TURVALLISUUSJÄRJESTELMIEN DIGITAALINEN TURVALLISUUS

JULKAISIJA
Sähköinfo oy ja Turva-alan yrittäjät ry

KUSTANTAJA
Huoltovarmuusorganisaation Digipooli

KIRJOITTAJA
Ari Järvinen, KyberGuide

TAITTO
Sähköinfo oy

KANNEN KUVA
Shutterstock

Espoo 2023

ISBN 978-952-231-375-1 (pdf)

Ohjetta ovat olleet tuottamassa seuraavat tahot:

Huoltovarmuusorganisaation Digipooli ja Huoltovarmuusorganisaation Rakennuspooli, Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus, Sähköinfo oy, Turva-alan yrittäjät ry ja Finanssiala ry. Ohjeen sisältö on vapaasti käytettävissä ja jaettavissa, jos sen sisältöä ei muuteta ja lähde on mainittu.

Lisätietoja:

Antti Nyqvist, Teknologiateollisuus ry, Digipooli
antti.nyqvist@teknologiateollisuus.fi
040 861 9446

Ari Järvinen, KyberGuide
ari.jarvinen@eou-palvelut.fi
040 736 4253

SISÄLTÖ

1 JOHDANTO

Turvallisuuden keskeinen menettely on riskienhallinta. Vain tunnistettuihin riskeihin voidaan varautua. Turvatekniikka on yksi keino parantaa turvallisuutta. Turvallisuusjärjestelmillä valvotaan, ohjataan ja tuotetaan fyysisen turvallisuuden palveluita, joilla on tarkoitus suojata henkilöitä ja omaisuutta.

Sähkötieto ry:n ylläpitämä S2022-sähkönimikkeistö, joka on tarkoitettu kiinteistöjen sähköteknisten järjestelmien luokitteluun ja jäsentelyyn, luokittelee turvallisuusjärjestelmät näin:

- T5 TILATURVALLISUUSJÄRJESTELMÄT
  - T510 Sähkölukitusjärjestelmä
  - T520 Kulunvalvontajärjestelmä
  - T530 Murtoilmaisujärjestelmä
  - T540 Ryöstöilmaisujärjestelmä
  - T550 Kameravalvontajärjestelmä
  - T570 Henkilöturvajärjestelmä
  - T580 Paikannusjärjestelmä
- T6 PALOTURVALLISUUSJÄRJESTELMÄT
  - T610 Paloilmoitinjärjestelmä
  - T620 Palovaroitinjärjestelmä
  - T630 Savunhallinnan ohjaus- ja valvontajärjestelmä
  - T670 Poistumishälytys- ja turvakuulutusjärjestelmä.

Digitaalisella turvallisuudella tarkoitetaan riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen, kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Myös termiä digiturvallisuus käytetään. Lähes kaikki turvallisuusjärjestelmien palvelut ovat digitaalisia, joko kokonaan tai osittain. Esimerkiksi mekaanisen lukituksen avaintenhallinta on usein toteutettu jollakin digitaalisella palvelulla, jota on tarkasteltava vastaavalla tavalla, kuin muidenkin turvallisuusjärjestelmien hallintapalveluita.

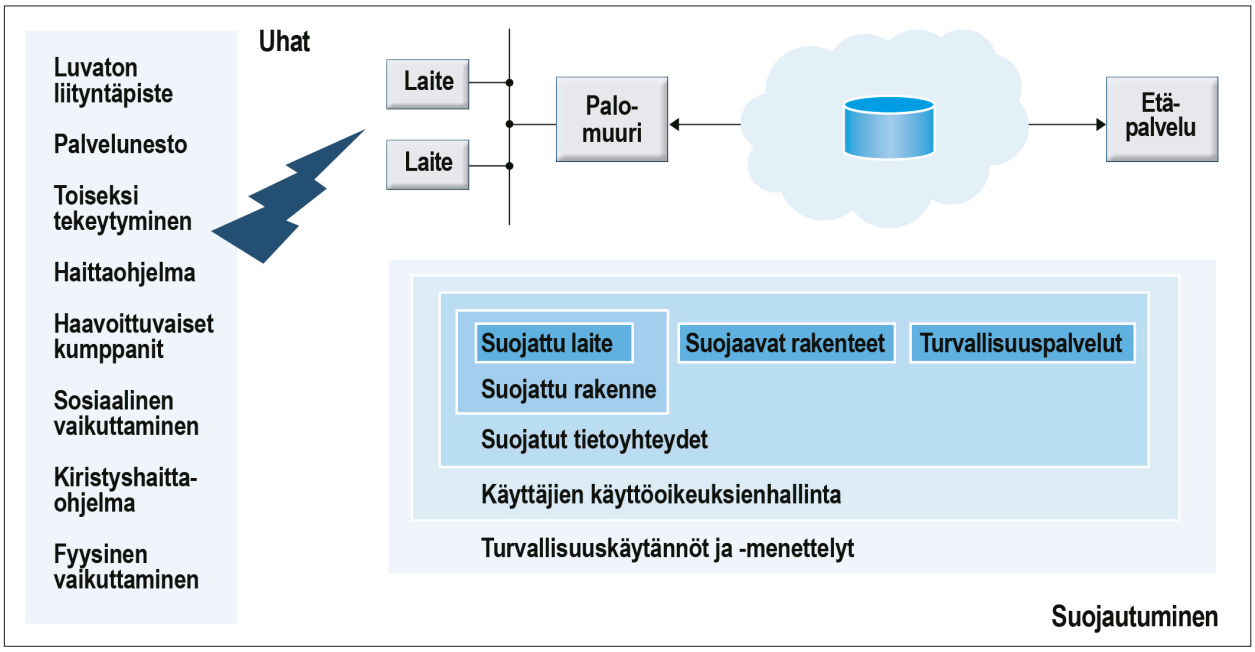
Turvajärjestelmiltä edellytetään erilaisia kyvykkyyksiä sen perusteella, ovatko ne osa tila- vai henkilöturvallisuutta, pitääkö niiden toimia palon aikana jne. Turvajärjestelmien digitaaliselle turvallisuudelle, kuten esimerkiksi ohjelmiston kyvylle estää luvaton digitaalinen vaikuttaminen, ei ole suoria vaatimuksia. Niiden digiturvavaatimukset on kuitenkin huomioitava kohteen koko elinkaaren ajan.

Tässä julkaisussa annetaan perustason ohjeita turvallisuusjärjestelmien digitaalisen turvallisuuden huomioimiseksi palvelukokonaisuuden suunnittelun ja hankinnan eri vaiheissa, toteutuksessa sekä käytössä ja ylläpidossa. Se soveltuu yleisohjeeksi turvaprojekteihin osallistuville ja myös käytettäväksi oppimateriaalina oppilaitoksissa. Ohjeessa ei oteta kantaa siihen, mitä turvallisuusjärjestelmiä ja mihin tarkoitukseen turvallisuusjärjestelmiä käytetään ja mitä yleisiä ominaisuuksia ja toiminnallisuuksia niissä tulisi olla.

Ohjeen lopussa on esitetty järjestelmäkohtaisia digitaaliseen turvallisuuteen liittyviä ohjeita sekä koottu aiemmissa luvuissa esitetyt digitaalisen turvallisuuden tarkistuslistat aihealueittain.

2 TURVALLISUUSJÄRJESTELMÄT OSANA KIINTEISTÖN DIGITAALISTA TOIMINTAYMPÄRISTÖÄ

Kiinteistöjen turvallisuusjärjestelmät ovat olennainen osa sen digitaalista toiminnallisuutta ja eri verkostoja.

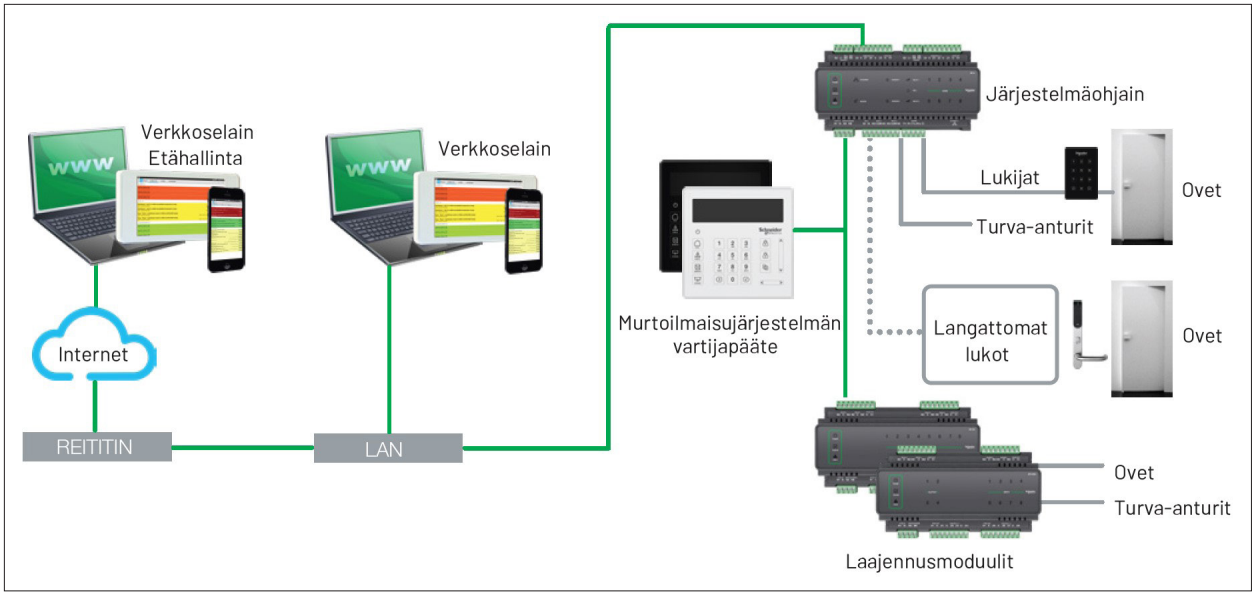


Kuva 1. Yleiskuva turvallisuusjärjestelmien digitaalisen turvallisuuden tekijöistä.

Turvallisuusjärjestelmällä tulee olla haluttu vaikutus sellaisen vahingon estämiseksi tai sellaisen vaikutuksen vähentämiseksi, joka voi kohdistua suojattavaan henkilöstöön tai omaisuuteen, joka voi olla fyysistä tai esimerkiksi dataa. Yksi keskeinen palvelukokonaisuuden kriteeri on, kuinka paljon sen avulla täytyy voittaa aikaa erilaisille, usein fyysisille suojaaville toimenpiteille, jotta uhkaava, vaarantava tai rikollinen vaikutus voidaan estää. Toisen kriteerin muodostavat kustannukset ja käytettävyys eli se, mitä suojaus maksaa ja kuinka paljon siitä voi aiheutua haittaa tavanomaiselle toiminnalle.

Kiinteistöjen turvallisuusjärjestelmät ovat kiinteistö- ja rakentamisalalla (KIRA) todennäköisiä kohteita digiturvaloukkauksille. Turvallisuusjärjestelmät eivät välttämättä ole varsinainen kohde, mutta koska niillä on tarkoitus suojata varsinaisia kohteita, turvallisuusjärjestelmien vaikutus on ensin eliminoitava tai väistettävä.

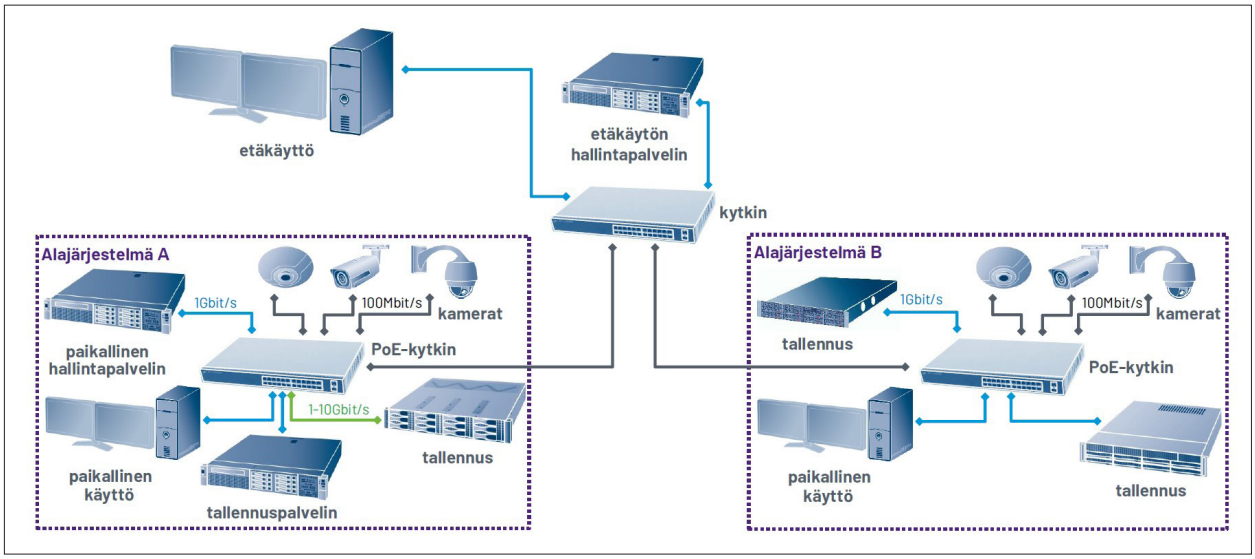
Verkkoon liitetyn tietotekniikan (IT, Information Technology) sekä operatiivisen tekniikan (OT, Operational Technology) lisääntyessä kiinteistöjen ohjaus- ja automaatiojärjestelmät (BACS/BCS, Building Automation and Control Systems) ja muun muassa tiedonsiirto integroituvat ja ulottuvat myös turvallisuusjärjestelmiin, jolloin suurempi kokonaisuus on alttiina verkkorikollisten ja muiden tietoturvallisuutta uhkaavien ryhmien vaikutukselle. Siksi on kriittistä, että digiturvallisuutta hallitaan asianmukaisesti KIRA-alan eri toimintojen (suunnittelu, toteutus, ylläpito, hallinto jne.) ja taloteknisten palveluiden suojaamiseksi mahdollisilta digiturvallisuusuhkilta ja vaikutuspyrkimyksiltä. Esimerkiksi järjestelmissä käytettävien ohjelmistojen turvallisuuteen tulee kiinnittää erityistä huomiota ja välttää maineeltaan kyseenalaisten tai tuntemattomien valmistajien ja valmistusmaiden tuotteiden ja palveluiden käyttöä, vaikka niitä tarjottaisiinkin edullisesti.



