärjestelmät ovat yhteydessä muihin järjestelmiin sekä tietoverkkoihin ja siten potentiaalisia hyökkäyskohteita rikollisille. Kameroiden suuri määrä tekee niistä houkuttelevan kohteen. [2] Onnistunut hyökkäys vaarantaa yksityisyyden sekä turvallisuuden. Tuloksena saattaa olla tietovuoto, tietojen manipulointi, palvelunestohyökkäys tai järjestelmän kaappaus ja siten jopa fyysisen turvallisuuden vaarantuminen. Tämä työ tarkastelee verkkoon liitettyjen videovalvontajärjestelmien keskeisiä haavoittuvuuksia ja hyökkäysmenetelmiä sekä esittelee tehokkaita suojautumiskeinoja näiden riskien minimoiseksi.

Työssä käytetään yleisesti kyberturvallisuudessa ja riskienhallinnassa määriteltyjä termejä. Haavoittuvuus on jokin heikkous tai aukko järjestelmässä. Se voi olla ohjelmistossa, laitteistossa, verkossa tai toimintatavassa. Tätä haavoittuvuutta hyödyntämällä jokin taho saa pääsyn järjestelmään suojausmekanismien ohi. Haavoittuvuuden hyödyntäminen tarvitsee yleensä siihen sopivan työkalun tai tekniikan käyttämistä. Uhan pitää pystyä hyödyntämään haavoittuvuutta aiheuttaakseen haittaa. Uhka on joku tai jokin, mikä voi hyödyntää haavoittuvuutta aiheuttaakseen haittaa järjestelmälle. Se voi olla esimerkiksi henkilö, organisaatio, tilanne tai olosuhde. Riski on uhan todennäköisyyden ja onnistuneen haavoittuvuuden hyväksikäytön vaikuttavuuden tulo. Jos siis uhka on suuri tai haavoittuvuus on helposti hyödynnettävissä, on riski varteenotettava. Mikäli molemmat toteutuvat, on riski suuri. Hyökkäys tapahtuu, kun uhka todella hyväksikäyttää haavoittuvuutta aiheuttaakseen haittaa, kuten tunkeutuu luvatta järjestelmään, varastaa tietoja tai estää järjestelmän toiminnan.

1.1 Tutkimuskysymykset

TK1: Mitkä ovat keskeiset valvontakamerajärjestelmien toteutuksessa käytetyt tekniset ratkaisut?

TK2: Mitä riskejä ja haavoittuvuuksia on tunnistettu erityisesti valvontakamerajärjestelmien osalta?

TK3: Miten tunnistettujen riskien vaikutusta voidaan minimoida?

1.2 Menetelmät ja tiedonhaku

Tutkielmaa varten on kerätty aineistoa Google Scholarin ja Gemini 2.5 Pron avulla siten, että Gemini on ehdottanut sopivia lähdeartikkeleita, josta varsinainen materiaali on kerätty. Lähteinä on suosittu IEEE:n palvelussa julkaistuja artikkeleita, mutta lähteet sisältävät myös muita akateemisia julkaisuja. Hakusanoina on käytetty: CCTV, video surveillance, threats, vulnerabilities, risks, hacking, mitigation, IoT cameras, internet connected cameras, penetration. Aineistoa on etsitty myös riippumattomista alan luotettavaksi tunnetuista verkkosivustoista, sekä eri uutislähteistä, kuten Traficom, Statista, ja Yhdysvaltain puolustusministeriö.

Kerätystä aineistosta on rajattu pois julkaisuvuoden perusteella kaikki ennen vuotta 2010 julkaistut artikkelit. Tapahtuneita hyökkäyksiä kuvaavassa kappaleessa on huomioitu myös vanhemmat tapaukset.

1.3 Tutkielman rakenne

Tutkielmassa on viisi lukua. Ensimmäinen luku on johdanto, jossa kuvataan tutkielmaa yleisellä tasolla, sekä käydään läpi sen tarkoitus, tutkimuskysymykset ja menetelmät. Toisessa luvussa käydään läpi valvontakamerajärjestelmien yleisimmät arkkitehtuurit, mistä järjestelmät koostuvat ja minkälaisia toiminnallisuuksia ne sisältävät. Kolmas luku kuvaa valvontakamerajärjestelmiin liittyviä haavoittuvuuksia sekä riskejä. Luku sisältää myös kuvauksia tapahtuneista hyökkäyksistä. Neljännessä luvussa etsitään keinoja suojautua näiltä hyökkäyksiltä estämällä ne tai pienentämällä niiden vaikutusta. Viidennessä luvussa pohditaan vastauksia tutkimuskysymyksiin ja tiivistetään tutkielma yhteenvedoksi.

2 Valvontakamerajärjestelmien arkkitehtuurit

Kameravalvontajärjestelmän tarkoitus on valvoa tilaa tai prosessia kuvasensoreiden, eli kameroiden, avulla. Usein järjestelmä tallentaa tämän informaation, eli niin sanotusti nauhoittaa videokuvaa, jolloin tapahtumat voidaan todentaa myös jälkikäteen. [3] Videovalvontajärjestelmä voidaan toteuttaa monella eri tavalla. Se voi koostua täysin paikallisista osista, osin paikallisessa verkossa olevista komponenteista tai hyödyntää lähes täysin pilvipalveluita.

Yksinkertaisimmillaan kamera toimii itsenäisesti ja tallentaa videomateriaalin omalle muistikortilleen. Tällöin tallennustila on hyvin rajoittunut, eikä järjestelmä ole skaalautuva. Koska valvottavia kohteita on hyvin erilaisia, myös kameratyyppejä on useita erilaisia eri käyttötarkoituksia varten. Kamera voi olla kiinteä, käännettävä sekä muuttuvalla optiikalla oleva Pan-Tilt-Zoom, eli PTZ-kamera, henkilön varusteissa oleva haalarikamera tai jopa liikkuva lennokki. Myös kameran keräämä tieto vaihtelee. Perinteiset kamerat kuvaavat näkyvää valoa, mutta lämpökamerat kuvaavat infrapunasäteilyä. Toisaalta myös kameran liitettävyys vaihtelee langallisesta langattomaan, mikä vaikuttaa kameran haavoittuvuuksiin.

Kamerat tuottavat suuren määrän dataa lähettäessään jatkuvaa videovirtaa. Tämän datamäärän tehokkaammaksi hallitsemiseksi sitä voidaan jalostaa datafuusiolla. Videodataan voidaan liittää esimerkiksi liike- tai paikkatietoa, ääntä tai hahmontunnistuksen tuloksia.[4] Viimeaikaisia trendejä valvontakamerajärjestelmissä ovat sensorien tarkkuuden parantuminen, lisääntynyt analytiikka sekä hallintajärjestelmän tarjoaminen pilvipalveluna [4].

2.1 Järjestelmätyypit

Kamerajärjestelmiä voidaan luokitella eri perustein. Tässä tutkielmassa tyypit määritellään niiden verkottuneisuuden mukaan, eli kuinka paikallisia tai hajautettuja järjestelmät ovat. DVR-järjestelmällä (Digital video recorder) tarkoitetaan ratkaisua, jossa kamerat on kytketty suoraan tallentimeen, ilman IP-verkkoa. NVR-järjestelmä (Network video recorder) hyödyntää IP-verkkoa kameroiden liittämiseen ja mahdollistaa järjestelmän levittämisen laajemmalle alueelle. DVR- ja NVR-pohjaiset järjestelmät tallentavat videomateriaalin paikallisesti, mutta eroavat etäkäyttömahdollisuuksiltaan.

DVR-järjestelmät ovat teknisesti yksinkertaisimpia, mikä tekee niistä luotettavia ja turvallisia, mutta tarjoavat vähiten ominaisuuksia. Perinteisesti tämän tyyppisissä järjestelmissä ei ole etäkäyttömahdollisuutta.[5]

NVR-järjestelmät mahdollistavat paremman skaalautuvuuden, kuvanlaadun sekä etäkäyttömahdollisuuden, koska ne hyödyntävät IP-verkkoa toiminnassaan. Ne ovat myös kalliimpia ja monimutkaisempia ylläpitää sekä haavoittuvaisempia hyökkäyksille. Verkkoa hyödyntävät kamerajärjestelmät on usein yhdistetty sekä lähiverkkoon, että Internetiin, mikä lisää hyökkäyspinta-alaa. Etäkäyttö vaatii yleensä verkkoyhteyden sallimisen suoraan ulkoverkosta tallentimelle.[6] Ylläpito, kuten päivitykset ja laitteiston viat, ovat asiakkaan vastuulla.

Pilvipalveluita hyödyntävät järjestelmät voivat olla joko täysin tai osittain ulkoistettuja. Täysin pilvipalveluihin perustuvat järjestelmät yhdistävät kamerat IP-verkon ja reitittimen kautta Internetissä olevaan palvelimeen salattuja yhteyksiä käyttäen. Tämän tyyppinen järjestelmä ei rajoita laitteiden määrää tai tallennustilaa vaan skaalautuu tarpeen mukaan. Järjestelmä ei vaadi paikallisia tallentimia. Järjestelmän ylläpito on palveluntarjoajan vastuulla. Pilvipalveluun perustuva valvontakamerajärjestelmä sopii monta erillistä pientä valvontakohdetta sisältävään järjestelmään. Etäkäyttö on ainoa tapa käyttää järjestelmää.