Kuva 2. Kulunvalvonnan ja murtoilmaisun yhdistävä turvallisuusjärjestelmä. (Kuva: Schneider Electric)

IT-järjestelmien riskit ovat lähinnä tietoturvaan ja -suojaan kohdistuvia ja vaikuttavat pääasiassa yritysten talouteen ja maineeseen, kun taas OT-järjestelmien riskit ovat enemmän kyberturvallisuuteen liittyviä ja voivat vaikuttaa toteutuessaan turvallisuuteen sekä uhata ihmishenkiä, omaisuutta ja ympäristöä. IT:n ja OT:n raja ei ole selvä, ja suuntaus on kohti OT:n sulautumista osaksi IT:tä.

KIRA-alan ja sen osana turvallisuusjärjestelmien digiturvallisuus on käytäntöjä, menettelyjä, ohjeita, toimenpiteitä, riskienhallintatoimia, koulutuksia, työkaluja ja tekniikoita, joita käytetään koko alan toimintojen ja kiinteistöjen palveluiden suojaamiseen. Tekniikalla on merkityksensä, mutta ihmisten toimintaa ohjaavilla aktiviteeteilla on lopputuloksen kannalta vähintään yhtä merkittävä rooli.



Kuva 3. Esimerkki laajasta kameravalvontajärjestelmästä. (Kuva: Robert Bosch Oy)

TARKISTUSLISTA | Turvallisuusjärjestelmien hallinta

Tarkista, että

- yrityksen toimitilojen turvajärjestelmien asiat on nimetty tietyn henkilön tehtäviin kuuluviksi
- turvajärjestelmille on nimetty elinkaaren eri vaiheissa vastuuhenkilö
- on olemassa kirjallinen ja hyväksytty turvallisuuskäytäntö, joka kattaa myös turvajärjestelmät
- käytössä on kirjoitettu ja hyväksytty turvallisuusohje tai turvallisuuden suunnitteluperusteet, jotka määrittävät turvatekniikan digitaalisen turvallisuuden tasot.

Muuta huomioitavaa:

- Pidetäänkö viranomaisiin, järjestöihin ja muihin organisaatioihin yhteyttä, jotta ollaan tietoisia parhaista suojauskäytännöistä?

3 TARVESELVITYS JA HANKESUUNNITTELU

Turvallisuusjärjestelmille voidaan asettaa vaatimuksia monin eri perustein. Niiltä voidaan vaatia jotakin tiettyä teknologiaa tai ominaisuutta, mutta vaatimusten on syytä perustua oikein laadittuihin uhka-arvioihin ja niistä johdettuihin vaatimuksiin, jotka halutut palvelut voivat todennetusti täyttää. Henkilöstön mukaan ottaminen turvallisuuden suunnitteluun, ylläpitämiseen ja kehittämiseen on ensiarvoisen tärkeää ja tietyissä tapauksissa myös lakisääteistä. Tarveselvitys ja hankesuunnitelma ovat luottamuksellisia, ja niissä määritellään hankkeen ja sen perusteella syntyvien muiden tietojen ja dokumenttien luottamuksellisuus mukaan lukien erilaisiin sopimuksiin, kuten suunnittelu-, ylläpito- ja palvelusopimuksiin liittyvien tietojen luottamuksellisuuden asteet.

3.1 TURVALLISUUSTASO UHKA-ARVION PERUSTEELLA

Kohteen turvallisuusjärjestelmien suunnittelu, turvasuunnitelma, perustuu suojattavaan ominaisuuteen kohdistuvien uhkien arviointiin ja niistä johdettuihin riskeihin. Turvallisuuden perustana on rakenteellinen suojaus, jota täydennetään muun muassa sähköisillä turvallisuusjärjestelmillä ja henkilöllisellä valvonnalla. Koska toimitilaturvallisuuden järjestelyt riippuvat paljon kohteen rakenteellisista turvallisuusratkaisuista, tulee turvasuunnittelu etenkin uudisrakennuksessa tehdä riittävän ajoissa.

Turvallisuusjärjestelmien tulee kiinteistön elinkaaren aikana mukautua monista syistä toimitilaturvallisuuden vaatimusten muutoksiin. Muutoksia tapahtuu muun muassa käyttäjäorganisaation vaihtuessa, jolloin turvallisuusvaatimuksetkin muuttuvat, tai kun niitä ohjaava järjestelmä, kuten esimerkiksi kulunvalvontajärjestelmä, vaihtuu eri valmistajan järjestelmäksi.

Turvallisuushanke kannattaa aloittaa perusteellisella turvallisuussuunnitelmalla. Siinä selvitetään tilan käyttäjän toimintaan ja kohteeseen liittyvät riskit sekä toimitilaturvallisuuteen vaikuttavat osatekijät unohtamatta digitaalista turvallisuutta. Suunnittelun tavoitteena on järjestää kiinteistöjen tilojen käytön sijoittelu, vyöhykkeet ja rakenteelliset suojaukset siten, että henkilöllistä valvontaa tarvitaan mahdollisimman vähän ja toisaalta sähköisten turvallisuusjärjestelmien määrä ja laajuus pysyvät kohtuullisina.

Turvallisuussuunnitelmaan kirjataan kohteen turvallisuustavoitteet ja määritellään turvaratkaisujen toiminnalliset vaatimukset. Koska turvallisuusjärjestelyt hankittavine tekniikkoineen edustavat merkittävää kustannusta, on tärkeää, että järjestelyt mitoitetaan oikein. Lisäksi suunnitelma toimii jatkossa työkaluna turvallisuutta kehitettäessä ja tavoitteita tarkistettaessa.

VINKKI

Turvallisuussuunnittelun apuna voi käyttää Seclion Oy:n laatimaa ilmaista työkalua, jonka avulla voi tunnistaa turvallisuuden ydinongelmat, saada yleisarvosanan turvallisuustilanteesta ja päästä alkuun soveltuvien kehitystoimenpiteiden määrittelyssä ja käynnistämisessä.

Linkki: **https://blog.seclion.fi/turvallisuus/turvallisuussuunnitelma**.

Turvallisuussuunnittelussa voidaan hyödyntää myös esimerkiksi seuraavia aineistoja:
- ST 70.40 Rakennusten digitaalinen turvallisuus. Tilaajan ohje (RT 103206)
- ST 70.41 Rakennusten digitaalinen turvallisuus. Suunnittelijan ohje (RT 103207)
- ST 95.12 Rakennusten digitaalinen turvallisuus. Kiinteistön ylläpidon ohje (RT 103208)
- ST-ohjeisto 4 Kiinteistö- ja tilaturvallisuuden tasot.

Nämä jakavat turvallisuustasot neljään digitaalisen turvallisuuden luokkaan seuraavasti:
- taso 1: perussuojaus (DT1)
- taso 2: tehostettu perussuojaus (DT2)
- taso 3: erityissuojaus (DT3)
- taso 4: täyssuojaus (DT4).

Näiden aineistojen avulla voidaan kartoittaa kiinteistössä tarvittava turvallisuustaso ottaen huomioon alueet, tilat, rakenteellinen suojaus, tarvittavat turvallisuusjärjestelmät ja digitaalinen turvallisuus.

TARKISTUSLISTA | Turvallisuustaso uhka-arvion perusteella

Tarkista, että
- rakennushankkeen asiakirjoille tehdään luottamuksellisuusluokittelu
- käytössä on turvajärjestelmän digitaaliseen turvallisuuteen kohdistuva uhka-arvio
- toimitilojen turvatekniikka on huomioitu riskienhallintamenettelyssä riittävän yksityiskohtaisesti
- toimitilojen kriittisyysluokat tunnetaan ja haavoittuvuudet on kartoitettu
- turvatekniikan toiminnot on sijoitettu riskiarvion edellyttämälle turvallisuusvyöhykkeelle
- turvajärjestelmien data säilytetään EU:n alueella ja sen käsittelyssä noudatetaan tietosuojasta annettuja lakeja ja asetuksia
- kaikki toimitilan turvajärjestelmiin liittyvät tehtävät ovat tiedossa ja niihin liittyvät riskiarviot on tehty
- järjestelmäkohtaiset kunnossapito-ohjelmat on laadittu.

3.2 KÄYTTÖ- JA YLLÄPITOMALLIT

Turvallisuusjärjestelmiä voidaan käyttää periaatteessa kolmella eri tavalla: suojattavan kohteen omin resurssein, ulkoistamalla operointi turva-alan yritykselle tai näiden yhdistelmänä. Vastaavasti tekninen ylläpito voidaan toteuttaa kolmella tavalla: omin resurssein, ulkoistamalla ylläpito toimittajille tai heidän edustajilleen tai näiden yhdistelmänä. Vastuu turvallisuusjärjestelmien ylläpidosta on kuitenkin niiden omistajalla tai haltijalla. Digitaalisen turvallisuuden kannalta ei ole merkitystä, miten operointi tai ylläpito toteutetaan, ainoastaan sovitut vastuut niihin liittyvästä huolehtimisesta ja laillisuuden noudattamisesta kohdistuvat eri tahoihin.

Turvallisuusjärjestelmiä käytetään vain niihin tarkoitetuissa ympäristöissä, päätelaitteilla ja tiedonsiirtoyhteyksillä. Ei siis omin laittein ja kotoa käsin, jos niin ei ole suunniteltu ja sovittu. Jäykkää, mutta riskittömämpää.

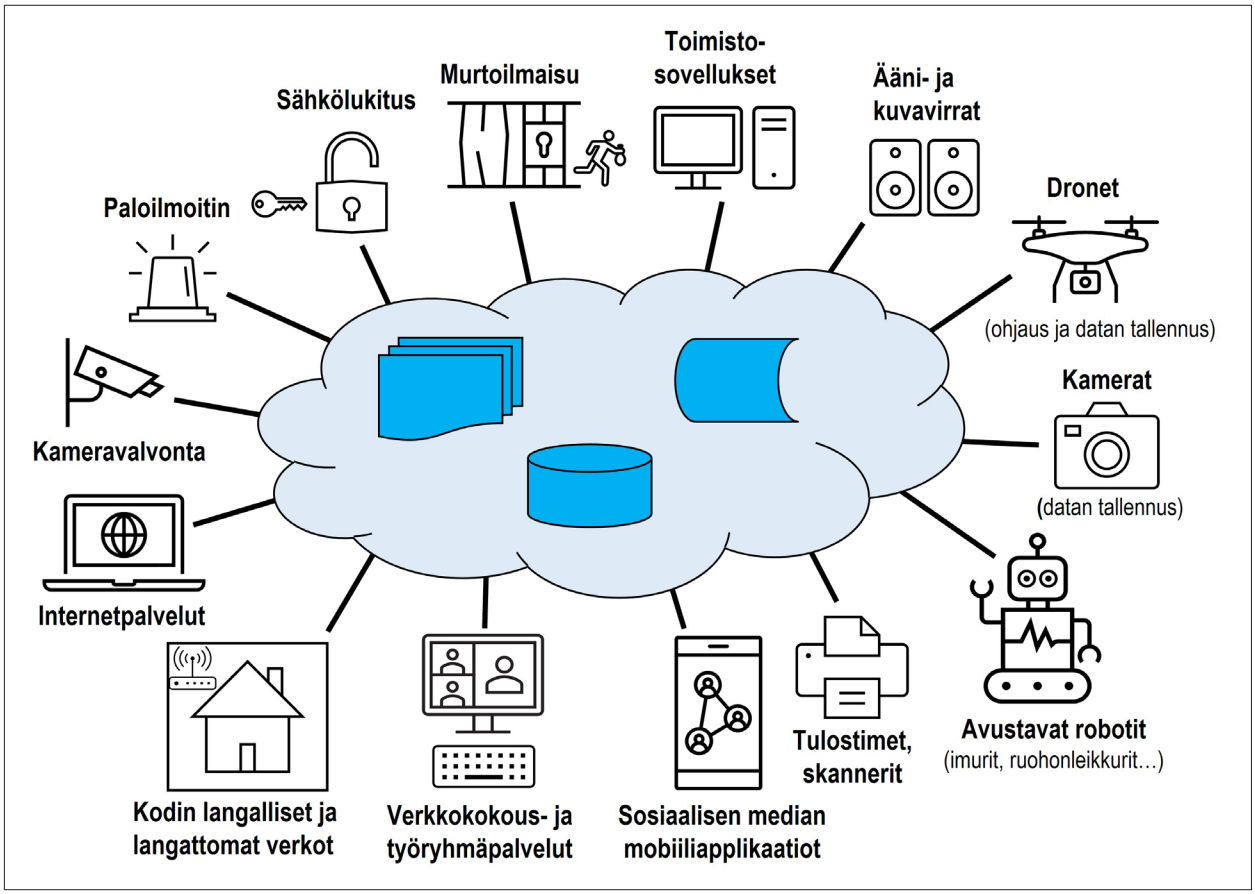
Digitaalisten riskien kannalta malleilla on eroja. Internetiä hyödyntävä etäkäyttö lisää digiriskejä ja ulospäin täysin yhteydetön käyttö vähentää niitä. Ulkoistuksen sopimuksissa on varmistuttava palveluntarjoajan toimintaympäristön ja -kulttuurin vastaavan sitä, mitä turvallisuussuunnitelman mukaan siltä edellytetään. Turvallisuussuunnitelma luo siis perusteet vaatimuksille, joihin operointimallin on vastattava. Ei siis ole vain yhtä mallia, joka soveltuu kaikille.

Turvallisuusjärjestelmää käyttävän organisaation velvollisuudet ja tehtävät digitaalisen turvallisuuden toteuttamisessa ja ylläpidossa tulee määritellä heti projektin alkuvaiheessa. Järjestelmän omistajaa edustavan tulevan pääkäyttäjän tulisi olla toteutuksessa mukana asennusten alusta lähtien, jotta hänellä olisi valmius suunnitella digitaalisen turvallisuuden osalta käytön prosessit, tehdä ohjeistus käyttäjille sekä ottaa vastaan annettu koulutus. On suositeltavaa, että kohteen turvallisuudesta vastaavalla henkilöstöllä on aina pääsy turvallisuusjärjestelmiin.

Harvalla käyttäjäorganisaatiolla itsellään on talotekniikan huoltoon tai digitaalisen turvallisuuden ylläpitoon koulutettua erityishenkilöstöä. IT-järjestelmiäkin huoltavat yleensä ulkopuolisen palveluntuottajan henkilöt. Myös turvallisuusjärjestelmien ja niiden digitaalisen turvallisuuden ylläpitotehtävät voidaan ulkoistaa valitulle palveluntuottajalle. Järjestelmän kehittäminen kannattaa kuitenkin pitää omissa käsissä. Jollei käyttäjällä ole kehittämisessä vaadittavia resursseja ja osaamista, voi kehitystarpeissa kääntyä riippumattoman asiantuntijan puoleen.

3.3 ARKKITEHTUURIMALLI

Turvallisuusjärjestelmien tietojenkäsittely voidaan toteuttaa pilvipalveluna (kuva 4), paikallisesti tai niiden yhdistelmänä, kunhan huolehditaan etenkin tietosuojaan liittyvistä vaatimuksista. Jos järjestelmälle asetetaan vaatimus häiriöttömästä toiminnasta ilman etäyhteyttä, paikallinen tietojenkäsittely ja -tallennus on toteutettava ainakin osittain. Pilvipalveluiden käytön sopimusten on vastattava kaikkia muitakin palvelusopimuksia vastuunjaon selkeyden ja LES-vaatimusten osalta (tietoturvan kolme osa-aluetta: luottamuksellisuus, eheys ja saatavuus).



Kuva 4. Pilvipalveluita ja niiden käyttäjiä.

Pilvipalvelut ei ole sama asia kuin etäkäyttö. Pilvipalveluissa suurin osa tietojenkäsittelyn tarvitsemasta infrastruktuurista, kuten palvelimet ja ohjelmistot, sijaitsevat joissain verkon lukuisista palvelinkeskuksista. Näiden suorituskyky voi vaihdella ja ajoympäristön fyysinen sijoittuminen voidaan rajoittaa esimerkiksi vain EU:n alueelle. Etäkäyttö on yksi palvelu, joka voi olla toteutettu pilvipalveluna, mutta näin ei välttämättä tarvitse olla.

Pilvipalveluilla on puolensa, mutta aina ei ole edes mahdollista valita, saako palvelun pilvestä vai tuottaako sen omin resurssein. Joskus pilvipalvelu on ainoa mahdollisuus. Pilvipalveluilla voidaan tavoitella kustannustehokkuutta, mutta aina, kun dataa käsitellään jossain muussa kuin omassa ympäristössä, siihen liittyvät turvallisuustekijät on huomioitava. Sinällään pilvipalvelut voivat olla etenkin suurilla toimijoilla hyvinkin turvallisesti toteutettuja. Mitään takeita ei välttämättä kuitenkaan ole siitä, etteivätkö pilvipalveluja tarjoavat yritykset käyttäisi palveluun tallentuvaa tietoa omaksi hyödykseen.

3.4 KÄYTTÖTARKOITUS

Turvallisuusjärjestelmän käyttötarkoitus ja sen eri alijärjestelmiltä halutut toiminnot vaihtelevat kohteittain. Usein turvajärjestelmä ei itsessään voi suojata omaisuutta tai henkilöstöä, vaan sen tehtävä on hälyttää riittävän aikaisin, jotta tilanteen kehittymiseen voidaan vaikuttaa oikeilla toimenpiteillä, kuten esimerkiksi alkusammutuksella tai turvahenkilöstön paikalle saamisella. Oikein mitoitetut toimitilaturvallisuuden ratkaisut helpottavat turvallisuustason ylläpidossa ja kehittämisessä. Nämä hankintaprosessin lähtötiedot on suositeltavaa kartoittaa ja määritellä jo kohdekohtaisessa turvallisuussuunnitelmassa ennen hankesuunnitelmaa ja varsinaisia investointipäätöksiä. Yhtä tärkeää on, että järjestelmän käyttötarkoitus, toiminnot ja esimerkiksi digitaalisen turvallisuuden ylläpito kuvataan yksiselitteisesti varsinaisissa urakkatarjouspyyntöasiakirjoissa ja urakkasopimuksessa.

ESIMERKKI

Pääsynhallinta liittyy useampaan turvallisuusjärjestelmään. Käsitteeseen sisältyvät muun muassa seuraavat osa-alueet, joissa digitaalinen turvallisuus tulee huomioida:

- kulunvalvontajärjestelmä
- avainjärjestelmä
- ovipuhelin
- vierailijahallinnan järjestelyt
- ID-kortin käyttö.

Näihin liittyvät järjestelyt tulee linjata ennen kuin lähdetään suunnittelemaan turvallisuusjärjestelmiä ja niiden digitaalista turvallisuutta. Hankinta- ja toteutusvaiheet hankaloituvat ja käytönaikainen turvallisuus vaarantuu, jos toimitilaturvallisuuden järjestelmät eivät ole toiminnallisesti ja digitaalisen turvallisuuden ylläpidon kannalta yhteensopivia.

Digitaalisen turvallisuuden osalta määrittelyt voidaan tehdä yleisesti kaikissa eri osajärjestelmissä noudatettavaksi tai räätälöidä ne järjestelmittäin kattaen myös asennukset, operoinnin, ylläpidon ja käytöstä poiston.

3.5 TIEDON LUOTTAMUKSELLISUUS JA TIETOSUOJA

Turvallisuusjärjestelmien tietoturvariskit voivat toteutuessaan aiheuttaa ongelmia sekä itse järjestelmien toiminnalle että myös muulle kiinteistön toiminnalle ja heikentää näin tilaturvallisuutta.

Lähes kaikki turvallisuusjärjestelmistä kerätty tieto ja kaikki järjestelmän suunnitelma- ja todennusdokumentit ovat luottamuksellisia. Lokit ja tallenteet voivat paljastaa järjestelmän heikkouksia tai puutteita tai niistä voi käydä ilmi henkilötietoja. Järjestelmän suunnitelma- ja todennusdokumentteja sekä käytön aikana syntyviä digitaaliseen turvallisuuteen liittyviä dokumentteja on säilytettävä ja ylläpidettävä niistä sovitulla tavalla, jotta luottamuksellisuus-, eheys- ja saatavuusvaatimukset toteutuvat elinkaaren eri vaiheissa ja tarpeissa. Lisäksi on huomioitava turvasuojaustehtäviin ja tietosuojaan liittyvä lainsäädäntö.

Erityistä huomiota tulee kiinnittää käytettyjen tiedonsiirtoverkkojen suojaukseen sekä etäkäytön ja mahdollisten pilvipalveluiden tietoturvaan, tietosuojaan ja käyttäjien hallintaan. Ei ole aivan yhdentekevää, missä maassa dataa säilytetään tai käsitellään ja mistä etänä tehtävät hallinnan operaatiot toteutetaan.

3.6 LAINSÄÄDÄNTÖ

Tietosuojaan ja salassapitoon liittyvien säädösten lisäksi turvallisuusjärjestelmiin liittyy paljon muutakin lainsäädäntöä. Osa siitä koskee järjestelmän teknisen toiminnan luotettavuuden varmistamista, kuten esimerkiksi palon ilmaisussa ja sammutuksessa, osa esimerkiksi tietosuojaa, kuten kameravalvonnassa. Koska kyseessä on yleensä luottamuksellisten tietojen käsittely ja palveluiden tuottaminen, vaaditaan eri osapuolilta pätevyyksiä, rekisteröitymistä tai viranomaisen lupa toimia kyseisissä tehtävissä.

ESIMERKKI

Laki yksityisistä turvallisuuspalveluista (LYTP, 1085/2015)

Lain mukaan lukitus-, murtoilmaisu- ja kulunvalvontajärjestelmien asentamis- ja ylläpitotehtäviä saa harjoittaa vain yritys, joka on saanut turvallisuusalan elinkeinoluvan. Kyseisiä hyväksymistä edellyttäviä turvasuojaustehtäviä suorittavilla henkilöillä tulee olla voimassa oleva turvasuojaajakortti.

Turvallisuusjärjestelmien lainsäädäntöä on käsitelty tarkemmin muun muassa seuraavissa julkaisuissa:

- ST-käsikirja 11 Kulunvalvonta- ja murtoilmaisujärjestelmät
- ST-käsikirja 13 Kameravalvontaopas
- ST-käsikirja 18 Sähköinen oviympäristö
- ST-ohjeisto 1 Paloilmoittimen suunnittelu, asennus ja ylläpito
- Turvaa oikein -opas (**https://www.turva-alanyrittajat.fi/turvaa_oikein_opas**).

4 PALVELUSOPIMUKSET

Turvallisuusjärjestelmien laitteiden ja ohjelmistojen valmistajasta riippuu, miten vapaat kädet käyttäjällä on ylläpitopalvelun tuottajan valintaan ja sopimuksen sisältöön. Yhteistyökumppania valittaessa tulee varmistaa, että kyseinen yritys hallitsee kohteessa toimivat järjestelmätuotteet, ohjelmistot ja laitteiden toimintaympäristöt, kuten palvelimet ja tietoverkot sekä palveluihin liittyvän digitaalisen turvallisuuden ja sen hallinnan. Turvasuojaajakortti tulee vaatia mahdollisimman laajasti palvelujen tuottamiseen osallistuvilta henkilöiltä ja vähintään hyväksymistä edellyttäviä turvasuojaustehtäviä tekeviltä.

Ylläpitosopimusten sisällössä ja kustannuksissa on suuria eroja. Sopimus voi kattaa kaikki kustannukset ennakkotarkastuksista huoltotyöhön varaosineen ja ohjelmistopäivityksineen tai ääritapauksessa kattaa vain sen, että yhteistyökumppani on tarvittaessa käytettävissä, mutta kustannukset peritään erillisen hinnaston mukaisesti.

Palvelusopimuksissa on huomioitava myös aktiivisen palvelun jälkeinen aika, jotta muun muassa salassapitoon ja tietosuojaan liittyvät sopimusehdot kattavat tarvittavan ajanjakson myös varsinaisen palvelutuotannon päättymisen jälkeen.

Keskeisiä digiturvallisuuden kannalta huomioitavia asioita hankkeissa ja niihin liittyvissä palvelusopimuksissa sekä niihin liittyvissä erilaisissa turvallisuussopimuksissa ovat:

- dokumentaatio palvelukokonaisuudesta on laadittu, ylläpidetty, säilytetty ja suojattu asiattomalta käytöltä sille asetettujen vaatimusten mukaisesti
- sopimukset kattavat myös poikkeamaraporttien käsittelyn ja niiden perusteella tehtävistä toimenpiteistä sopimisen, jotta tilanne ei voisi uusiutua
- turvallisuusjärjestelmien suunnittelun ja toteutuksen hankintatavat ja sopimusten sisältö tehdään niille asetettujen vaatimusten mukaisesti
- hankittavan kokonaisuuden digiturvavaatimukset ovat harkittuja, asianmukaisesti katselmoituja ja riskiarvioihin suhteutettuja
- eri toimijoihin kohdistuvat luottamuksellisuusvaatimukset ovat dokumentoituja ja vaatimusten täyttymistä seurataan dokumentoidusti
- eri osapuolten velvollisuudet ja vastuut poikkeustilanteissa on sovittu ja dokumentoitu mukaan lukien eri tapaustyyppeihin liittyvät prosessit (esimerkiksi kokonaispalvelusopimuksessa palvelutoimittajan velvollisuus vastata vartioinnista tai opastuksesta tilaturvallisuus- tai poistumisvalojärjestelmien häiriötilanteissa).

VINKKI

Laitevalintojen yhteydessä voi soveltaa **sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimuksia**.

TARKISTUSLISTA | Palvelusopimukset

Tarkista, että

- toimitilojen turvajärjestelmien ylläpitäjät mukaan lukien urakoitsijat ja kolmannet osapuolet on tarkistettu ja valtuutettu tehtäviinsä
- turvajärjestelmien ulkoistetut ylläpitäjät toimivat valvotusti
- ylläpidon reagointi- ja palautumisajat turvajärjestelmien häiriöihin on määritetty.

5 LAITEVALINNAT

Laitevalinnoille ja toteutusvaihtoehdoille on useita kriteerejä. Jotkut vaatimuksista ovat ehdottomia, jotkut ehdollisia, jolloin vaatimuksen täyttymyksen aste vaikuttaa valintoihin. Hankkeessa kannattaa käyttää sellaista vaatimusten hallinnan sovellusta (RM, Requirements Management), josta tilaajaorganisaatiolla on kokemusta. Kun digiturvallisuus on yksi kriteerijoukko, se vaikuttaa valintoihin vain, jos joku tarjoajista ei täytä asetettuja vaatimuksia. Esimerkiksi järjestelmissä käytettävien ohjelmistojen turvallisuuteen tulee kiinnittää erityistä huomiota ja välttää maineeltaan kyseenalaisten tai tuntemattomien valmistajien ja valmistusmaiden tuotteiden ja palveluiden käyttöä, vaikka niitä tarjottaisiinkin edullisesti.