Perinteiset pilvipalveluihin liittyvät kustannusedut ja -haitat koskevat myös videovalvontajärjestelmiä. Videon tallennus pilvipalveluun aiheuttaa suuren määrän verkkoliikennettä sekä vaatii erittäin paljon tallennustilaa.[5]

Pilvipalveluiden tarjoaminen videovalvontamarkkinoilla on kasvanut suuresti myös kuluttajamarkkinan ulkopuolella viimeisen kahden vuoden aikana. Suuret valmistajat ovat kehittäneet omia ratkaisuja tai ostaneet toisia yrityksiä mahdollistaakseen kilpailun SaaS-tyyppisissä pilvipalveluissa. Tämän ennustetaan parantavan järjestelmien ylläpitoa päivitysten ja laitteiden osalta, mutta kasvattaa huolia yksityisyyden vaarantumisesta lisääntyneen analytiikan takia.[7]

Osittain pilvipalveluun perustuvat järjestelmät, eli niin sanotut pilvihallitut järjestelmät yhdistävät NVR- ja pilvipalvelujärjestelmien etuja. Tällaisissa järjestelmissä videomateriaali tallennetaan NVR-tallentimille paikallisesti, mutta niiden hallinta ja etäkäyttö perustuu pilvipalveluun. Videomateriaali on silloin omassa hallinnassa, mutta järjestelmän ylläpito, kuten päivitykset, ovat palveluntarjoajan vastuulla. Järjestelmä on etäkäytettävä ja

skaalautuva, mutta tietyiltä osin rajoitetummin kuin täysin pilvipalveluun perustuvassa järjestelmässä.[5] Kameravalmistajat tarjoavat omaa pilvihallintaa suoraan kameroilla hyödyntäen kameran omaa muistikorttia tai pilvipalvelua tallennustilana. Tällöin kamera muodostaa yhteyden valmistajan pilvipalveluun eikä sille tarvitse avata suoraa yhteyttä ulkoverkosta päin.[8], [9]

2.2 Palvelut ja protokollat

Verkkoon liitetyt valvontakamerat sisältävät monia ominaisuuksia hallinnan, videon katselun ja liitettävyyden kannalta. Monet näistä ominaisuuksista käyttävät tiettyä, siihen tarkoitukseen soveltuvaa protokollaa kommunikoidessaan käyttäjän tai taustajärjestelmän kanssa. Jokainen protokolla ja palvelu lisää hyökkäyspinta-alaa, sillä niissä jokaisessa saattaa olla haavoittuvuuksia. Osa palveluista kuuntelee saapuvia yhteyksiä kameran päässä ja osa hyödyntää muualla olevia resursseja esimerkiksi yhdistämällä ja rekisteröitymällä kameravalmistajan pilvipalveluun.

2.2.1 Paikalliset palvelut

Eri valmistajien kameroissa on käytössä erilaisia omaisuuksia, riippuen esimerkiksi siitä, onko se paikallisesti hallittava vai hyödyntääkö se pilvipalvelua. Yleensä paikallisesti hallittavissa ja käytettävissä kameroissa Web-käyttöliittymä konfigurointia varten ja ONVIF- sekä RTSP-palvelut videon striimausta ja kameran ohjausta varten. [6], [8], [10] Web-käyttöliittymä sekä ONVIF-palvelu käyttävät HTTP-protokollaa ja kuuntelevat yleensä portissa 80,443 tai yleisesti käytetyissä vaihtoehtoisessa portissa 8080.

Lisäksi monet kamerat käyttävät SSH- tai Telnet-protokollaa laitteen etähallintaan. Noin 8%:ssa julkisesti verkossa näkyvissä kameroissa on SSH tai Telnet-palvelu käynnissä. Nämä toimivat porteissa 22 tai 23 sekä joskus vaihtoehtoisissa porteissa 2222 tai 2323. Joissain kameroissa palvelun saa erikseen päälle haavoittuvuutta hyödyntäen. Edellä mainitut portit ovat tyypillisiä kohteita haittaohjelmille ja verkkoa kartoittaville toimijoille. [2], [6], [11] Videon striimaus on yleensä toteutettu ensisijaisesti UDP-liikenteenä RTP-protokollaa hyödyntäen. [6] UDP ja RTP mahdollistavat viiveen pysyvän pienenä ja toisaalta toteutuksen kevyenä kameran päässä.

2.2.2 Pilvipalvelut

Monet verkkoon liitettävistä kameroista sisältävät mahdollisuuden yhdistää se pilvipalveluun, jonka avulla kameran etäkäyttö on suoraviivaista. Oikein toteutettuna se on tietoturvallinen tapa, mutta usein edullisissa kotikäyttöön tarkoitetuissa IoT-laitteissa toteutus on huono. Yhteys saattaa olla salaamaton tai se käyttää laitteen ja käyttäjän tunnistamiseen liian heikkoa salasanaa. [9]

2.2.3 Esimerkkilaite

Tarkasteltaessa yhtä yleistä valvontakameramallia, Dahua IPC-HDW2431T, havaittiin sen tukevan monia muitakin palveluita ja protokollia, kuin edellä mainitut.

Asetuksissa on valmistajakohtaisen protokollan portit, oletuksena TCP 37777 ja UDP 37778. Nämä voi muuttaa, mutta palvelua ei saa pois päältä. Shodan hakukone löytää 15.3.2025 1 342 307 julkisesti verkossa olevaa laitetta, jotka kuuntelevat portissa 37777. Samaa porttia käyttää myös usea muu kameravalmistaja. Tähän protokollaan liittyen on löydetty useita haavoittuvuuksia, kuten CVE-2013-6117, CVE-2017-6432, CVE-2020-5736 ja CVE-2020-5735). Kyseessä on ainakin tietyissä tapauksissa salaamattomasta protokollasta.[12], [13], [14]

Laitteen hallinta käyttää yleisiä HTTP- tai HTTPS- protokollia TCP-porteissa 80 ja 443, jotka mahdollistavat käytön verkkoselaimen avulla. Videokuvan välitykseen käytetään RTSP-protokollaa (Real-time streaming protocol) portissa 554. Näistä salaamattomat HTTP ja RTSP altistavat käyttäjätunnukset ja salasanat urkkimiselle. Kamerassa käytetään myös paljon muita palveluita sen käyttöönottoon ja liitettävyyteen. ONVIF-rajapinta mahdollistaa laitteen liittämisen osaksi järjestelmää. UPnP helpottaa kameran liitettävyyttä, mutta sen avulla kamera saattaa avata portteja reitittimestä lähiverkkoon automaattisesti, mikä altistaa sen suorille hyökkäyksille ulkoverkosta ja altistaa ne esimerkiksi palvelunestohyökkäykselle[15]. DynDNS helpottaa kameran etäkäyttöä, mikäli se käyttää vaihtuvaa IP-osoitetta yhteydessään ulkoverkkoon. Bonjour-protokollan avulla kamera mainostaa omia palveluitaan lähiverkossa. SMTP (Simple mail transfer protocol) mahdollistaa sähköposti-ilmoitusten lähettämisen hälytyksen sattuessa. Turvallisuutta parantavat protokollat verkkoyhteyden todennukseen liittyvä 802.1x ja liikenteen priorisointiin liittyvä QoS (Quality of service). Lisäksi kamerassa on kaksi vaihtoehtoa, ”Auto register” sekä ”P2P-pilvipalvelu”, valmistajan omiin pilvipalveluihin liittymistä varten. Vaikka nämä palvelut poistavat tarpeen avata saapuvia

yhteyksiä palomuurista, niiden tietoturva riippuu täysin palveluntarjoajan toteutuksesta. Jokainen näistä palveluista ja protokollista kasvattaa laitteen hyökkäyspinta-alaa. Näiden virheelliset konfiguraatiot tai toteutukset lisäävät haavoittuvuuksia, joita hyökkääjä voi käyttää laitteen kaappaamiseen tai häirintään.

3 Valvontakameroiden haavoittuvuudet ja riskit

Yleisesti tietoturvaan liittyvää CIA-kolmiota voidaan soveltaa myös valvontakamerajärjestelmiin hyvin havainnollisesti. Luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability) ovat kaikki oleellisia toimivan ja turvallisen järjestelmän kannalta. Luottamuksellisuus menetetään, jos laitteisiin tai videoon saadaan luvattomasti pääsy. Hyökkääjä saattaa loukata yksityisyyttä katselemalla kamerakuvaa toisen henkilön kodista. Eheys menetetään, jos hyökkääjä muokkaa kameran lähettämää videokuvaa tai tallennettua videota joko poistamalla tai korvaamalla sen peukaloidulla materiaalilla. Saatavuus menetetään, jos kameran tai järjestelmän käyttö estetään. Hyökkääjä voi esimerkiksi katkaista kameran videokuvan, poistaa tallennettuja videoita tai aiheuttaa häiriötä hallintajärjestelmälle.[6]

Aikaisemmin paikallisten videovalvontajärjestelmiin kohdistetut hyökkäykset olivat fyysisiä, kuten johtojen katkaisuja, videon syöttämistä kamerasta tulevaan kaapeliin tai tallennuslaitteen peukalointeja. Nykyaikaiset järjestelmät käyttävät monimutkaisempaa arkkitehtuuria ja teknologioita sekä ovat monesti yhteydessä Internetiin, mikä kasvattaa niiden hyökkäyspinta-alaa huomattavasti ja asettaa ne jatkuvien hyökkäysten kohteeksi.[6] Verkkoon liitettyjen valvontakameroiden määrä on lisääntynyt kotikäyttäjien ja yritysten keskuudessa. Ne mahdollistavat omaisuuden ja tilojen turvaamisen edullisesti ja etänä.[16] Arvion mukaan verkkoon liitettyjä IoT-kameroita on vuonna 2027 yli 180:ssä miljoonassa kotitaloudessa. Nousua vuodesta 2023 vuoteen 2027 arvioidaan olevan 82,79%.[17] Älykotien turvalaitteiden markkinan, josta kamerat ovat valtaosa, arvioidaan kasvavan vuodesta 2024 vuoteen 2029 lähes 100%.[18] Älykkäitä valvontakameroita arvioidaan olevan vuonna 2025 23,9%:ssa kotitalouksista. [19]

Motivaatio hyökkäyksen tekemiselle saattaa vaihdella. Se voi olla taloudellinen, jännityksen hakeminen tai osa suurempaa operaatiota, kuten ryöstöä tai vakoilua. Kameroita voidaan myös käyttää astinlautana seuraavalle hyökkäykselle, sillä kamerajärjestelmät ovat usein yhdistetty sekä paikalliseen verkkoon, että Internetiin. [6], [16]

3.1 Haavoittuvuudet

Haavoittuvuus viittaa heikkouteen tai aukkoon tietojärjestelmässä, ohjelmistossa tai laitteistossa, joka mahdollistaa hyökkääjän pääsyn järjestelmään tai sen manipulointiin tavalla, joka ei ole tarkoitus. Tämä voi johtaa tietojen vuotamiseen, järjestelmän käyttöoikeuksien laittomaan hankkimiseen tai muuhun ei-toivottuun toimintaan. Haavoittuvuudet voivat johtua monista tekijöistä, kuten ohjelmointivirheistä, suunnitteluvirheistä, virheellisestä konfiguroinnista tai puutteellisista turvatoimista.[20] Haavoittuvuuksia ovat esimerkiksi heikot salasanat tai ohjelmakoodissa olevat virheet, joiden avulla hyökkääjä saa laitteen luvattomasti haltuunsa.