Vaatimustenhallinta tuo lisää varmuutta koko elinkaaren hankintapäätöksiin ja pitävyyttä sopimuksiin, kun vaatimukset on laadittu ja ylläpidetty oikein, eli yksilöivästi ja vaatimalla myös todisteet vaatimusten täyttymisestä. Laitevalmistajan digiturvallisuuspanostuksia voi arvioida sen tuotekehityksen auditoinneilla tai testaamalla tuotteita ja vertaamalla niitä valittuihin vaatimuksiin, standardeihin ja sertifikaatteihin. Myös auditointien ja sertifikaattien ajantasaisuuteen tulee kiinnittää huomiota ja hyväksyä vain riittävän tuoreet osoitukset.

Turvallisuusjärjestelmien tulee mukautua toimitilaturvallisuuden vaatimusten muutoksiin, jotka voivat olla seurausta esimerkiksi tilan käyttötarkoituksen muutoksesta aiheutuvan luokituksen muutoksesta tai kokonaan uuden toimipisteen lisäämisestä. Turvallisuusjärjestelmien digitaalisen turvallisuuden tulee mukautua sitä uhkaavien riskitekijöiden muutoksiin siten, että asetettu vaatimustaso pystytään toteuttamaan.

Turvallisuusjärjestelmiin kohdistuvia muutostarpeita voi vähentää, jos niissä on alun perin käytetty avoimia, valmistajasta riippumattomia komponentteja. Tietoverkkojen kytkimien on suositeltavinta olla sellaisia, jotka ilmaisevat fyysisen yhteyden poikkeamat. Kun ne ylittävät tietyn tai tietyt raja-arvot, yhteys katkaistaan odottamaan tarkastusta ja hallittua uudelleenaktivointia tai vähintään kytkimen hallintaohjelmiston tuottamien hälytysten selkeää käsittelyä valvomo-ohjelmistoissa. Eri toimittajien laitteiden käyttöön voi vaikuttaa myös esimerkiksi yhteensopivuus kaapeloinnin sabotoinnin ilmaisuun käytettävissä päätevastuksissa.

TARKISTUSLISTA | Laitevalinnat
Tarkista, että • käytetään luotettavia laitevalmistajia • laitevalmistajilla on dokumentoitua näyttöä laitteiden ja järjestelmien turvallisuudesta.

6 SUUNNITTELU

Kokonaisturvallisuus on monen tekijän tulo, ja niin on myös digiturvallisuus. Sen toteuttamiseksi turvallisuusjärjestelmien suunnittelussa on huomioitava muun muassa hallinnolliset keinot ja henkilöturvallisuus, digitaalisen ympäristön fyysinen suojaus, itse digiturva sekä toimet digiturvan osalta turvallisuusjärjestelmien poikkeus- ja hälytystilanteissa, toiminnan jatkuvuuden hallinnassa ja järjestelmien sekä palveluiden yhteensopivuudessa ja ylläpidossa.

Lähtökohtaisesti turvallisuuspalveluiden vaatima tekniikka tulee sijoittaa suojatun rakenteen sisäpuolelle. Ulkopuolelle jäävien teknisten järjestelmien ja niiden osien koskemattomuutta pitää valvoa tehostetusti ja soveltuvin menetelmin. Erityistä huomiota tulee kiinnittää käytettyjen tiedonsiirtoverkkojen suojaukseen sekä etäkäytön ja mahdollisten pilvipalveluiden tietoturvaan, tietosuojaan ja käyttäjien hallintaan. Lisäksi on sovittava, miten digitaaliseen turvallisuuteen liittyvät asiat dokumentoidaan ja säilytetään käyttöoikeudet huomioiden.

VINKKI

Turvallisuusjärjestelmien suunnittelussa on hyvä noudattaa ohjetta Cenelec TC79/WG17 "Reference Standards and Guidance on Best Practice Cyber Security for Alarm Systems" ja siinä viitattuja ohjeita sekä standardeja.

6.1 KAAPELOINTI, LAITESIJOITTELU JA LAITTEIDEN TOIMINTAVARMUUS

Liikenne- ja viestintäviraston määräys 65 kiinteistön sisäverkoista ja teleurakoinnista sisältää yleiset vaatimukset rakennusten teletilojen, kuten jakamojen ja vastaavien laitetilojen sekä jakorasioiden lukitukselle. Liikekiinteistön laitetilojen turvallisuusvaatimukset voivat olla määräystä tiukemmat. Turvallisuusjärjestelmien käyttö- ja ohjauslaitteet sijoitetaan aina valvotulle alueelle, ja valvontaan esimerkiksi magneettikoskettimilla tai liikeilmaisimilla ohjelmoidaan viive, jonka aikana käyttö- tai ohjauslaitetta voidaan käyttää aiheuttamatta hälytystä. Käytännössä kaikkien muiden laitteiden ja niihin kytkeytymisen mahdollistavien liitosten ja liittimien on oltava vähintään lukitussa tilassa, aktiivilaitteiden ja kaapeloinnin kytkentäkaappien mieluiten valvotussa ja murtoilmailmaisimilla varustetussa tilassa. KTL1E-lukitusjärjestelmä on suosituksen mukainen tapa lukita kiinteistöjen tekniset tilat sekä reittiavaimille tarkoitetut avainsäilöt uusissa ja saneerauskohteissa.

Kaapelointiin liittyviä vaatimuksia ovat sähköinen yhteensopivuus siten, että toiminnallisuus (esim. signaalit siirtyvät vääristymättä) ja ympäristö (mm. EMC, paloturvallisuus ja palonkesto sekä fyysinen suojaus) huomioidaan. Kaapelointia ohjaavat standardit EN 50173-6 Rakennusten hajautetut järjestelmät ja EN 50174 -sarja, joka koskee kaapeloinnin spesifiointia, suunnittelua, laadunvarmistusta, asennusta, käyttöä ja ylläpitoa. Kaapelireitit tulee suojata mahdollisuuksien mukaan, ja järjestelmän tulee ilmaista kaapelien sabotointi. Kaapeloinnin kytkentärasioissa pitää käyttää kansikytkimiä, ja lukittavien päätekaappien pitää olla valvotuissa tiloissa turvallisuusjärjestelmien muiden laitteiden yhteydessä suojattavan kohteen sisäalueilla.

Turvallisuusjärjestelmien laitteiden tilaa ja kuntoa valvotaan. Niiden energian saanti (UPS tai DC-syötön akusto) varmistetaan kunkin järjestelmän vaatiman tehon ja toiminta-ajan mukaisella kapasiteetilla. Tehonsyöttöä valvotaan siten, että ennen akku- tai UPS-varmistuksen kapasiteetin loppumista tieto siitä voidaan välittää valittuun valvomoon. Langattomien laitteiden paristojen vaihto suunnitellaan huolto-ohjelmaan.

Laitevalintoja tehtäessä tuotteilta vaaditaan riskiarvion mukaista luotettavuutta (MTBF, Mean Time Between Failures, keskimääräinen vikaväli) ja käytettävyyttä, joita voidaan parantaa redundanttisuudella. Laitetoimittajan sopimusten tulisi kattaa myös selkeät menettelyt siitä, miten raportoidaan tuotteiden vanhentumisesta ja laitetyypin tai sen kriittisten komponenttien todetusta luotettavuudesta.

TARKISTUSLISTA | Kaapelointi ja laitesuojaus

Tarkista, että
- turvallisuusstrategia huomioi turvajärjestelmien fyysisen suojaamisen
- turvatekniikan kaapelien ja verkkojen fyysisessä suojauksessa noudatetaan rakennusten sisäverkoista annettuja määräyksiä esimerkiksi lukituksessa
- fyysistä pääsyä kaikkiin turvatekniikan järjestelmiin ja niiden laitteistoihin ja ohjelmistoihin hallitaan ja valvotaan
- turvatekniikan ohjaimet, reitittimet ja verkkokytkimet on fyysisesti suojattu
- turvatekniikan verkkolaitteet ja ohjaimet on sijoitettu valvottuihin tai kahdella toisistaan riippumattomalla tavalla valvottuihin tiloihin
- turvatekniikan laite- ja kytkentäkotelot ovat turvallisella ja suojatulla alueella / lukittu
- käytössä on turvatekniikan vaatimien tilojen fyysisten avainten hallinnan käytännöt ja menettelyt mukaan lukien palauttamisen valvonta
- turvatekniikan laitteissa on ilmaisu niiden peukaloinnille / kotelot ovat tunkeutumisen kestäviä / koteloissa on ilmaisu luvattomalle tunkeutumiselle / säilytys on toteutettu siten, että niitä ei voi siirtää tiloista pois
- toimitilojen turvatekniikan tietoliikennekaapelit on suojattu
- turvajärjestelmien kenttätason laitteet on yhdistetty sabotaasin ilmaisevia kaapeleita käyttäen
- kaapelien valvonta ilmaisee häiriön ja laitteiden peukaloinnin myös laitteen ollessa poissa käytöstä
- fyysinen suojaus tarjoaa todisteita turvatekniikan järjestelmien ja laitteiden luvattomasta käytöstä, peukaloinnista tai niiden yrityksestä.

6.2 SALAAMINEN, HÄIRINNÄNSIETO JA OMASUOJAUS

Järjestelmän rakenne, toteutusratkaisut ja vasteajat ovat luottamuksellisia tietoja. Suunnitelmatietoihin ja tarkastuspöytäkirjoihin on siis estettävä pääsy asiattomilta, mutta niihin on kuitenkin oltava pääsy asianmukaisilla henkilöillä siten, että käytettävyys ei vaarannu, vaikka tiedot säilytetään salattuina ja niitä luovutetaan vain kontrolloidusti ja salatusti.

Itse järjestelmissä salaaminen liittyy lähinnä tiedonsiirtoon sekä loki- ja konfiguraatiotietoihin. Tiedonsiirto voi tapahtua langallisesti tai langattomasti, ja se on aina salattava sekä osapuolet tunnistettava (autentikoitava). Salaus- ja tunnistustekniikat ja niiden taso vaihtelevat eri toimittajien tuotteissa, joten tässäkin on syytä viitata suunnitelmiin ja vaatimustenhallintaan, jotta soveltuva ratkaisu tulee valituksi.

Turvallisuusjärjestelmien toimintaa voidaan pyrkiä myös häiritsemään. Häirintä voi olla harhauttavaa tai peittävää, ja vaikka se olisi analogista tai fyysistä, sen vaikutus ulottuu digitaaliseen tietojenkäsittelyyn, joten kyse on myös digitaalisesta turvallisuudesta. Häirintään voidaan varautua ja sen vaikutuksia pienentää hyvällä suunnittelulla ja vaatimustenhallinnalla. Pienet ilmaisualueet ja rinnakkaisten tekniikoiden käyttö helpottavat vaikutuksen rajaamista ja poikkeustilanteen vaatimaa lisäresursointia, mutta vastaavasti investointikustannukset lisääntyvät. Myös isoihin turvallisuusvalvomoihin syntyvä laaja tilannekuva voi auttaa tunnistamaan harhautukset ja havaitsemaan ajoissa suojattavaa kohdetta uhkaavan toiminnan. Keskittämällä turvallisuuspalvelut yhdelle operaattorille voidaan myös säästää kustannuksissa.

Omasuojaus on lähinnä ilmaisimiin tai niiden kytkentöihin vaikuttamiselta sekä sabotoinnilta suojautumista. Järjestelmän kaapelointiin ja sen kytkentäkoteloihin tunkeutuminen tai vaikuttaminen katkaisemalla, oiko- tai maasuluin tai muilla tavoin voidaan ilmaista monin keinoin.

ESIMERKKI

Kameravalvonnassa ja valvomoiden etähallintayhteyksissä käytetään yleisesti sähköistä, moniparista kaapelia ja Ethernetiä tiedonsiirtoon. Jos siirtotiellä tapahtuu muutos, se voidaan ilmaista, ja myös paikantaa muutoskohta. Myös valokuituyhteydet ovat valvottavissa vastaavalla tavalla.

Langattomassa tiedonsiirrossa väärinkäyttö tulee estää salaamalla ja autentikoimalla. Valvomoyhteyden häiriintymisestä tai katkeamisesta tulisi tehdä myös paikallinen hälytys. Tapahtumista syntyvät lokimerkinnät ja käynnistettävät toimenpiteet tulee käsitellä luottamuksellisesti. Sähköisen suojauksen EMC-vaatimukset (sähkömagneettinen yhteensopivuus) löytyvät standardista SFS-EN 50130-4.

Myös turvallisuusjärjestelmien käyttämän aikareferenssin suojaus on huomioitava. Internetistä käytettävää NTP-palvelua (Network Time Protocol) voidaan häiritä, samoin kuin GPS:ään ja muihin satelliittipaikannuspalveluihin perustuvaa aikareferenssiä, joten niiden häirintä pitää pystyä havaitsemaan ja siirtymään tarvittaessa automaattisesti paikallisen, suojatun referenssin käyttöön, jotta esimerkiksi tallenteiden ja lokien analysointi ja todistusvoimaisuus mahdollistuvat.

TARKISTUSLISTA | Salaus

Tarkista, että
- turvatekniikan kenttätason yhteydet on toteutettu kaksisuuntaisesti pollaavasti ja vähintään 128-bittisellä AES-avaimella (Advanced Encryption Standard) salatusti.

6.3 VERKON RAKENNE

Verkolla tarkoitetaan tässä yhteydessä eri keskusten ja järjestelmien sekä etäyhteyksien käyttämiä IP-verkkoja (Internet Protocol). Fyysisesti verkko koostuu välityslaitteista, kuten kytkimet, reitittimet ja langattoman tiedonsiirron tukiasemat, kaapeloinnista, kuten yleiskaapeloinnista (toteutettu kierretyistä johdinpareista muodostuvalla kaapeloinnilla tai valokuiduilla), sekä muiden liittyvien laitteiden verkkoliitynnöistä. Loogisesti verkko on huomattavasti fyysistä verkkoa monimutkaisempi ja rakentuu erilaisista tiedonsiirtoa ohjaavista ja rajoittavista säännöistä, tasoista, protokollista jne.

Yhden tiedonsiirtoväylän tai -tavan vian tai häiriön vaikutusta voi vähentää käyttämällä kahdennettuja ratkaisuja. Langallinen tiedonsiirto voidaan korvata langattomalla tai siirtää liikenne käyttämään toista langallista yhteyttä. Tällaisen järjestelmän suunnittelu, laitevalinnat ja ylläpito vaativat hieman enemmän osaamista, kun tehdään verkon fyysistä toteutusta, mutta vielä enemmän osaamista tarvitaan järjestelmän loogisen toiminnan hallitsemiseen.

Verkko on suunniteltava huolella, jotta sen toteutukseen tarvittavien hankintojen vaatimusmäärittelystä saadaan riittävän tarkka. Koska IT-alalla kehitys on nopeaa, suunnitelmien ja toteutusten elinkaaret eivät voi olla kovin pitkiä muuten kuin kaapeloinnissa, jossa on hyvä huomioida mahdollisia muutos- ja laajennustarpeita myös hieman pidemmälle tulevaisuuteen. Aktiivilaitteiden, kuten kytkimien ja reitittimien, elinkaaressa tarkasteluväli ei saisi olla yli kolme vuotta, ja hyvä lähtökohta uusimisvälille on kaksi tarkasteluväliä eli noin 5–6 vuotta.

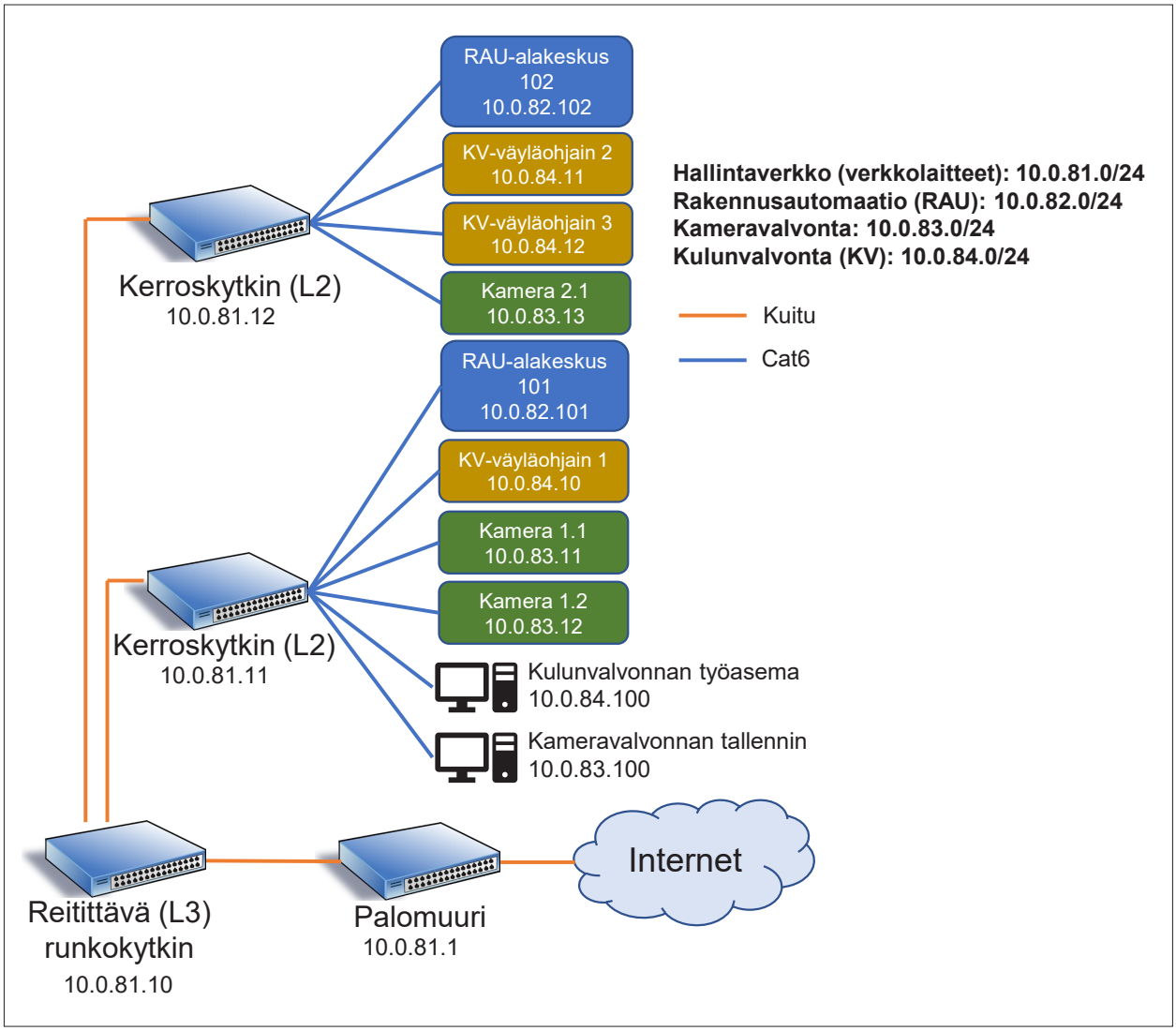
6.3.1 Verkon segmentointi, suojaaminen ja pääsynhallinta

Segmentointi eli aliverkkoihin jako on yksi laajemman verkkoympäristön suojaamisen edellyttämistä perustoiminnoista. Sillä halutaan saada aikaan toiminnallisuus, jossa tietyn ryhmän tai toiminnallisuuden sisällä tiedonvaihto tapahtuu vapaasti, mutta tiedonvaihto niiden ulkopuolelle

tai ulkopuolelta pakotetaan kulkemaan osia yhdistävän prosessin läpi. Verkon laitteet ja palvelut ryhmitellään loogisesti siten, että niille voidaan luoda omat aliverkkonsa. Tällöin eri aliverkkojenkin välistä liikennettä voidaan valvoa palomuurien (IDS/IPS, Intrusion Detection System / Intrusion Prevention System) tai vastaavien palveluiden avulla.

ESIMERKKI

Valvontakamerat muodostavat yhden tai useamman – esimerkiksi ulko- ja sisäkamerat ominaan – loogisen segmentin ja kunkin turvallisuusjärjestelmän IP-verkkoon yhteydessä olevat osat omat aliverkkonsa eli segmenttinsä. Tällöin niiden väliseen tai esimerkiksi internetin suuntaan tapahtuvaan tiedonsiirtoon voidaan kohdistaa valvontaa. Myös laitteiden hallintaverkko tulee huomioida.



Kuva 5. Esimerkki talotekniikan verkkotopologiasta. (Kuva: Sähköinfo oy)

Fyysisesti verkkoa tulee suojata kuten muitakin turvallisuusjärjestelmien osia. Kaapelireitit pitää suojata ja sabotointia valvoa, aktiivilaitteet tulee sijoittaa valvotuissa tiloissa oleviin lukittuihin kaappeihin ja estää kytkeytyminen vapaisiin liityntöihin. Myös energian saanti on varmistettava. Tiedonsiirto tulee salata ainakin sisällön osalta, ja tarpeen mukaan tulee salata myös tiedonsiirron

osapuolet eli lähde ja kohde, etenkin etäyhteyksillä. Loogisesti verkkoa suojataan vaatimalla siihen kytkeytyviä käyttäjiä ja prosesseja tunnistautumaan siten, että käyttäjät tunnistetaan kaksivaiheisesti (2FA, Dual/Two Factor Authentication). Käyttäjien oikeudet muun muassa rooliensa, kirjautumisympäristönsä ja ajankohdan mukaan tulee rajata vastaamaan turvallisuussuunnitelmassa määrättyä. Erityisesti on varmistuttava laitteiden hallintaverkon suojauksesta.

TARKISTUSLISTA | Pääsynhallinta

Tarkista, että

- tehdas- tai oletussalasanat ja muut vastaavat kirjautumistunnukset on poistettu käytöstä
- turvajärjestelmiin kirjautumisten valvonta asettaa epäonnistuneille kirjautumisyrityksille rajoitteita, esimerkiksi automaattinen lukitus tai muita toimenpiteitä
- turvajärjestelmien salasanoilla on monimutkaisuussääntöjä ja kirjautumisaikaa on rajoitettu automaattisella istunnon lopetuksella
- tiedetään, kenellä on pääsy turvajärjestelmiin, pääsy on rajoitettu ja vaatii valtuutuksen
- käytössä ovat käyttöoikeuksien hallinnan käytännöt ja menettelyt sekä auditoitavissa oleva menettely turvatekniikan järjestelmien pääsyoikeuksien hallintaan
- operaattoreiden ja ylläpitäjien käyttöoikeudet turvajärjestelmiin ovat tiedossa ja minimoitu
- turvatekniikan ylläpitäjän tunnistaminen ja todentaminen vaaditaan ennen pääsyä turvallisuusjärjestelmiin ja kirjautumisia valvotaan lokien avulla
- turvajärjestelmiä ylläpitävien pääsyoikeudet tarkastetaan säännöllisesti
- henkilön käyttöoikeudet turvajärjestelmistä poistetaan hänen lähtiessään organisaatiosta tai vaihtaessaan tehtävää.

6.3.2 Liikenteen rajoittaminen palomuureilla, verkkoliikenteen suodattaminen ja valvontatoimet

Kun verkko on segmentoitu, sen rajapintojen läpäisevää tietoliikennettä voidaan valvoa ja suodattaa vastaavalla tavalla kuin liikennettä internetin suuntaan. Segmentoinnin avulla voidaan myös tehostaa verkon toimintaa, kun esimerkiksi suuren tiedonsiirtovolyymin kameravalvonta tapahtuu muita palveluita ja kilpavarausverkon osia kuormittamatta. Vastaavasti myös laitevian tai ohjelmiston häiriintymisen aiheuttama suuri verkkoliikenne saadaan rajattua vain tiettyyn segmenttiin.

Palomuurit ovat yksi mahdollisuus suodattaa ja rajoittaa verkon liikennettä. Palomuureille annetaan säännöstö, joka sallii vain hyväksyttävän tiedonsiirron, jotta luvaton, esimerkiksi haittaohjelman synnyttämä liikenne saadaan rajoitettua vain osaan verkkoa. Säännöstöä muodostettaessa lähtökohta on, että ensin kaikki kielletään, ja vain halutunlainen liikenne sallitaan siihen luvallisten osapuolten välillä. Säännöt voivat perustua osoitteisiin, protokolliin tai esimerkiksi ajankohtaan, mutta ne ovat ennalta asetettavia ja siinä mielessä mukautumattomia. Toki sääntöjä voi vaihtaa ja lisätä tilanteen mukaan, mutta tämä vaatii omat resurssinsa. Kehittyneempään heuristiseen verkonvalvontatekniikkaan perustuvat ratkaisut (IDS) voivat tunnistaa vaikutusyritykset automaattisesti sekä laajemmin ja estää näin tunnistetun sopimattoman liikenteen (IPS).

Verkon palveluita voidaan yrittää estää kuormittamalla niitä tuottavia järjestelmiä suurella määrällä verkkoliikennettä. Tällainen palvelunestohyökkäys (DoS / DDoS, Denial-of-Service / Distributed Denial-of-Service) voidaan torjua monin keinoin huolellisen riski- ja järjestelmäanalyysin perusteella oikein laaditun vaatimusmäärittelyn tuloksena. Yksi hyvä lähtökohta on käyttää pilvipalveluna tarjottavaa, aina päällä olevaa puhdistuspalvelua, joka pyrkii poistamaan palvelunestoliikenteen mahdollistaen hyötyliikenteen.

Verkonvalvonnan tarkoitus on havainnoida hallittavassa verkossa tapahtuvia muutoksia, jotka voivat olla joko käyttäjien tai verkkovian aiheuttamia. Esimerkiksi verkon suorituskykyä tai virheitä voidaan havainnoida. Valvonnalla kerätään tietoa sekä sallitun liikenteen statistiikasta että suodatetusta liikenteestä.

TARKISTUSLISTA | Verkon valvonta

Tarkista, että
- turvajärjestelmien tietoverkoissa ja laitteissa on kyky havaita tunkeutuminen
- tiedonkulku talo- ja turvatekniikan eri osien sisällä ja välillä on valtuutettua ja valvottua
- turvajärjestelmien toiminta ja konfiguraatio tarkastetaan säännöllisesti siihen oikeutettujen toimesta
- turvajärjestelmien digitaalisen turvallisuuden valvonnan auditointeja tehdään vahvistetun, mutta satunnaisen aikataulun mukaisesti.

6.4 RAJAPINNAT MUIHIN JÄRJESTELMIIN JA INTEGRAATIO

Eri turvallisuusjärjestelmissä toiminnot ovat osin keskenään tai muun talotekniikan kanssa päällekkäisiä, joten toimintojen yhdistäminen voi tuoda etuja valvonnan tehokkuuden sekä helpomman ohjelmoitavuuden ja muutosten hallittavuuden kannalta myös järjestelmien digitaaliselle turvallisuudelle. Se, miten laajasti ja millä tasolla integraatio toteutetaan, riippuu täysin kohteesta ja vaadittavasta turvallisuustasosta sekä järjestelmiltä vaadittavista toiminnoista ja ominaisuuksista. Perussääntö on kuitenkin se, että kunkin integroidun järjestelmän pitää pystyä toimimaan myös itsenäisesti omana järjestelmänään.