Verkkoon kytkettyjä laitteita, kuten valvontakameroita skannataan jatkuvasti kartoittaen mistä osoitteista niitä löytyy ja mitä tunnettuja haavoittuvuuksia niissä mahdollisesti on. Shodan- ja Censys-hakukoneet ovat erikoistuneet tähän. Yleinen tietokanta löydetyistä haavoittuvuuksista on MITRE:n ylläpitämä CVE-tietokanta. Muita merkittäviä haavoittuvuustietokantoja ovat mm. Exploit Database, VulnDB ja Rapid7 Vulnerability and Exploit Database. Niihin kerätään tietoa haavoittuvuuksista, kuten mitä laitteita ja palveluita se koskee, kuinka suuren haitan se aiheuttaa hyväksikäytettynä ja kuinka todennäköistä sen hyväksikäyttö on. [16]

3.1.1 Yleisimmät haavoittuvuudet

Verkkoon liitetyissä valvontakameroissa on samankaltaisia tietoturvaongelmia kuin IoT-laitteissa yleensä, eli heikot palvelinohjelmiston suojaukset, heikko tai olematon kryptografia, ei ohjelmiston allekirjoitusta, huonosti toteutettu autentikointi ja auktorisointi tai huonosti toteutetut verkkopalvelut.[21]

Kyberturvallisuuskeskus on julkaissut Tietoturvamerkin vaatimustenmukaisuuslomakkeen, jonka avulla voidaan arvioida IoT-laitteen, kuten valvontakameran, tietoturvallisuutta. Se pohjautuu ETSI EN 303 645 ”Cyber; Cybersecurity for Consumer Internet of Things” standardiin [22]. Tietoturvamerkin myöntämisessä otetaan kantaa seuraaviin suojausmekanismeihin [23]:

1. Heikot, helposti arvattavat tai kovakoodatut salasanat.
2. Turvattomien tai vanhentuneiden komponenttien käyttö.
3. Riittämätön tietosuoja.

4. Turvaton tiedon siirto ja varastointi.
5. Turvattomat verkkopalvelut ja ekosysteemirajapinnat.
6. Turvattomat oletusasetukset.

Tietyt kiinalaiset kameravalmistajat ovat päätyneet Yhdysvaltain ja useiden muiden maiden kieltolistalle. Kameroista löytyneet haavoittuvuudet, takaportit ja valmistajien läheinen yhteistyö Kiinan hallinnon kanssa on arvioitu liian suureksi riskiksi, jotta kyseisten valmistajien laitteita voitaisiin käyttää julkishallinnon järjestelmissä.[24]

Vuonna 2017 Hikvision-merkkisistä kameroista löytyi kovakoodattu järjestelmänvalvoja-tasoinen salasana [25]. Tällä salasanalla hyökkääjä pystyi ottamaan haltuunsa minkä tahansa tämän valmistajan kameran. Myös saman valmistajan pilvipalvelun käyttäjän tunnistautumisessa oli vakavia puutteita. Liikennettä tarkastelemalla hyökkääjä pystyi saamaan selville käyttäjän kirjautumistiedot. Dahua, toinen suuri kiinalainen kameravalmistaja, kärsi haavoittuvuuksista kameroiden hallintaohjelmassa. Haavoittuvuutta hyväksikäyttäen hyökkääjä sai haltuunsa kaikki järjestelmän kamerat. [25] Dahuan kameroista on myös ollut mahdollista ladata käyttäjälistaus salasanatiivisteineen, joita on voinut käyttää sellaisenaan kirjautumisessa, eli käyttäen ”pass the hash” menetelmää. [26] Molemmat valmistajat ovat sittemmin julkaisseet päivityksiä, jotka korjaavat kyseiset haavoittuvuudet. Vuonna 2023 BBC:n toimittajat löysivät edelleen julkisesta verkosta yli 100 000 haavoittuvaa kameraa [25].

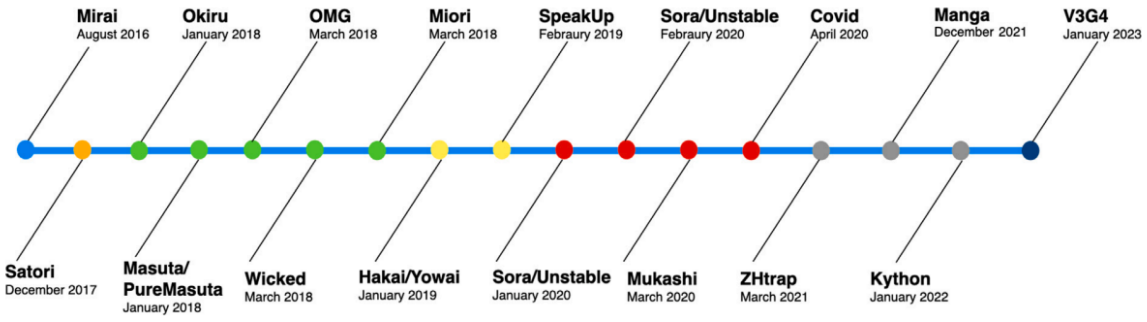
Kaikki haavoittuvuudet eivät liity laitteen etäkäyttöön. 2019 tutkijat analysoivat yrityskäyttöön suunnatun Swann NVW-470 IP-kameran laiteohjelmistoa ja löysivät siitä MD5-tiivistealgoritmilla suojatun pääkäyttäjän salasanan. [27] MD5 on vanhentunut algoritmi, eikä sitä tule käyttää, sillä sen murtaminen onnistuu sekunneissa nopeasti jopa kannettavalla tietokoneella.[28] Samasta kamerasta oli mahdollista saada videokuvaa ilman tunnistautumista, sillä vaikka kameran selainhallintanäkymä vaati tunnistautumista, RTSP-palvelu ei tarvinnut salasanaa session muodostamiseksi.[27]

Kamerajärjestelmään voidaan hyökätä myös vaikuttamalla sen käyttämään infrastruktuuriin. Valvontakameratallenteissa aikaleimat ovat tärkeitä. Niiden avulla voidaan osoittaa tapahtumien kulku jälkikäteen tiettynä hetkenä. Monesti kamerajärjestelmät luottavat aikapalvelimen NTP-protokollan lähettämään aikatietoon, jonka mukaan ne synkronoivat oman kellonsa. Lähettämällä väärennettyä aikaa, hyökkääjä voi siirtää tallenteiden aikaleimaa

mielivaltaiseen arvoon. Tämä voi aiheuttaa tallenteiden ylikirjoituksen tai hankaloittaa tapahtuman löytämistä. Vaikka tapahtuma löytyisi, rikoksen todentaminen väärän ajan tai jopa väärän päivän tallenteista heikentää sen uskottavuutta. [29]

3.2 Esimerkkejä toteutetuista hyökkäyksistä

Tunnetuimmat verkkoon kytkettyihin kameroihin kohdistuneet hyökkäykset liittyvät Mirai-haittaohjelmaperheeseen. Mirai on haittaohjelmisto alun perin vuodelta 2016, joka leviää laitteesta toiseen, kuten mato. Tämän ansiosta se tavoittaa myös laitteita, jotka eivät suoraan näy internetiin. Se etsii haavoittuvaisia, yleensä ARC-prosessoria käyttäviä, laitteita verkosta ja leviää näihin, asettaen kohdelaitteet osaksi bottiverkkoa. Tätä bottiverkkoa voidaan myöhemmin käyttää palvelunestohyökkäyksiin tai piilottamamaan muun hyökkäyksen alkuperä reitittäen liikenne bottiverkon läpi. Miraista on tehty useita eri variantteja, joista erityisesti valvontakamerajärjestelmiin kohdistuu Reaper, OMG, Hakai/Yowai, V3G4. Muita merkittäviä ovat mm. Okiru, Satori, Masuta, PureMasuta ja IoTrooper. Jatkuva muutos ja kehitys tekee siitä edelleen vaarallisen. Nykyisin Mirai-variantit kohdistavat hyökkäyksiä myös perinteisiä palvelimia ja verkon aktiivilaitteita kohtaan.[30] Kuvassa 1 esitellään Mirai-haittaohjelman kehityskulkua ja tuodaan esille sen pitkä elinkaari.



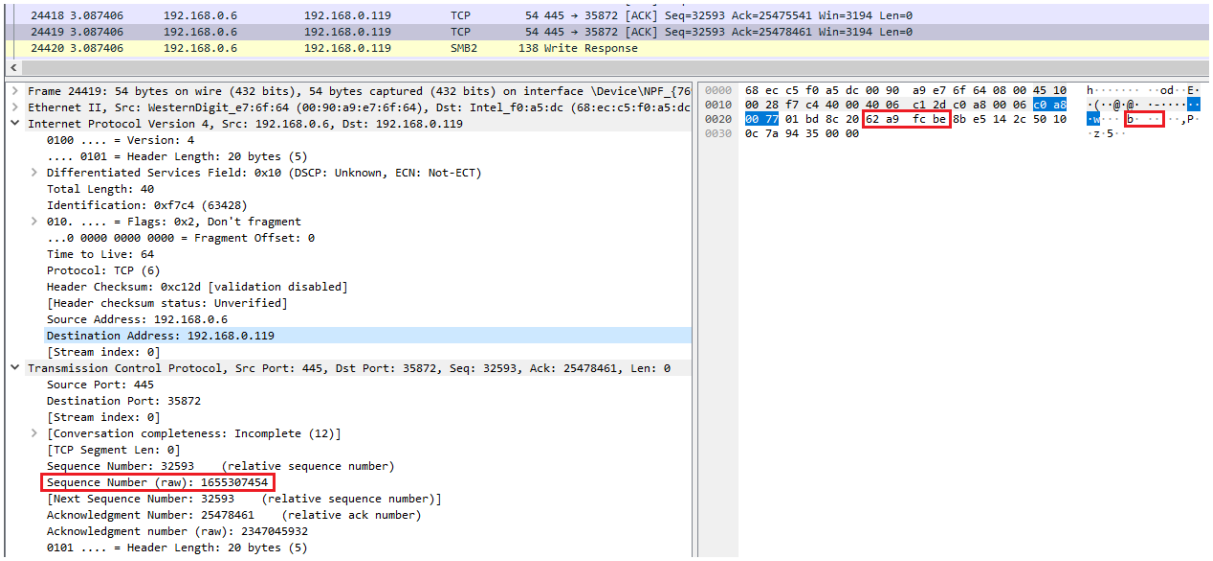
Kuva 1 - Mirai-haittaohjelman kehityksen aikajana [11]

Mirain variantit eroavat toisistaan siinä, miten ne etsivät uusia kohteita ja mitä haavoittuvuuksia ne käyttävät sekä mihin tarkoitukseen ne kohdelaitteen kaappaavat. Yksinkertaisimmillaan haittaohjelma skannaa verkon laitteita tarkistamalla tiettyjä TCP-portteja lähettämällä TCP SYN-paketteja. Useimmin tarkastetut portit ovat 23, 2323. Muita portteja on myöhemmin lisätty skannattavien listalle. Jos laite vastaa, niin haittaohjelma yrittää avata istunnon jollakin valmiiksi määritetyllä yleisellä käyttäjätunnus ja salasana

parilla. Mikäli istunto aukeaa, haittaohjelma lataa kohdelaitteelle oman kopion Miraista ja raportoi sen osaksi bottiverkkoa.

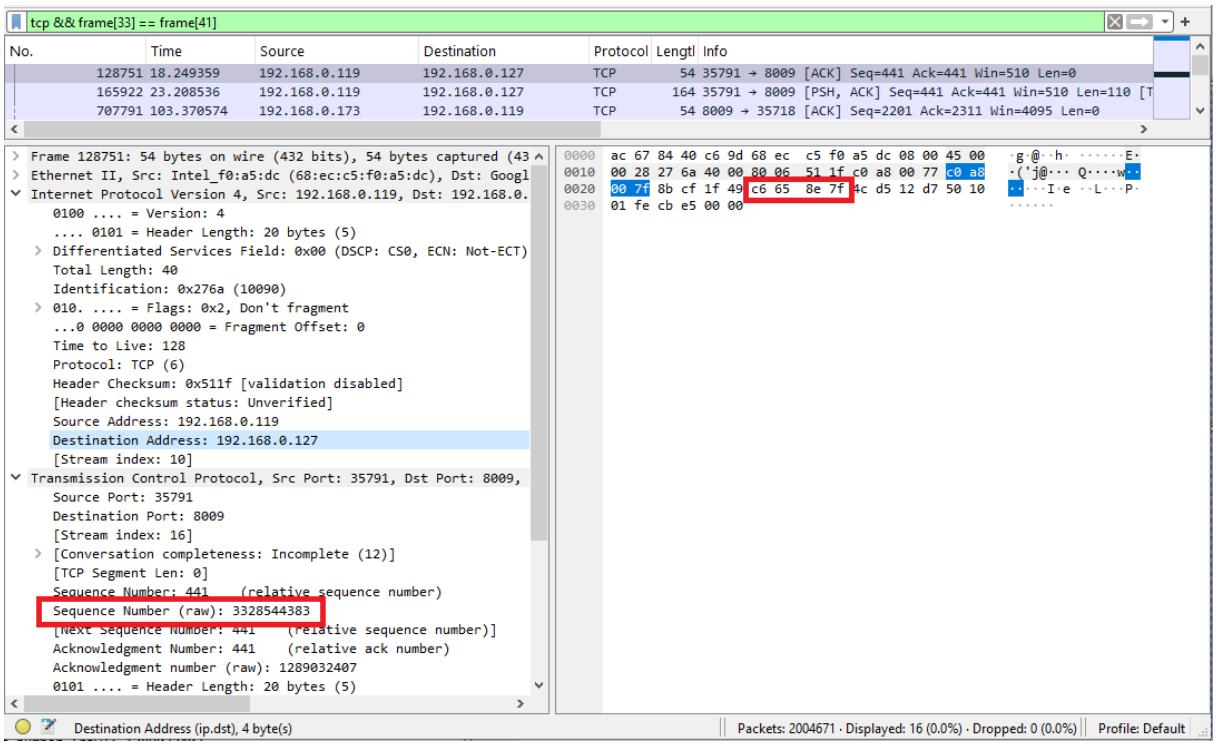
Mirai pystyy toteuttamaan useita erilaisia palvelunestohyökkäyksiä, kuten generoimalla DNS, UDP, STOMP, SYN- ja ACK-paketteja. Sen saastuttamia laitteita käytetään myös varastamaan tietoja tai kryptovaluutan louhintaan.[21]

Mielenkiintoisena yksityiskohtana, Mirain tunnistettavana piirteenä skannausvaiheessa on säilynyt tapa asettaa TCP-paketin sekvenssinumero samaksi kohde IP:n kanssa, mikä on normaalissa verkkoliikenteessä erittäin epätodennäköinen sattuma. Wireshark ohjelman tyyppinen vertaus ”TCP.seq == IP.dst” kuvaa samaa tilannetta. TCP-pakettia tarkasteltaessa kuvassa 2 havainnollistetaan, että nämä arvot voivat olla samat, sillä niille on varattu sama määrä bittejä, eli 32. IP-osoitetta 192.168.0.119 vastaava arvo sekvenssinumerona olisi desimaalilukuna 3232235639.



Kuva 2 - TCP-paketti Wireshark-ohjelmassa

Kotiverkossa suoritetussa kokeessa suodatettaessa 2 004 671 pakettia, joista TCP-paketteja oli 2 001 632, löydettiin 16 osumaa vain kohdeosoitteen ja sekvenssinumeron viimeisiä tavuja vertaamalla. Vertailemalla kaikkia tavuja yhtä aikaa ei löydetty yhtään osumaa. Wireshark ei pysty suoraan vertailemaan erityyppisiä arvoja keskenään. Vertailu onnistuu määrittämällä kehyksen vertailtavat tavut suodattimeen.



Kuva 3 - Kohdeosoitteen ja sekvenssinumeron viimeisten tavujen vertailu

Washington D.C. kärsi laajasta valvontakameroihin kohdistuvasta kiristyshaittaohjelmahyökkäyksestä vuonna 2017. [31] 70% poliisin käyttämistä yleiseen kaupunkiympäristön valvontaan tarkoitetuista valvontakameroista oli toimimattomassa tilassa 3 päivää. Tuona aikana hyökkäyksen kohteena olleet verkkotallentimet (NVR) eivät pystyneet tallentamaan videomateriaalia. Hyökkäys havaittiin, kun osa laitteista ei toiminut, jonka jälkeen verkossa olevista tallentimista löytyi kaksi erilaista kiristyshaittaohjelmaa. Haittaohjelmat levisivät automaattisesti laitteesta toiseen, mutta eivät päässeet tartuttamaan laitteita kameraverkon ulkopuolella. Kaupunki ei maksanut lunnaita, vaan asensi laitteiden ohjelmistot uudelleen.[32]

Suurin pilvipalvelupohjaisiin järjestelmiin liittyvä hyökkäys tapahtui 2021, kun hyökkääjät murtautuivat Verkadan järjestelmään, saaden haltuunsa jopa 150 000 valvontakameraa ympäri maailmaa. Joukossa oli kameroita vankiloista, sairaaloista poliisilaitoksilta ja tuotantolinjoilta. Motiivi ei vaikuttanut olevan taloudellinen, vaan ennemmin kantaaottava haktivisimi kapitalismia vastaan. Hyökkäyksessä käytettiin hyväksi Microsoft Exchange:ssa olleita nollapäivähaavoittuvuuksia sekä vuotaneita salasanoja.[33]

Valvontakameroihin kohdistuvia hyökkäyksiä on toteutettu paljon osana Ukrainan ja Venäjän sotaa. Ukrainalaiset ovat käyttäneet kameroita propagandan lähettämiseen Venäjälle [34] ja

Venäjä on käyttänyt Ukrainassa olevia kameroita tiedusteluun ja tulenjohtoon. [35] Valvontakameroiden hakkeroinnin tavoitteena on ollut seurata Ukrainan rajanylityksiä ja materiaaliliikennettä, varsinkin sotilaallista apua. [36]

Hyökkäyksiä valvontakameroihin tehdään jatkuvasti. Toukokuussa 2025 noin 20 tiedustelu- ja kyberturvallisuusviranomaista julkaisivat yhteisen varoituksen, jonka mukaan Venäjän sotilastiedustelu GRU:n kybertoimijat ovat pyrkineet saamaan pääsyn yksityisiin ja kunnallisiin IP-kameroihin, jotka sijaitsevat rajanylityspaikkojen, sotilaallisten kohteiden sekä rautatieasemien läheisyydessä. Kohteina on ollut yli 10000 valvontakameraa, joista yli 80 prosenttia sijaitsi Ukrainassa ja loput muualla itäisessä Euroopassa. [36] Verkkoon liitetyissä valvontakameroissa on hyvin usein RTSP palvelin, jota käytetään videostriimin istunnon neuvottelemiseen. Se siis kuuntelee yhteyspyyntöjä, huolehtii autentikoinnista ja kuvailee videostriimin ominaisuudet, kuten videokoodekin, resoluution ja striimausosoitteen. Hyökkääjät käyttivät brute force -menetelmää salasanojen arvaamiseen, hyödyntäen laitteiden oletustunnuksia sekä yleisimmin käytettyjä salasanoja. Lähetettäessä RTSP DESCRIBE pyyntö oikeilla tunnuksilla, kamera vastaa lähettämällä edellä mainitut tiedot kysyjälle, sekä lähettää pysäytyskuvan videosta. Tämä on huomaamaton tapa kerätä tietoa, koska se ei vaadi pääsyä kameran käyttöliittymään, eikä aiheuta merkittävää verkkoliikenteen lisääntymistä, kuten täysi videostriimi tekisi. Kameran salasanan vaihtaminen käyttöliittymässä ei aina muuta RTSP-palvelun salasanaa, vaan se pitää muuttaa erikseen, jolloin oletussalasanojen käyttöön jääminen on todennäköisempää.