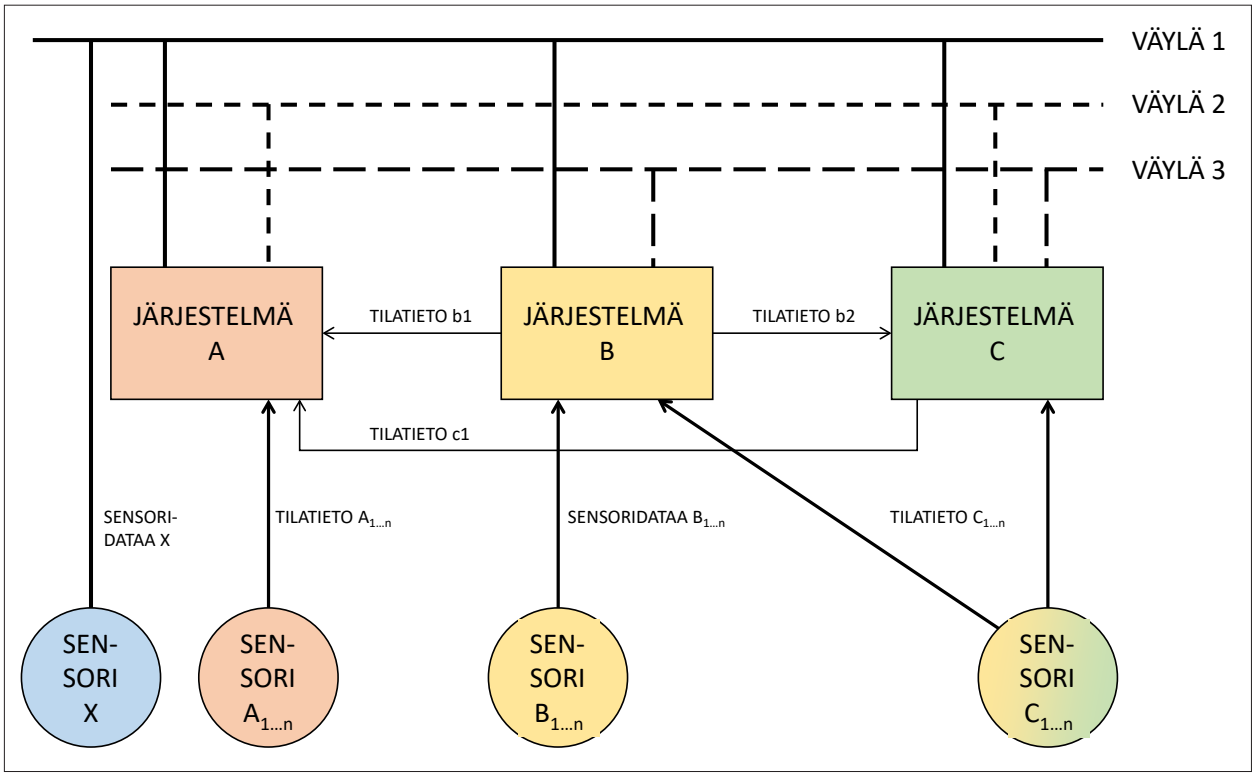
Lisätietoa on on saatavissa muun muassa seuraavista standardeista:
– SFS-EN 60839-11-3X ja SFS-EN 62676-2-3X (turvajärjestelmien viestintäprotokollat)
– SFS-EN 62820 (kiinteistöjen viestintäjärjestelmät).
– SFS-EN 50136 ja IEC 60839-5-X (ilmoituksensiirtojärjestelmät).

Turvallisuusjärjestelmien välisissä tai turvallisuusjärjestelmät muuhun talotekniikkaan yhdistävässä integraatiossa eri järjestelmien välisiä tietoja voi vaihtaa joko IP-verkon kautta, sarjaliikenneyhteyksillä tai johdinpareissa välittyvinä ON/OFF-tilatietoina (kuva 7). Kaikkiin näihin liittyy mahdollisuus virheellisen tiedon välittymisestä. Siksi ilmoitettu tila pitäisi pystyä varmistamaan jonkin toisen yhteyden tai palvelun kautta ennen kuin kohdejärjestelmä muuttaa itse tilaansa.

IP-verkon kautta tapahtuvassa tiedonvaihdossa on muita järjestelmiä syytä pitää yhtä uhkaavina kuin internetyhteyttäkin pidetään. Järjestelmien ja ulkoisten palveluiden rajapinnoissa on oltava palomuurit varmistamassa tiedonsiirron oikeellisuutta. Integraatiossa on huomioitava myös yhteensopivuus ja kääntäen häiritsemättömyys, jotta järjestelmät eivät tahattomasti vaikuta toisiinsa.

ESIMERKKI

Loogisilla varmistuksilla vältytään joko turhilta hälytyksiltä tai turvallisuusvajeilta, kun yksittäistä anturitietoa verrataan sitä ohjaavan järjestelmän tilaan. Jos esimerkiksi savunpoistoluukusta tulee aukiolotieto, se on tilaturvallisuuden valvonnan tai palontorjunnan kannalta hälytyksen arvoinen, jos samalla savunpoistojärjestelmästä ei saada tietoa luukun avauksesta tai luukun tila on ristiriidassa luukun ohjaustiedon kanssa. Savunpoistojärjestelmä on voinut saada luukun avauskäskyn myös esimerkiksi ilmanvaihtoa ohjaavalta automaatiolta kesäajan yöviilennyksen toteuttamiseksi, jolloin aukiolotieto ei saa aiheuttaa hälytystä. Varmistuksia voi lisätä esimerkiksi yhdistämällä erillisen luukun aukiolotiedon ja sitä ohjaavan toimilaitteen tilatiedon.



Kuva 6. Eri järjestelmien välisiä rajapintoja ja tiedonvaihtomenetelmiä.

TARKISTUSLISTA | Rajapinnat muihin järjestelmiin ja integraatio

Tarkista, että

- verkon kapasiteetti on riittävä
- integraatioita varten on avattu vain niin vähän oikeuksia kuin on tarpeellista
- järjestelmien rajapinnoissa on palomuurit
- kukin osajärjestelmä pystyy toimimaan myös itsenäisesti.

7 TOTEUTUS

Turvaprojektissa käsitellään runsaasti luottamuksellista tietoa sekä suunnittelu- että toteutusvaiheessa. Projektiin osallistujien tulee sitoutua noudattamaan projektin johdon määrittelemää tietoturvaohjeistusta. Sitoutuminen voidaan varmistaa kirjallisella sopimuksella, ja erikoiskohteissa luotettavuus voidaan myös tarkistaa tilan käyttäjän määrittelemällä selvityksellä. Projektin johto nimeää ne rakennuttajan tai käyttäjän edustajat, jotka saavat käsitellä turvahankkeeseen liittyviä asioita.

Hyväkään suunnittelu ei takaa hyvää lopputulosta, jos asennusten ja käyttöönoton aikana tehdään virheitä. Tavoitellut turvallisuusjärjestelmien digiturvavaatimukset voidaan saavuttaa vain, kun toteutus vastaa suunniteltua ja käyttäjät sekä operoijat on koulutettu toimimaan oikein. Suunnitelmista poikkeamista ei aina voida välttää, joten muun muassa ylläpidon tarpeita varten toteutuksen luovutusdokumentaation on vastattava toteutunutta.

7.1 ASENNUS JA KÄYTTÖÖNOTTO

Henkilöillä, jotka työskentelevät asiakkaiden tiloissa ja suorittavat hyväksymistä edellyttäviä turvasuojaustehtäviä, on oltava riittävä koulutus ja osaaminen sekä poliisin myöntämä turvasuojaajakortti. Alihankintaa käytettäessä on varmistuttava, että kaikki projektiin liittyvät henkilöt ovat tietoisia digitaalisen turvallisuuden käytännöistä ja myös toimivat niiden mukaisesti. Turvallisuusjärjestelmiin liittyvät tiedot ja dokumentaatio ovat luottamuksellista, joten niitä on käsiteltävä vain sallittuihin tarkoituksiin ja sallituilla menetelmillä.

Turvajärjestelmäasentajan ensimmäisiä tehtäviä on varmistaa suunnitteluasiakirjoissa määritellyt menettelytavat työkohteessa. Sen jälkeen menettelytapoja noudattaen perehdytään suunnitelmiin sekä esimerkiksi urakkarajojen mukaisesti edeltävien vaiheiden luovutusdokumentaatioon, jonka luotettavuus voidaan tarkastaa pistokokein. Tarvittaessa varmistutaan tulkinnanvaraisten suunnitelmien toteutustavasta tai pyydetään korjaamaan aiempien vaiheiden luovutus vastaamaan sovittua. Materiaalihankinnoista vastaavan tahon kanssa varmistetaan tilausten toimitusaikojen sopivuus työvaiheiden aikatauluihin sekä arkaluonteisen materiaalin säilytystavat työmaalla.

Turvallisuusjärjestelmien kenttälaitteiden (anturit ja sellainen niiden vaatima elektroniikka, joka ei ole suoraan kiinni IP-verkossa) ja niiden kaapelointien tarkastukselle ja käyttöönotolle on yleensä omat ohjeensa. Ennen asennusta laitteiden ohjelmistoversiot on tarkistettava ja tarvittaessa päivitettävä sekä tehtävä suunnitellut kovennukset, millä tarkoitetaan tarpeettomien ominaisuuksien ja toimintojen poistamista käytöstä.

Jos suunnittelija ei ole määrittänyt käyttöönottojärjestystä, ensin asennetaan kaikki turvallisuusjärjestelmien digiturvallisuutta valvovat ja turvaavat laitteet ja palvelut siihen verkkoon, joka ei ole yhteydessä internetiin. Palveluiden (esimerkiksi palomuurit ja verkon segmentointi) konfiguraatiot, kuten esimerkiksi käyttäjien ja käyttöoikeuksien hallinta sekä aikapalvelu, kovennukset ja toimivuus varmistetaan. Kovennuksessa muutetaan palveluiden toimintaparametrejä siten, että ne poikkeavat oletusarvoista. Näin vähennetään väärinkäytösmahdollisuuksia, helpotetaan muun muassa palomuurisäännöstön laadintaa ja ylläpitoa sekä IDS/IPS-toimintaedellytyksiä. Samoin lisätään vaikuttamispyrkimyksen edellyttämään tiedusteluun vaadittavaa ja omille toimenpiteille jäävää aikaa. Koventamiseen voi käyttää seuraavaa periaatetta: ensin kielletään kaikki, jonka jälkeen sallitaan vain se, mikä on tarpeen.

Tämän jälkeen avataan yhteys internetiin ilman, että verkossa on vielä yhtään varsinaista turvallisuusjärjestelmän laitetta tai palvelua kytkettynä. Palvelut ja laitteet liitetään vaiheittain verkkoon alkaen vähiten kriittisestä. Jokaisessa vaiheessa tarkkaillaan lokien, verkonvalvonnan yms. digiturvaa valvovan palvelun avulla, ettei mitään odottamatonta tai poikkeavaa kuormitusta tai tietoliikennettä esiinny. Kun kaikki palvelut toimivat, otetaan tarvittavat varmuuskopiot ja testataan myös niiden avulla tehtävän palautumisen toimivuus. Vaiheet dokumentoidaan ja asiakirjat sekä tallenteet liitetään mukaan osajärjestelmien ja kokonaisuuden luovutusdokumentteihin.

Tietojärjestelmän salaamisella voidaan parantaa digitaalista turvallisuutta. Siitä ei ole haittaa eikä se aiheuta riskiä palauttamiselle, jos offline-varmuuskopiota voidaan säilyttää turvallisesti ilman salausta.

7.2 KÄYTTÄJÄHALLINTA

Järjestelmien käyttäjähallinta on toteutettava suunnitelmien mukaisesti. Turvallisuusjärjestelmien tekniseen ja toiminnalliseen käyttäjähallintaan tulee nimetä vastuuhenkilöt ja määrittää heidän käyttämilleen rooleille tarvittavat käyttö- ja pääsyoikeudet. Turvallisuusjärjestelmien käyttäjähallinta on syytä liittää henkilöstöhallinnon (HR) prosesseihin. Myös alihankintana tai muuten ulkoistetun palvelun tuottajilta tulee edellyttää vastaavaa.

Käyttöoikeuksia ei yleensä hallita suoraan käyttäjäkohtaisesti, vaan käyttäjä kuuluu yhteen tai useampaan ryhmään, joille on määritetty tarvittavia oikeuksia. Käyttäjällä on siis rooli tai rooleja ja niiden mukaiset oikeudet. Käyttäjähallintaan liittyy myös käyttäjän tunnistamisen varmentaminen, jotta pelkällä käyttäjätunnuksella ei pääse kirjautumaan palveluihin. Käyttäjä varmennetaan vähintään yhdellä tavalla, yleensä salasanalla, mutta monivaiheinen tunnistus on jo laajalti käytössä. Yleensä käytetään kaksivaiheista tunnistusta (2FA, Two-Factor Authentication). Siinä toinen tunnistustapa voi olla biometrinen tai esimerkiksi erillinen tunnistusväline.

TARKISTUSLISTA | Käyttäjähallinta

Tarkista, että

- tietokalastelusta tai muusta henkilövaikuttamiseen pyrkivästä epäilyttävästä toiminnasta ilmoittamisen käytännöt ja menettelyt ovat käytössä
- henkilöstön muut turvallisuuskäytännöt ja -menettelyt ovat käytössä ja ajantasaiset, ja niihin sisältyy työlainsäädännön mukaisten työntekijän oikeuksien, sopimuksien ja velvollisuuksien huomioiminen
- henkilöstön taustat ja turvallisuustekijät tarkistetaan ennen työhön ottoa, myös turvajärjestelmiä ylläpitävien urakoitsijoiden ja kolmansien osapuolien henkilöstöltä ennen työn aloitusta
- turvallisuuteen liittyvät tarkistuskäytännöt ja -menettelyt ovat käytössä henkilön vaihtaessa tehtävää
- toimitilojen turvajärjestelmien operaattoreille ja ylläpitäjille tehdään lähtöhaastattelut
- kulunvalvonnan turvakäytännöt ja -menettelyt ovat käytössä ja ajantasaiset
- käytössä on jatkuva arviointi tehtävään soveltuvuudesta.