3.3 Riskit

Vaikka haavoittuvuus olisi olemassa, riski realisoituu vasta, kun jokin uhka hyödyntää sitä ja aiheuttaa haittaa. Riskin suuruus riippuu siitä, kuinka todennäköinen hyökkäys on ja kuinka suuri on sen vaikutus. Hyökkääjien motivaatio vaihtelee kohteen ja tavoitteen mukaan ja sen ymmärtäminen helpottaa myös riskien tunnistamista. [6] Kameroiden haavoittuvuuksien hyväksikäyttö voi johtaa erilaisiin väärinkäyttötilanteisiin. Hyökkääjä saattaa esimerkiksi nähdä luvattomasti reaaliaikaista videokuvaa tai tallenteita. Taulukossa 1 listataan tunnistettuja riskejä ja niiden toteutuessaan aiheuttamia vaikutuksia.

Luottamuksellisuuden menettämiseen liittyvät riskit:		
Yksityisyyden loukkaaminen ja vakoilu.	Hyökkääjä pääsee käsiksi reaaliaikaiseen videokuvaan tai tallenteisiin. Tämä voi johtaa arkaluontoisten tietojen, kuten henkilötietojen tai käyttäytymismallien paljastumiseen.	[3], [6], [8], [37]
Sotilaallinen ja kaupallinen vakoilu.	Vihamielinen valtio tai kilpaileva yritys voi käyttää kameroita tiedusteluun, kuten Ukrainan sodassa on nähty Venäjän hyödyntävän siviilikameroita tulenjohtoon ja tiedusteluun.	[6], [16], [36]
Salasanojen tai muiden tietojen vuotaminen.	Kaapatun laitteen kautta hyökkääjä voi päästä käsiksi verkon muihin salasanoihin tai konfiguraatiotietoihin.	[6], [16], [38]
Eheyden menettämiseen liittyvät riskit		
Videon manipulointi ja väärentäminen.	Hyökkääjä voi muokata tallennettua videomateriaalia tai syöttää järjestelmään väärennettyä live-kuvaa. Tällä voidaan esimerkiksi peitellä murtoa toistamalla vanhaa materiaalia, jossa ei näy poikkeavaa toimintaa.	[6], [39]
Järjestelmän toimintaan vaikuttaminen.	Hyökkääjä voi muuttaa kameran asetuksia, kuten kääntää kameran pois valvottavasta kohteesta tai poistaa tallennuksen pois käytöstä.	[27], [38]
Saatavuuden menettämiseen liittyvät riskit		
Palvelunestohyökkäykset ja järjestelmän lamauttaminen.	Hyökkääjä voi estää kameran tai koko järjestelmän toiminnan. Tämä voidaan toteuttaa vaikuttamalla kameroihin, tallentimiin, hallintajärjestelmään tai sen hyödyntämään infrastruktuuriin, kuten tietoverkkoon.	[6], [8]
Kiristyshaittaohjelmat.	Kamerajärjestelmään ujutettu haittaohjelma voi lukita koko järjestelmän ja vaatia lunnaita sen avaamiseksi.	[31], [38]
Järjestelmän väärinkäyttöön liittyvät riskit		
Kameran kaappaaminen osaksi bottiverkkoa.	Laitteet voidaan kaapata osaksi laajempaa bottiverkkoa, jolla vaikutetaan muihin kohteisiin, käytetään kryptovaluutan louhintaan tai liikenteen alkuperän piilottamiseen.	[6], [8], [21], [30]
Käyttäminen väliportaana toisiin järjestelmiin tunkeutumisessa.	Kamerajärjestelmä saattaa olla heikommin suojattu, kuin jokin toinen kohteessa oleva järjestelmä, jolloin sitä kautta hyökkääjä voi päästä helpommin käsiksi toiseen kohteeseen.	[6], [10], [16]
Muut kuin tekniset riskit		
Tietosuoja-asetuksen (GDPR) rikkominen.	Tietosuoja-asetuksen (GDPR) rikkominen. Valvontavideon henkilötietojen oikea käsittely on tarkasti määritetty ja siitä poikkeaminen voi johtaa merkittäviin sakkoihin.	[37]
Salakatselu.	Teknisten välineiden käyttäminen ihmisten valvontaan on kielletty kotirauhan suojaamilla alueilla. Väärin asennettu tai suunnattu kamera saattaa täyttää rikoslaissa mainitun salakatselun tunnusmerkit.	[50]
Fyysiset riskit.	Erityisesti suojaamattomassa tilassa olevat laitteet ovat alttiita fyysiselle peukaloinnille ja sabotaasille.	[3], [6], [37]
Sosiaalinen manipulointi.	Hyökkääjä voi huijata käyttäjää asentamaan haittaohjelman tai luovuttamaan tunnuksensa esiintymällä esimerkiksi teknisenä tukena.	[6], [10], [38]

Taulukko 1 – Tunnistetut riskit tyypeittäin

4 Suojautuminen ja vaikutusten minimointi

Aiemmissa kappaleissa käytiin läpi verkkoon liitettyjen valvontakameroiden haavoittuvuuksia ja niihin liittyviä riskejä, kuten laitteiden kaappaaminen osaksi bottiverkkoa, arkaluontoisten tietojen vuotaminen tai käyttäminen väliportaana seuraavalle hyökkäykselle. Näitä haavoittuvuuksia vastaan on mahdollista suojautua sekä pienentää onnistuneiden hyökkäysten vaikutusta. Haavoittuvuuksien ja riskien lieventäminen, eli suojautuminen ja vaikutusten pienentäminen, ei ole yksittäinen toimenpide, vaan jatkuva prosessi, joka vaatii monipuolista lähestymistapaa. Nämä eivät ole toisiaan poissulkevia vaan täydentäviä keinoja. Tehokkaaseen vaikutusten minimointiin, vaaditaan teknisiä ratkaisuja, toimintatapoja sekä käyttäjien koulutusta. Tässä kappaleessa käydään läpi suojautumisen mekanismeja, joilla pyritään estämään haavoittuvuuksien hyväksikäyttö. Se sisältää laitteiden ja järjestelmän turvallisen konfiguroinnin ja tiedonsiirtoon sekä ylläpitoon liittyviä seikkoja, kuten laitteiden ja ohjelmiston päivitykset. Kappaleen toinen osuus käy läpi vaikutusten minimointia, eli miten voidaan rajata mahdollisen onnistuneen hyökkäyksen aiheuttama haitta. Suojautumisesta huolimatta osa hyökkäyksistä onnistuu, jolloin pääsyn rajoittaminen mahdollisimman pieneen osaan järjestelmää suojaa kokonaisuutta ja varmistaa muun toiminnan jatkumisen mahdollisimman normaalisti.

4.1 Suojautuminen

Järjestelmän suojaaminen usealla kerroksella parantaa mahdollisuuksia estää hyökkäysten eteneminen ja rajoittaa niiden vaikutusta. Verkkoon liitetyissä valvontakamerajärjestelmissä tunnistettuja kerroksia on ainakin käyttö- ja laitekerros, tiedonsiirtokerros ja järjestelmän hallintakerros. Näiden sisälläkin voidaan järjestelmä jakaa useampaan osa-alueeseen, jotka voidaan suojata omilla mekanismeillaan. [38] Käyttäjiä ja laitteita voidaan suojata fyysisesti sekä riittävän vahvalla todennuksella. Tiedonsiirtokerroksella oleellista on käyttää vahvaa salausta tiedonsiirrossa sekä rajata pääsyä vain tarvittaviin resursseihin. Hallintakerroksella sovellusten ja pilvipalveluiden tietoturvallisuus varmistavat osaltaan järjestelmän kokonaisturvallisuutta.

Haavoittuvuuksilta ja hyökkäyksiltä suojautumisessa on tärkeää ymmärtää hyökkääjän motivaatio. Arvioimalla mahdollisen hyökkäyksen syytä ja tavoitetta, voidaan paremmin kohdistaa suojaustoimenpiteet oikealla tavalla. Esimerkiksi pankkia suojaava järjestelmä

halutaan todennäköisesti saada epäkuntoon, kun taas valtion virastossa olevaa järjestelmää voidaan haluta käyttää vakoiluun.[6]

4.1.1 Vahvat salasanat ja pääsynhallinta

Mahdollisimman vahva tunnistautuminen ja huolellinen pääsynhallinta suojaavat laitetta luvattomalta käytöltä. Valmistajan asettaman oletussalasanan vaihtaminen on kriittisin yksittäinen toimenpide laitteen suojaamiseksi. Hyökkääjät käyttävät usein automatisoituja työkaluja heikkojen ja oletusarvoisten tunnusten kokeilemiseen. Käyttäjän pääsy tulisi rajoittaa vain tarvittaviin osuuksiin. Vähimpien oikeuksien periaatteen mukaisesti tulisi käyttää eri käyttäjätilejä normaaliin laitteen tai järjestelmän käyttämiseen ja sen ylläpitoon. Tämä rajoittaa vahinkoa, mikäli tavallisen käyttäjän tunnus murrettaisiin hyökkääjän toimesta. Monivaiheinen tunnistautuminen lisää tunnistautumisen vahvuutta eikä pelkkä salasanan vuotaminen aiheuta yhtä suurta uhkaa. Erityisesti järjestelmään kirjauduttaessa olisi hyvä vaatia salasanan lisäksi toinen varmennustapa. [6], [40], [41]

4.1.2 Säännöllinen ohjelmiston päivittäminen

Sovellusten sekä laiteohjelmistojen ajan tasalla pitäminen on erittäin tärkeää laitteiden suojaamiseksi. Laitteiden ohjelmistot eivät ole koskaan täysin virheettömiä ja uusia haavoittuvuuksia löydetään jatkuvasti. Automaattinen päivitysten asennus takaa niiden nopean ja systemaattisen käyttöönoton. Kriittisessä järjestelmässä päivityksiä tulisi testata ensin rajatussa määrässä laitteita, jotta varmistutaan niiden toimivuudesta. Uusien haavoittuvuustietojen (CVE) seuraaminen on oleellista suojauksen varmistamiseksi. Pilvipohjaisissa järjestelmissä päivitykset ovat usein palveluntarjoajan vastuulla, mutta paikallisesti hallituissa järjestelmissä vastuu asentamisesta on laitteiston omistajalla. [6], [40], [42], [43]

4.1.3 Tiedon salaus

Salaus varmistaa, että vaikka hyökkääjä onnistuisi pääsemään käsiksi dataan, se ei voi hyödyntää sitä ilman salausavainta. Selkokielisten protokollien estäminen ja vain suojattujen protokollien, kuten HTTPS, käyttäminen suojaa sekä käyttäjätunnuksia, että järjestelmän hallintaa. Tiedonsiirron lisäksi on tärkeää salata myös tallennettu data. Tämä tarkoittaa videomateriaalia, joka on varastoitu NVR-tallentimen kiintolevylle tai kameran muistikortille.

Järjestelmän etäkäyttö voidaan suojata käyttämällä VPN-yhteyttä, eli tunneloimalla verkkoliikenne salattuna julkisen verkon yli sen sijaan, että yksittäisiä portteja avattaisiin laitetta tai järjestelmää varten julkiseen internetiin. Päästä päähän -salaus suojaa tietoja siirto- ja tallennusvaiheessa. Tämä tarkoittaa, ettei edes pilvipalvelun tarjoaja pääse käsiksi videomateriaaliin, koska se on salattu jo lähettävän laitteen päässä ja puretaan vasta päätelaitteessa. [6], [40], [42], [44]

4.1.4 Laitteen konfigurointi

Laitteen huolellinen konfigurointi on yksi tehokas tapa minimoida laitteen hyökkäyspinta-ala. Kaikki toiminnallisuuksien kannalta tarpeettomat verkon- ja loogiset rajapinnat tulee poistaa käytöstä. Jokainen aktiivinen palvelu tai avoin portti on potentiaalinen reitti hyökkääjälle ja jokainen niistä saattaa sisältää haavoittuvuuksia. Erityisesti laitteen etähallintaominaisuudet, kuten Telnet- ja SSH-palvelut tulisi kytkeä pois päältä, mikäli niitä ei tarvita. Ohjelmiston tulisi toimia mahdollisimman vähillä käyttöoikeuksilla huomioiden sekä tietoturvan että toiminnallisuudet. Järjestelmään tulee siis luoda eri käyttäjätasoja eri tarkoituksiin. Järjestelmänvalvojan tiliä, jolla on täydet oikeudet muuttaa asetuksia ja hallinnoida laitetta, tulisi käyttää vain, kun se on välttämätöntä. On myös oleellista tarkistaa mitä tietoja ja kenelle laite niitä jakaa. Jos pilvipalvelua ei ole tarkoitus käyttää, nämä ominaisuudet tulee asettaa pois päältä, jotta laite ei lähetä tietoja ulkopuolisille tahoille eikä ole riippuvainen valmistajan palvelun tietoturvasta. Lisäksi laitteen verkkoliikennettä tulisi rajoittaa siten, että se kommunikoi vain tarpeellisten laitteiden, kuten paikallisen NVR-tallentimen kanssa. [22], [30], [45]

4.1.5 Käyttäjien koulutus

Järjestelmää käyttävien henkilöiden koulutus kyberturvalliseen toimintaan on tärkeää myös videovalvontajärjestelmissä. Vaikka järjestelmä olisi teknisesti hyvin suojattu, inhimillinen virhe voi avata reitin hyökkääjälle. Jos järjestelmän käyttöön on määritelty ohjesääntöjä, on ne oltava kaikkien käyttäjien tiedossa. Sosiaalinen manipulointi saattaa olla yksi hyökkäystapa irti verkosta olevaan järjestelmään. Hyökkääjä voi yrittää esiintyä teknisenä tukena tai muuna luotettavana tahona ja huijata käyttäjää luovuttamaan salasanansa tai muuttamaan järjestelmän asetuksia. [10]

4.1.6 Luotettavien valmistajien suosiminen

Erityisesti pilvipohjaista järjestelmää käytettäessä on hyödyllistä valita luotettavien valmistajien tuotteita, joihin on saatavissa päivityksiä. Edullisissa IoT-laitteissa pilvipalveluiden toteutus ei välttämättä ole laadukas ja tietoturvallinen. EU:n kyberturvallisuusasetus ohjaa valmistajien toimintaa, jotta kuluttajille tarjottaisiin tietoturvallisia laitteita. [38], [46]

4.1.7 Fyysinen suojautuminen

Fyysinen turvallisuus on erityisesti valvontakamerajärjestelmissä olennaista, sillä osa laitteista on sijoitettu suojattavan kohteen reunalle, missä ne ovat alttiita niin ihmisen aiheuttamille vahingoille kuin luonnonilmiöillekin. Fyysinen suojaus on usein ensimmäinen puolustuslinja puhuttaessa kerroksellisesta suojautumisesta. Fyysinen suojaus kattaa sekä itse kamerat, että järjestelmän ja siihen liittyvän infrastruktuurin, kuten tallentimet ja verkkolaitteet. Laitteet tulisi sijoittaa mahdollisuuksien mukaan lukittuun, pääsyvalvottuun tilaan. Myös suojautuminen sähkökatkoilta ja virtapiikeiltä UPS-laitteella kuuluu fyysiseen suojautumiseen. [6], [37]

4.1.8 Tietoturvatestaus

Itse tehtävä palveluiden ja sovellusten listaus sekä penetraatiotestaus auttaa suojautumaan hyökkäyksiltä. Tämä on teknisesti haastavaa ja vaatii tietoturva-ammattilaisen osallistumista. EU:n kyberturvallisuusasetus (EU) 2019/881 (The EU Cybersecurity Act, CSA) vaatii korkean kyberturvallisuussertifikaatin saamiselle tuotteen tai palvelun penetraatiotestausta.[47] Tekemällä penetraatiotestausta omalle järjestelmälle, voi löytää haavoittuvuudet ennen pahantahtoista toimijaa. Penetraatiotestauksessa käytetään usein samoja työkaluja, mitä varsinaiset hyökkääjätkin käyttävät, jolloin saadaan mahdollisimman todenmukainen kuva järjestelmän suojauksen tasosta. Yleisiä penetraatiotestauksessa käytettyjä työkaluja, jotka tulevat myös Kali-linuxin mukana, ovat esimerkiksi Nmap, Wireshark, Metasploit ja John the Ripper. Tietoturvatestausta tehdessä MITRE ATT&CK tietämyskanta on hyvä resurssi [43]. Se auttaa löytämään järjestelmien heikot kohdat listaamalla mahdollisia hyökkäysvektoreita, eli tapoja hyödyntää järjestelmän haavoittuvuuksia [36].

4.1.9 Muut toimenpiteet

Käyttäjät voivat parantaa älykkäiden valvontakameroiden sekä muiden IoT-laitteiden tietoturvaa myös vaatimalla myyjältä tietoa siitä, miten pitkään laitteen ohjelmistoa tuetaan ja miten se päivitetään. Laitteen käyttö pitäisi lopettaa, kun sen ohjelmiston tuki lakkaa.[30]

Suojautumista pyritään parantamaan myös sääntelyllä. EU:n komission asetuksessa 2022/30 ja myöhemmin 2023/2444 sekä näihin liittyvissä dokumenteissa asetetaan tietoturvavaatimukset Internetiin liitettäville laitteille, leluille, lastenhoitolaitteille sekä päälle puettaville laitteille. Varsinaiset EU:n radiolaitedirektiivin tietoturvavaatimukset on määritelty EN 18031:2024 -standardisarjassa.[46]

Tulevaisuudessa tekoälyn hyödyntäminen valvontakamerajärjestelmissä mahdollistaa suurten tietomassojen läpikäynnin poikkeavuuksien tunnistamiseksi. Tämä auttaa tunnistamaan mahdollisia hyökkäyksiä. Lohkoketjujen hyödyntäminen varmistaa tallennetun materiaalin eheyden. Se varmistaa, ettei videotallenteita voi muokata tai peukaloida ilman valtuutusta. Kvanttiturvallisen kryptografian käyttö on tulevaisuudessa oleellista, jotta voidaan varmistaa toimiva päästä päähän -salaus myös valvontakamerajärjestelmissä.[41], [42]

4.2 Vaikutusten minimointi

Vaikka suojaustoimenpiteet olisivat kattavia, täydellistä turvaa on vaikea saavuttaa. Siksi on tärkeää käsitellä miten mahdollisten tietoturvaloukkausten tai haavoittuvuuksien hyödyntämisen seurauksia voidaan rajata ja minimoida.