7.3 KOULUTUS

Turvallisuusjärjestelmää käyttävän organisaation velvollisuudet ja tehtävät digitaalisen turvallisuuden toteuttamisessa ja ylläpidossa tulee määritellä heti projektin alkuvaiheessa tarvittavan koulutuksen suunnittelemiseksi. Järjestelmän omistajaa edustavan tulevan pääkäyttäjän tulisi olla toteutuksessa mukana asennusten alusta lähtien, jotta hänellä olisi valmius suunnitella digitaalisen turvallisuuden osalta käytön prosessit, tehdä ohjeistus muille käyttäjille ja henkilöstölle sekä ottaa vastaan annettu koulutus. Sen painopiste tulee olla poikkeustilanteiden ja jatkuvuuden hallinnan käytänteissä ja niiden harjoittelussa. Myös etäkäyttäjien koulutus on huomioitava.

Turvallisuusjärjestelmien ylläpitotehtävät ulkoistetaan yleensä palveluntuottajalle. Mutta jos käyttäjäorganisaatio tekee niitä itse, on vastuussa oleville toteutettava tarpeellinen perus- ja jatkokoulutus.

TARKISTUSLISTA | Koulutus

Tarkista, että
- käytössä on dokumentoitu turvallisuustietoisuuden ja sen kouluttamisen ohjelma
- turvatekniikka on osana turvallisuustietoisuuden koulutuspakettia
- turvatekniikan digiturvakoulutuksen kokonaisuus on testattu, tulokset dokumentoidaan ja osaamisen kehitystä seurataan
- myös etäkäyttäjien koulutus on huomioitu.

7.4 DIGITURVALLISUUSPÖYTÄKIRJA

Turvaurakoitsija huolehtii urakan päätyttyä myös siitä, että kaikki toimeksiantoon liittyvät dokumentit, tallenteet sekä materiaali palautetaan tilaajalle tai tuhotaan. Turvaurakoitsija sopii erikseen tilan käyttäjän kanssa takuu- ja huoltovastuun hoitamisessa tarvittavan tiedon säilyttämisestä. Digiturvallisuuspöytäkirjaan tulee liittää tiedot eri dokumenttien käsittelijöistä, palautuksista ja tuhoamisesta.

VINKKI

Käytä digiturvallisuuspöytäkirjan tekoon lomaketta ST 730.05 Sähkö- ja tietoteknisten järjestelmien tietoturvan tarkastuspöytäkirja. Täydennä lomaketta – esimerkiksi tietosuoja-asioilla – erillisillä liitteillä.

8 KÄYTTÖ JA YLLÄPITO

Harvalla käyttäjäorganisaatiolla on itsellään talotekniikan huoltoon koulutettua erityishenkilöstöä. IT-järjestelmiäkin huoltavat yleensä ulkopuolisen palveluntuottajan henkilöt. Myös turvallisuusjärjestelmien ylläpitotehtävät voidaan ulkoistaa.

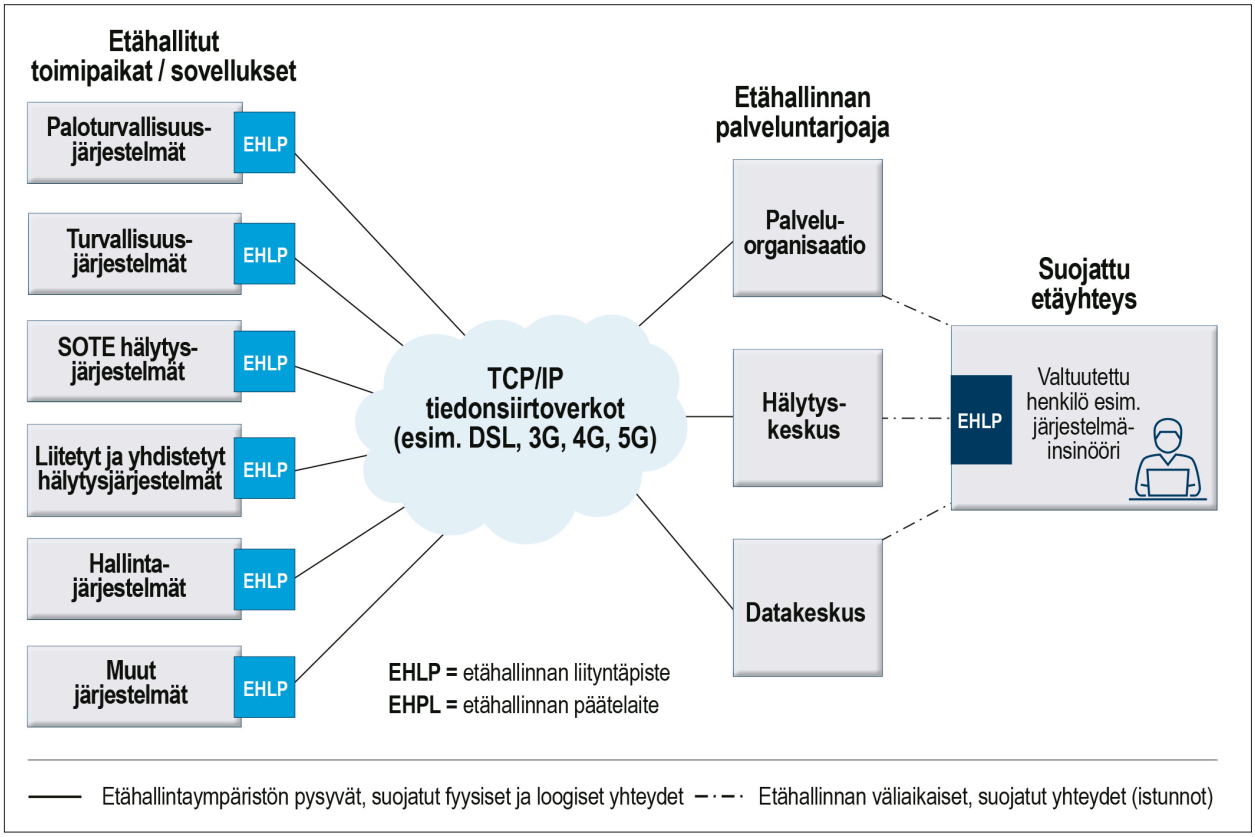
Turvallisuusjärjestelmien toimintaa valvotaan käytön aikana. Eri ilmaisimien, kuten murto- ja paloilmaisimien, toiminta testataan säännönmukaisesti, mutta myös digitaalista turvallisuutta varmentavien toimintojen, kuten varayhteyksien ja -laitteiden, testausta on syytä tehdä ja sen osana myös harjoitella toimintaa poikkeus- ja jatkuvuudenhallinnan tilanteissa.

8.1 ETÄKÄYTTÖ

Etäkäytössä palvelun tai sen osan vaatima henkilötyö tehdään jostain muusta toimipaikasta ja organisaatiosta kuin mitä itse kohde edustaa. Kyseessä voi olla turvallisuusjärjestelmien ylläpitoon tai niiden käyttöön liittyvästä palvelusta, joka toteutetaan internetyhteyden avulla.

Suunniteltaessa järjestelmän ylläpitoa tulee päättää, sallitaanko järjestelmän etäkäyttö ja jos sallitaan, mitkä ovat sallitut tekniikat ja miten varmistetaan pääsy etäkäyttöön vain niille henkilöille, joilla on siihen valtuutus. Suoria, internetiin avoimia etäkäyttöyhteyksiä ei tule käyttää, ja varayhteyksienkin on oltava suojattuja.

Myös hyvin suunniteltuun ja toteutettuun etäkäyttöön voi jäädä turvallisuuspuutteita tai -riskejä, joita paikallisessa käytössä ei ole. Yleensä riittävinä turvallisuusratkaisuina pidetään hyvin salattua, tunneloitua tiedonsiirtoa, jolla luotettavasti tunnistettu etäkäyttäjä yhdistetään internetin kautta paikallisiin palveluihin, joita yhdistävä verkko on segmentoitu ja varusteltu tarvittavalla määrällä haittaohjelmia tunnistavia ja niiden toiminnan estäviä ratkaisuja. Turvallisuusjärjestelmien etähallinnan turvallisuusvaatimuksille on julkaistu standardi SFS-EN 50710:en, jonka esiversiosta kuva 7 on. Standardi on laadittu ensisijaisesti turvallisuusjärjestelmien etähallintaa varten, ja etäkäyttö tai muu operatiivinen toiminta on poissuljettu sen piiristä. Näille on oma standardinsa SFS-EN 50518.



Kuva 7. Turvajärjestelmien etäkäyttöstandardin mukainen etähallintaympäristö.

Tunnelointiin ja salaukseen on useita ratkaisuja, joista VPN (Virtual Private Network) on yksi. VPN-toteutuksia on tarjolla moniin eri tarkoituksiin ja teknisesti eri tavoin toteutettuna. Pahimmillaan VPN tarkoittaa erittäin suurta digiturvariskiä, joten jälleen korostuu luotettavien toimijoiden valitseminen.

TARKISTUSLISTA | Etäkäyttö

Tarkista, että
- turvajärjestelmien etäkäyttöyhteys on tarpeellinen
- turvajärjestelmien langatonta etäyhteyttä käytetään vain rajoitettujen ja hallittujen liityntäpisteiden kautta
- operaattoreiden ja ylläpitäjien käyttöoikeudet turvajärjestelmiin ovat tiedossa ja minimoitu.

8.2 LOKITUS JA LOKISEURANTA

Lokituksen tarkoituksena on tallentaa tietoa järjestelmän tapahtumista, jotta toimintaa voidaan valvoa reaaliajassa tai tarkastella jälkikäteen. Lokeja kerätään useisiin eri käyttötarkoituksiin, jolloin myös lokitettavat asiat ja esimerkiksi lokituksen tiheys vaihtelevat. Lokeihin kerättävät tiedot ja pääsyoikeudet lokeihin, tietojen formaatti, säilytysaika jne. suunnitellaan siten, että tietoja voidaan analysoida joko ohjelmallisesti tai manuaalisesti.

Esimerkiksi käyttölokiin (tapahtumalokiin) kirjattavia tapahtumia ovat muun muassa käyttäjien kirjautuminen ja kirjautumisen yritykset, yhteyksien ja tiedostojen avaaminen, siirrettävän muistivälineen kytkentä. Teknisen kuormituksen lokituksella taas voidaan esimerkiksi palvelimien kuormituksen ja tiedonsiirron määrien perusteella analysoida, onko järjestelmässä häiriö tai poikkeavuus, jonka syynä on esimerkiksi haittaohjelma.

VINKKI

Kyberturvallisuuskeskus on julkaissut oppaan **Näin keräät ja käytät lokitietoja**. Se on tarkoitettu organisaatioille, joilla on omaa tietoturvaosaamista.

Tapahtumalokeihin kerättävät tapahtumatiedot voidaan analysoida joko ohjelmallisesti tai manuaalisesti, kun selvitetään mahdollisia turvallisuuspoikkeamia tai etsitään vian tai häiriön aiheuttajaa. Lokien manuaalinen seuranta voi olla vaikeaa tai ilmaisukynnys voidaan joutua asettamaan niin ylös, että poikkeustilanteeseen reagoidaan liian myöhään. Lokitietoja voi hyödyntää tehokkaasti yhdistämällä niiden tietoja jonkun soveltuvan SIEM-prosessin (Security Information and Event Management) avulla.

Ylläpitovaiheessa on ohjelmisto- ja laitepäivitysten yhteydessä huomioitava niiden vaikutukset suunniteltuun lokitukseen ja varmistuttava uusien lokien käytettävyydestä.

TARKISTUSLISTA | Lokitus ja lokiseuranta

Tarkista, että
- käytössä on kaikkien yksittäisten turvajärjestelmiä operoivien kirjautumiset tunnistettavasti tallettava loki, josta henkilöt voidaan tunnistaa ja todentaa
- kaikki turvajärjestelmien laitteisto- ja ohjelmistomuutokset sekä korjaukset voidaan tarkistaa lokeista
- turvatekniikan vika- ja/tai tunkeiluhälytyksiä seurataan reaaliaikaisesti
- pääsyä turvajärjestelmiin tiloja käyttävien yritysten verkoista seurataan
- turvatekniikkaan kohdistuneet turvallisuuspoikkeamat raportoidaan ja tutkitaan asianmukaisesti
- ohjelmistopäivityksissä huomioidaan lokien käytettävyys.

8.3 VARMUUSKOPIOINTI

Kuten lokitiedostoja, myös varmuuskopioita on useisiin eri käyttötarkoituksiin. Jotta järjestelmän toimintaa voidaan jatkaa tietoja korruptoineen tai tuhonneen tapahtuman jälkeen, on oltava toisaalta mahdollisimman tuore, mutta myös riittävän vanha varmuuskopio, jota esimerkiksi poikkeustilanteen aiheuttanut haittaohjelma ei ole saastuttanut. Puhtaan ja viimeisimmän varmuuskopion erotuksen voi usein pystyä palauttamaan, kun haittaohjelman mekanismit ovat selvinneet ja vahingon korjaavat toimenpiteet on tehty.

Varmuuskopioita on säilytettävä hajautetusti, jotta niiden fyysisen vaurioitumisen riskit voidaan minimoida. Ne tai ainakin osa varmuuskopioista on myös säilytettävä irrallaan verkosta. Varmuuskopiot, niiden säilytystapa ja -paikka, palautus sekä toimivuuden tarkastukset on suunniteltava ja toteutettava huolella siten, että alkuperäisen datan turvallisuusvaatimukset säilyvät. Salaamaton offline-varmuuskopio esimerkiksi ulkoisella kovalevyllä turvatason vaatimassa suojatussa tilassa mahdollistaa palautukset tilanteissa, joissa salatun varmuuskopion palauttaminen ei syystä tai toisesta ole mahdollista.