Palomuurit ja virtuaaliset lähiverkot muodostavat loogisia kokonaisuuksia samassa fyysisessä verkossa. Järjestelmän eristämisellä omaan fyysiseen tai loogiseen verkkoonsa muusta koti- tai yrityksen verkosta, eli segmentoimalla, voidaan rajoittaa sivuttaisliikkumista (lateral movement), eli kamerajärjestelmän käyttämistä väliportaana ja hyökkäyksen etenemistä toisiin järjestelmiin. Käyttämällä nollaluottamusperiaatetta (Zero Trust) sallitaan ainoastaan tarpeellinen pääsy verkosta ja järjestelmästä toiseen. Kriittisimmät järjestelmät voidaan pitää täysin irrallaan (air-gapped) muista järjestelmistä, jolloin niihin tunkeutuminen vaikeutuu huomattavasti. [6], [36]

Hyökkäyksen mahdollisimman aikainen havaitseminen auttaa estämään hyökkäyksen etenemisen pidemmälle. Lokien ja verkkoliikenteen valvonta tunkeutumisen havaitsemis- tai

estojärjestelmällä (IDS/IPS) voi paljastaa hyökkäyksen jo aikaisessa vaiheessa. Tunnetut hyökkäykset voidaan tunnistaa ennalta määritettyjen toimintatapojen, kuten Mirai-haittaohjelman tapauksessa tyypillisten skannausten, perusteella. Entuudestaan tuntemattomatkin hyökkäykset saatetaan havaita, esimerkiksi epätavallisen monen epäonnistuneen kirjautumisyrityksen, laitteiden kuormittumisen tai huomattavasti kasvaneen verkkoliikenteen takia.[6], [11], [42], [48]

Järjestelmän kannalta oleellisten komponenttien kahdentaminen ja varmuuskopiointi nopeuttavat ongelmatilanteesta palaustumista, mikäli järjestelmä joutuu hyökkäyksen kohteeksi ja sen toiminta estyy. Tarvittaessa voidaan ottaa käyttöön varapalvelin, tai palauttaa järjestelmä varmuuskopiosta aiempaan toimivaan tilaan. [10] Pilvipohjaisten VSaaS-järjestelmien tapauksessa palveluntarjoaja yleensä vastaa näistä toimenpiteistä.[49]

5 Yhteenveto

Tutkielmassa selvitettiin verkkoon liitettyjen valvontakameroiden haavoittuvuuksia ja niiden aiheuttamia riskejä. Perinteiset valvontakamerajärjestelmät olivat analogisia, nimensä mukaisesti eristettyjä järjestelmiä (CCTV, closed-circuit television). Digitalisaation myötä valvontakamerajärjestelmiin tuli etäkäyttömahdollisuus ja myöhemmin järjestelmien koon kasvaessa ja teknologian mahdollistaessa ne ovat siirtyneet toimimaan kokonaan tietoverkoissa tai jopa pilvipalveluna. Valvontakamerat ovat luonteeltaan sellaisia, että ne sijoitetaan usein kriittisiin sijainteihin yksityisyyden tai omaisuuden kannalta, mutta niitä halutaan käyttää etänä mahdollisimman helposti. Siten ne voivat mahdollistaa pääsyn syvemmälle suojattuihin verkkoihin. Ne myös usein kuvaavat koteja ja työpaikkoja eli voivat paljastaa arkaluontoista tietoa, eikä niitä välttämättä mielletä IT-laitteiksi, joiden säännöllinen päivittäminen olisi välttämätöntä.

Tämä tutkielma löysi vastauksen ensimmäiseen tutkimuskysymykseen (TK1), joka käsitteli valvontakamerajärjestelmien keskeisiä teknisiä ratkaisuja. Valvontakamerajärjestelmät voidaan toteuttaa usealla eri arkkitehtuurilla. Perinteisemmät DVR- ja NVR- pohjaiset järjestelmät ovat paikallisia tallennusjärjestelmiä. NVR-tyyppiset järjestelmät kuitenkin mahdollistavat verkotetun järjestelmän ja etäkäyttömahdollisuuden. Nykyaikaisemmat ratkaisut hyödyntävät yhä useammin joko osittain tai kokonaan pilvipalveluita, joissa videotallenteet ja järjestelmän hallinta on ulkoistettu palveluntarjoajalle. Järjestelmien toiminta perustuu laajaan joukkoon verkkoprotokollia, joita esiteltiin luvussa 2. Hallinta tapahtuu tyypillisesti HTTP- ja HTTPS-protokollien avulla, kun taas videokuvan suoratoistoon käytetään yleisesti RTSP-protokollaa. Joukko muita, kuten ONVIF, UPnP ja valmistajien omat pilviratkaisut, mahdollistavat kameroiden etäkäytön ja liittämisen osaksi järjestelmää.

Toiseen tutkimuskysymykseen (TK2), joka koski riskejä ja haavoittuvuuksia, tunnistettiin useita merkittäviä tekijöitä, jotka vaikuttavat järjestelmien luottamuksellisuuteen, eheyteen ja saatavuuteen. Keskeisimmät haavoittuvuudet liittyvät heikkoon todennukseen, kuten helposti arvattaviin tai muuttamattomiin oletussalasanoihin, sekä laiteohjelmistossa oleviin virheisiin. Suojaamattomien protokollien käyttäminen ja turvattomat laitteiden oletusasetukset ovat yleisiä haavoittuvuuksia. Myös fyysiset hyökkäykset ovat mahdollisia, sillä valvontakameroita luonnollisesti sijoitetaan alueiden reunoille, osana fyysistä turvajärjestelmää. Nämä heikkoudet aiheuttavat vakavia riskejä. Hyökkääjä voi saada

haltuunsa arkaluontoista videokuvaa, mikä voi johtaa yksityisyyden menettämiseen tai jopa sotilaalliseen vakoiluun. Kaapattuja kameroita käytetään laajasti osana bottiverkkoja, kuten Mirai-haittaohjelman tapauksessa, palvelunestohyökkäyksen toteuttamiseen. Järjestelmiin voidaan vaikuttaa syöttämällä niihin peukaloitua videota tai estämällä niiden toiminta, esimerkiksi kiristyshaittaohjelmalla.

Kolmanteen tutkimuskysymykseen (TK3), eli tunnistettujen riskien minimointiin, löydettiin selkeitä ja tehokkaita keinoja. Paras tapa suojautua on yhdistää useita menetelmiä kerroksellisen suojan saamiseksi. Perustason toimenpiteitä ovat laitteiden oletussalasanojen vaihtaminen, säännöllinen laiteohjelmistojen päivittäminen sekä tarpeettomien verkkopalveluiden ja ominaisuuksien kytkeminen pois päältä. Etäkäyttö tulisi aina toteuttaa suojattuja ja salattuja protokollia, kuten HTTPS:ää tai VPN-yhteyttä käyttäen, jotta verkkoliikenteen sieppaaminen ei paljastaisi arkaluontoisia tietoja. Tehokas keino rajoittaa hyökkäyksen leviämistä on eristää kamerat omaan verkkosegmenttiinsä palomuurien ja virtuaalisten lähiverkkojen (VLAN) avulla. Lisäksi verkkoliikennettä ja lokitietoja aktiivisesti valvomalla voidaan havaita poikkeuksia ja tunnistaa käynnissä olevia hyökkäyksiä. Järjestelmän palautumisen kannalta varmuuskopiot ja kahdennetut palvelut ovat oleellisia.

Tulevaisuudessa tekoälyn ja hyödyntäminen poikkeavuuksien tunnistamisessa voi nopeuttaa hyökkäysten havaitsemista. Myös lohkoketjuteknologia käyttö tallenteiden eheyden varmistamisessa sekä siirtyminen kvanttiturvalliseen kryptografiaan parantavat järjestelmien tietoturvaa huomattavasti.

Lähteet

[1] E. Cosgrove, CNBC, ”One billion surveillance cameras will be watching around the world in 2021, a new study says”, url: https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html (viitattu 11.6.2025)

[2] Z. Zhao, S. Srinivasa, ja E. Vasilomanolakis, ”SweetCam: an IP Camera Honeypot”, Proceedings of the 5th Workshop on CPS&IoT Security and Privacy, Kööpenhamina Tanska: ACM, marraskuu 2023, ss. 75–81. doi: 10.1145/3605758.3623495.

[3] O. Elharrouss, N. Almaadeed, ja S. Al-Maadeed, ”A review of video surveillance systems”, Journal of Visual Communication and Image Representation, vsk. 77, s. 103116, toukokuu 2021, doi: 10.1016/j.jvcir.2021.103116.

[4] V. Tsakanikas ja T. Dagiuklas, ”Video surveillance systems-current status and future trends”, Computers & Electrical Engineering, vsk. 70, ss. 736–753, elokuu 2018, doi: 10.1016/j.compeleceng.2017.11.011.

[5] Eagle Eye Networks, ”DVR Vs NVR – Where Is My Surveillance Video Stored?”, url: https://www.een.com/blog/dvr-vs-nvr/ (viitattu 10.4.2025)

[6] N. Kalbo, Y. Mirsky, A. Shabtai, ja Y. Elovici, ”The Security of IP-Based Video Surveillance Systems”, Sensors, vsk. 20, nro 17, s. 4806, elokuu 2020, doi: 10.3390/s20174806.

[7] IPVM, ”Cloud Going Mainstream In Video Surveillance”, url: https://ipvm.com/reports/cloud-main (viitattu 15.3.2025)

[8] P. Biondi, S. Bognanni, ja G. Bella, ”Vulnerability Assessment and Penetration Testing on IP camera”, 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Gandia, Espanja: IEEE, joulukuu 2021, ss. 1–8. doi: 10.1109/IOTSMS53705.2021.9704890.

[9] P. A. Abdalla ja C. Varol, ”Testing IoT Security: The Case Study of an IP Camera”, 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Libanon: IEEE, kesäkuu 2020, ss. 1–5. doi: 10.1109/ISDFS49300.2020.9116392.

[10] A. Gomez, H. Shahriar, V. Clincy, ja A. Shalan, ”Hands-on Lab on Smart City Vulnerability Exploitation”, 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Espanja: IEEE, heinäkuu 2020, ss. 1777–1782. doi: 10.1109/COMPSAC48688.2020.00046.

[11] A. Affinito, S. Zinno, G. Stanco, A. Botta, ja G. Ventre, ”The evolution of Mirai botnet scans over a six-year period”, Journal of Information Security and Applications, vsk. 79, s. 103629, joulukuu 2023, doi: 10.1016/j.jisa.2023.103629.

[12] SpeedGuide, ”Port 37777 (tcp/udp)”, url: https://www.speedguide.net/port.php?port=37777 (viitattu 15.3.2025)

[13] Shodan Search Engine, ”Shodan Search”, url: https://www.shodan.io/search?query=port%3A%2237777%22 (viitattu: 15.3.2025)

[14] CVE Program, ”CVE - CVE-2017-6432”, url: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6432 (viitattu: 15.3.2025)

[15] Kyberturvallisuuskeskus, ”Haavoittuvuus UPnP-teknologiassa”, url: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus-upnp-teknologiassa (viitattu: 16.4.2025)

[16] J. Bugeja, D. Jonsson, ja A. Jacobsson, ”An Investigation of Vulnerabilities in Smart Connected Cameras”, 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Ateena, Kreikka: IEEE, maaliskuu 2018, ss. 537–542. doi: 10.1109/PERCOMW.2018.8480184.

[17] Statista, ”Global: smart security cameras number of households 2016-2027”, url: https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes (viitattu: 20.3.2025)

[18] Statista, ”Security & surveillance technology - statistics & facts | Statista”. url: https://www.statista.com/topics/2646/security-and-surveillance-technology/ (viitattu: 18.5.2025)

[19] Statista, ”Smart Security Cameras - Worldwide | Market Forecast”, url: http://frontend.xmo.prod.aws.statista.com/outlook/cmo/smart-home/security/smart-security-cameras/worldwide (viitattu: 18.5.2025)

[20] Hakatemia, ”Haavoittuvuudet | Perusteet haltuun”, url: https://www.hakatemia.fi/courses/perusteet/haavoittuvuudet (viitattu: 20.5.2025)

[21] Y. Seralathan ym., ”IoT security vulnerability: A case study of a Web camera”, 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Etelä-Korea: IEEE, helmikuu 2018, ss. 172–177. doi: 10.23919/ICACT.2018.8323686.

[22] ETSI, ”EN 303 645 - V3.1.3 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”, url: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf (viitattu: 2.6.2025)

[23] Traficom, ”Tietoturvamerkin_vaatimustenmukaisuuslomake”, url: https://tietoturvamerkki.fi/sites/default/files/media/file/tietoturvamerkin_vaatimustenmukaisuuslomake.pdf (viitattu: 2.6.2025)

[24] Yhdysvaltain puolustusministeriö, ”PUBLIC LAW 115–232—AUG. 13, 2018”, url: https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf (viitattu: 10.6.2025)

[25] BBC Panorama reporting team, ”The tech flaw that lets hackers control surveillance cameras”, 26.6.2023, url: https://www.bbc.com/news/technology-65975446 (viitattu: 10.6.2025)

[26] E. Kovacs, SecurityWeek, ”Backdoor Found in Dahua Video Recorders, Cameras”, url: https://www.securityweek.com/backdoor-found-dahua-video-recorders-cameras/ (viitattu: 11.6.2025)

[27] J. Valente, K. Koneru, ja A. Cardenas, ”Privacy and Security in Internet-Connected Cameras”, 2019 IEEE International Congress on Internet of Things (ICIOT), Milano, Italia: IEEE, heinäkuu 2019, ss. 173–180. doi: 10.1109/ICIOT.2019.00037.

[28] V. Klima, ”Tunnels in Hash Functions: MD5 Collisions Within a Minute”, 2006, 2006/105, url: https://eprint.iacr.org/2006/105 (viitattu: 10.3.2025)

[29] C. T. Kong ja S. M. Yiu, ”Hacking CCTV by changing time”, 2021 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), kesäkuu 2021, ss. 1–8. doi: 10.1109/ICECCE52056.2021.9514241.

[30] Traficom, ”Miraissa on tulevaisuus”, url: https://traficom.fi/fi/ajankohtaista/blogit/miraissa-tulevaisuus (viitattu: 19.4.2025)

[31] L. PASCU, Hot for Security, ”70% of Washington DC’s CCTV cameras infected with ransomware”, url: https://www.bitdefender.com/en-us/blog/hotforsecurity/70-washington-dcs-cctv-cameras-infected-ransomware (viitattu: 20.5.2025)

[32] C. Williams, The Washington Post, ”Hackers hit D.C. police closed-circuit camera network, city officials disclose”, 28. tammikuuta 2017. url: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html (viitattu: 24.5.2025)

[33] BBC, ”Hack of ’150,000 cameras’ investigated by camera firm”, 10. maaliskuuta 2021, url: https://www.bbc.com/news/technology-56342525 (viitattu: 11.6.2025)

[34] С. Надтока, Korrespondent, ”Хакеры запустили в РФ обращение Зеленского”, url: https://korrespondent.net/world/russia/4588653-khakery-zapustyly-v-rf-obraschenye-zelenskoho (viitattu: 20.5.2025)

[35] E. Kovacs, SecurityWeek, ”Russia Hacked Residential Cameras in Ukraine to Spy on Air Defense, Critical Infrastructure”, url: https://www.securityweek.com/russia-hacked-residential-cameras-in-ukraine-to-spy-on-air-defense-critical-infrastructure/ (viitattu: 20.5.2025)

[36] Yhdysvaltain puolustusministeriö, ”Russian GRU Targeting Western Logistics Entities and Technology Companies”, url: https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF (viitattu: 24.5.2025)

[37] Euroopan tietosuojaneuvosto, ”Ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla Versio 2.0”. url: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_fi_0.pdf (viitattu: 15.5.2025)

[38] P. Vennam, P. T. C., T. B. M., Y.-G. Kim, ja P. K. B. N., ”Attacks and Preventive Measures on Video Surveillance Systems: A Review”, Applied Sciences, vsk. 11, nro 12, s. 5571, kesäkuu 2021, doi: 10.3390/app11125571.

[39] T. Vakaliuk, D. Talchenko, V. Osadchyi, Y. Bailiuk, ja O. Pokotylo, ”Vulnerabilities and Methods of Unauthorized Gaining Access to Video Surveillance Systems”. CPITS 2023:

Workshop on Cybersecurity Providing in Information and Telecommunication Systems, 28.2.2023, Kiova, Ukraina

[40] A. Costin, ”Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations”, Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, Wien, Itävalta: ACM, lokakuu 2016, ss. 45–54. doi: 10.1145/2995289.2995290.

[41] P. Khan, Y.-C. Byun, ja N. Park, ”A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities”, Electronics, vsk. 9, nro 3, s. 484, maaliskuu 2020, doi: 10.3390/electronics9030484.

[42] R. U. Cybersecurity, Medium, ”Cybersecurity for Video Surveillance Networks — Mitigating Vulnerabilities in IoT Camera Systems”, url: https://medium.com/@RocketMeUpCybersecurity/cybersecurity-for-video-surveillance-networks-mitigating-vulnerabilities-in-iot-camera-systems-81bb262bf451 (viitattu: 22.5.2025)

[43] B.-J. Han, H. Jeong, ja Y.-J. Won, ”The privacy protection framework for biometric information in network based CCTV environment”, 2011 IEEE Conference on Open Systems, Langkawi, Malesia: IEEE, syyskuu 2011, ss. 86–90. doi: 10.1109/ICOS.2011.6079313.

[44] R. U. Cybersecurity, Medium, ”Cybersecurity Risks of Smart Home Devices”, url: https://medium.com/@RocketMeUpCybersecurity/introduction-to-smart-home-cybersecurity-risks-a88a0feb6f1f (viitattu: 25.5.2025)

[45] Kyberturvallisuuskeskus, ”EU:n kyberturvallisuusasetus (CSA)”, url: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/kansallinen-kyberturvallisuus-sertifioinnin-viranomainen/eun-kyberturvallisuusasetus (viitattu: 29.5.2025)

[46] MITRE, ”MITRE ATT&CK®”. url: https://attack.mitre.org/ (viitattu: 16.6.2025)

[47] Traficom, ”Radiolaitteiden tietoturvavaatimukset täsmentyvät – tarkista tuotteen vaatimustenmukaisuus ajoissa”, url: https://traficom.fi/fi/ajankohtaista/radiolaitteiden-tietoturvavaatimukset-tasmentyvat-tarkista-tuotteen (viitattu: 29.5.2025)

[48] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, ja A. Zanella, ”IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices”, IEEE Internet Things J., vsk. 6, nro 5, ss. 8182–8201, lokakuu 2019, doi: 10.1109/JIOT.2019.2935189.

[49] P. Dašić, J. Dašić, ja B. Crvenković, ”SERVICE MODELS FOR CLOUD COMPUTING: VIDEO SURVEILLANCE AS A SERVICE (VSaaS)”. Bulletin of the Transilvania University of Braşov • Series I • Vol. 9 (58) No. 2 Special Issue - 2016

[50] Rikoslaki, 24 luku 6-7§, “39-001/1889”, url: https://finlex.fi/fi/lainsaadanto/1889/39-001 (viitattu: 10.6.2025)