TARKISTUSLISTA | Varmuuskopiointi

Tarkista, että
- turvajärjestelmien pääkäyttäjien tunnukset, PIN-koodit ja tunnisteet säilytetään turvallisessa paikassa
- turvajärjestelmien ja laitteiden ohjelmistojen, asetusten ja kokoonpanotietojen tallenteet säilytetään suojatusti toimitilan ulkopuolella ja että niiden asennusta on harjoiteltu ja testattu
- ohjelmistopäivityksissä huomioidaan varmuuskopioiden käytettävyys.

8.4 OHJELMISTO- JA LAITEPÄIVITYKSET

Turvallisuusjärjestelmät vaativat aika ajoin päivittämistä, jotta toiminnallisuus ja digitaalinen turvallisuus säilyvät. Lähes kaikista järjestelmistä löydetään jatkuvasti haavoittuvuuksia, ja niitä korjaamaan järjestelmätoimittajat luovat uusia versioita ohjelmistoista, joten laitteiden ja järjestelmien päivityksen tulisi olla osa järjestelmän säännönmukaista ylläpitoa.

Tarjolla olevien ohjelmistopäivitysten luonne ja merkitys (versiokuvaus) vaikuttavat siihen, kuinka nopeasti ne on tehtävä. Jos kyse on vain tietyn toiminnallisuuden parantamisesta eikä turvallisuuteen kriittisesti vaikuttavasta tekijästä, päivityksissä on hyvä noudattaa malttia ja tehdä niitä yhteensopivuuden varmistamisen jälkeen useita samalla kertaa.

Kiinteistön toiminnan kannalta kriittisten laitteiden ja järjestelmien päivitys saattaa vaatia käyttökatkosta järjestelmän toimintaan, ja valitettavan usein on olemassa riski, että päivityksen jälkeen järjestelmä ei toimikaan enää halutulla tavalla. Ennen päivityksiä onkin perusteltua tehdä (mahdollisuuksien mukaan) integraatiotestaus ennen asennusta tuotantoympäristöön. Siinä varmistetaan, että järjestelmäkokonaisuus toimii oikein päivityksenkin jälkeen, myös lokien toiminta ja varmuuskopiot.

Päivityksien asentamiseen saatetaan tarvita toimenpiteeseen perehtynyt ammattilainen tai erillinen lisenssi, ja sen yhteydessä tulee varautua tilapäiseen lisäykseen henkilövalvonnassa, etenkin jos päivitystä edeltävää testausta ei tehdä. Päivitysten yhteydessä noudatetaan tehostettua valmiutta poikkeustilanteiden hallinnassa, ja ohjelmistopäivityksissä varaudutaan palauttamaan vähintään päivityksen kohde varmuuskopion avulla päivitystä edeltävään tilaan.

TARKISTUSLISTA | Ohjelmisto- ja laitepäivitykset

Tarkista, että
- turvajärjestelmät ovat osana toimitilan omaisuuden seurantajärjestelmää
- järjestelmissä on uusimmat ohjelmistopäivitykset
- turvajärjestelmille on korvaussuunnitelmia niiden vanhentuessa.

8.5 POIKKEUSTILANTEET JA NIISTÄ PALAUTUMINEN

Turvallisuusjärjestelmien toiminta voi häiriintyä useista syistä, ja vaikutukset voivat kohdistua myös järjestelmien digiturvallisuuteen. Poikkeustilanteet voivat edellyttää joidenkin palveluiden tai toimintojen normaalitilanteeseen verrattuna toisenlaista konfigurointia poikkeustilanteen vaikutusten estämiseksi tai minimoimiseksi. Erityistä huomiota tulee kiinnittää varateholähteiden toimivuuteen ja riittävään mitoitukseen, jotta varmistetaan järjestelmien toimivuus sähkökatkon aikana – sekä myös siitä palautuminen.

VINKKI

Kyberturvallisuuskeskus tuottaa ajankohtaista tietoa ja varoituksia tietoturvapoikkeamista ja ohjelmistohaavoittuvuuksista: **https://www.kyberturvallisuuskeskus.fi/fi**.

Tehdyistä muutoksista on pidettävä kirjaa, jotta toiminnot muistetaan myös palauttaa ennalleen poikkeustilanteen päätyttyä. Dokumentointi on tärkeää myös tehtäessä jälkikäteen arvioita toimien sopivuudesta ja päivitettäessä opitun perusteella ohjeita ja harjoittelusuunnitelmia.

Poikkeustilanteisiin voi liittyä myös teknisen valvonnan korvaaminen tilapäisesti henkilövalvonnalla. Tämänkin on oltava etukäteen suunniteltua ja huomioitu henkilöstön ohjeistuksessa sekä palvelusopimuksissa.

Poikkeustilanteet voivat johtaa myös vakavampaan, jatkuvuuden hallintaa edellyttävään tilanteeseen, jossa esimerkiksi laitteiden ja järjestelmien ohjelmistot on asennettava ja otettava käyttöön uudestaan. Tilanteeseen voi varautua pitämällä varastossa järjestelmän kriittisimpien komponenttien varalaitteita, mutta muuten palauttamisen pitää onnistua varmuuskopioilta, jotka sisältävät esimerkiksi konfiguraatiotiedot ja käyttäjähallintaan tarvittavat tiedot. Palauttamisen on oltava suunnitelmallista ja sen on edettävä oikeassa järjestyksessä, jotta poikkeustilanne ei pitkity tai pahene.

TARKISTUSLISTA | Poikkeustilanteet ja niistä palautuminen

Tarkista, että
- turvajärjestelmät on varustettu katkottomalla jännitesyötöllä ja ne pystyvät ylläpitämään vähintään hätätilan digiturvatoimintoja kaikissa poikkeustilanteissa
- poikkeustilanteen jälkeen tehdään tilanteen purku ja analyysi
- toimitilan turvatekniikka huomioidaan sitä käyttävän toimijan jatkuvuuden hallinnan suunnitelmissa ja poikkeustilanteiden hallinnan harjoituksien strategioissa
- poikkeustilanteiden ja jatkuvuuden hallinnan suunnitelmat testataan sovituin aikatauluin järjestettävillä työpöytäharjoituksilla ja käytännön harjoituksilla.

8.6 RIKKOONTUNEEN LAITTEEN TOIMITTAMINEN HUOLTOON

Laitehuollossa ja siihen liittyvässä logistiikassa on noudatettava tiedon luottamuksellisuuden mukaisia menettelyjä. Mikäli laitteen korjausta ei voida tehdä luottamuksellisuuden vaatimalla tavalla, laitetta ei korjata.

Järjestelmistä talletetaan kiinteistön tallennusalustaan laitteiden korjausohjeet ja niiden korjaustoimenpiteet. Ohjeissa on huomioitava digitaalinen turvallisuus ja tietosuoja. Korjaukset tehdään ohjeiden mukaisesti.

8.7 TIETOJEN LUOVUTTAMINEN

Turvallisuusjärjestelmistä luovutetaan tietoja pääsääntöisesti vain tietosuojaselosteessa ilmoitettuihin tarkoituksiin ja tahoille. Viranomaisten tietopyynnöt käsitellään niiden edellyttämällä tavalla. Kaikki tietojen luovutukset dokumentoidaan asianmukaisesti.

9 PURKU JA POISTO

Turvallisuusjärjestelmissä käytetään ja niissä säilytetään luottamuksellista tietoa, joten laitteiden tai niiden tallennuskomponenttien käytön päättyessä niiden sisältämät tiedot on tuhottava. Myös muille kuin sähköisille medioille tallennetut turvallisuusjärjestelmien dokumentit on tuhottava vaatimusten mukaisesti.

Tietoja sisältäviä komponentteja ovat massamuistit, varmuuskopioissa käytettävät nauhat ja useisiin eri tarkoituksiin käytettävät flash-muistit sekä laitteiden kiinteät muistit. Jos käytössä on räätälöity, sulautettu ohjelmisto, kuten esimerkiksi käyttöliittymä, senkin sisältämät tiedot voivat olla luottamuksellisia.

Massamuistit, emolevyt, puolijohdemuistit ja nauhat voidaan hävittää varmimmin kaikista järjestelmän osista murskaamalla ne riittävän pieneksi silpuksi tai kuumentamalla niitä riittävästi muistiominaisuuden poistamiseksi. Hävittäminen on dokumentoitava ja dokumentti varmennettava kahden henkilön allekirjoituksin. Vaaditut jaekoot on määritetty standardissa DIN 66399.

TARKISTUSLISTA | Purku ja poisto
Tarkista, että • tehdään purkusuunnitelma, valitaan toteuttaja ja toteutusta valvotaan • valitaan oikeat poistotavat ja jätelajit • myös tiedot poistetaan • tuhoamista tai loppusijoitusta valvotaan.

10 JÄRJESTELMÄKOHTAISIA OHJEITA

Tässä luvussa on esitetty järjestelmäkohtaisia digitaaliseen turvallisuuteen liittyviä ohjeita.

Sähkölukitusjärjestelmä

Kiinteistön sähkölukitusjärjestelmällä tehdään mahdolliseksi ohjata ja etähallita ovien lukitusta sekä valvoa ovien asentotiloja (kiinni/auki). Ovien ja niissä olevien lukituslaitteiden ohjaus ja valvonta tapahtuu muiden järjestelmien, kuten kulunvalvonta-, murtoilmaisu- ja rakennusautomaatiojärjestelmän, avulla.

Sähköisen oviympäristön lukitus- ja tunnistusratkaisut ovat osa turvatekniikkaa ja toimitilaturvallisuuden kokonaisjärjestelyjä. Oviympäristöt ja niiden pääsynhallinta vaikuttavat turvatekniikoista eniten ihmisten jokapäiväiseen toimintaan työpaikoilla. Turvajärjestelyjen tehokkuuteen vaikuttavat puolestaan eniten työpaikan ihmiset.

Oviympäristön kaapelointi ja elektroniikka on yksi digitaalisen vaikuttamisen mahdollisuuden paikka. Kytkennät tehdään ovirasiassa, ja runkokaapeli yhdistää oviympäristön järjestelmään. Ovirasian on syytä olla oven valvotulla puolella, ja suojaamattomalle puolelle asennettaessa se pitää varustaa vähintään kansikoskettimella. Kaapeloinnissa on käytettävä suojattuja kaapeleita.

Ovirasia voi korvaantua elektroniikkaa sisältävällä ovipäätteellä. Ovipäätteet sijoitetaan joko oviympäristöön tai ne keskitetään yhteiseen lukittuun laitetilaan. Keskitetty sijoitus on huollon kannalta parempi ratkaisu kuin oviympäristöön asentaminen. Ovirasia ja ovipääte pitää kiinnittää aina rakenteisiin.

Mikäli oviympäristö on suunniteltu toteutettavaksi langattomasti, asentaminen yksinkertaistuu, mutta langattomuuden myötä tulevat uhat on hallittava ja esimerkiksi paristojen vaihtovälin pituuden tulee perustua palveluntuottajan tai valmistajan ohjeisiin. Langattoman lukko-ohjaimen yhteydessä ei käytetä ovirasiaa, koska runkokaapelia ei ovelle tarvita. Keskittimet, yhdyskäytävät tai muut vastaavat langattoman oviympäristön tietoliikennelaitteet asennetaan valmistajan ohjeiden mukaisesti kattoon tai seinään huomioiden määräys 65 kiinteistön sisäverkoista ja teleurakoinnista.

Sekä langallinen (RS-232/485, TCP/IP jne.) että langaton (RFID, NFC, Bluetooth, WLAN jne.) tiedonsiirto tulee salata ja sen osapuolet tunnistaa luotettavasti. Häirinnänsietoa voi parantaa sijoittamalla todennäköisiin vaikutussuuntiin käytettävää radiotaajuutta vaimentavia rakenteita ja tehostamalla ohjelmiston mahdollisuuksia eliminoida häirinnän vaikutus.

Poikkeustilanteissa on varmistettava rakennuksesta ulospääsy sekä tarvittaessa valvottava sisäänpääsy. Poistumisen ja esimerkiksi avaimilla sisäänkulun voi valvoa rakennuksen ulkopuolella olevan vyöhykkeen henkilövalvonnalla. Tarvittaessa myös rakennuksen sisällä käytetään henkilövalvontaa. Tällaisia tilanteita varten on oltava selkeät ohjeet ja harjoiteltu viestintä.

Huomioi ainakin nämä:
- lukitustuotteet testattuja ja hyväksyttyjä
- keskuslaitteet lukitussa ja valvotussa tilassa, päätelaitteet näkymättömissä oven suojatulla puolella
- tiedonsiirron salaus
- tuotteiden automaattiset ohjelmistopäivitykset
- ylläpito-ohjelmiston kaksivaiheinen tunnistus
- henkilötietojen käsittely ja muu GDPR:n mukainen toiminta käytössä ja ylläpidossa
- elinkeinolupa ja turvasuojaajakortti asennuksessa ja ylläpidossa.

Kulunvalvontajärjestelmä

Kulunvalvontajärjestelmän avulla hallitaan rakennuksessa kulkemista, ovien yms. aukkojen aukioloa sekä lukitusta. Se on yksi yrityksen turvatekniikan peruspilareista ja siksi myös kiinnostava kohde digitaaliselle vaikuttamiselle.

Keskusyksikkö, joko paikallinen tai vaikkapa pilvessä tuotettava SaaS, hallitsee koko järjestelmän toimintaa kuten kulkuoikeuksia, henkilörekisteriä, raportointia, lukkojen ohjauksia jne. Myös alakeskukset ja useimmat päätelaitteet ovat prosessointikykyä omaavia, joten digitaalisesta turvallisuudesta huolehtimisen on ulotuttava myös niihin.

Kulunvalvontajärjestelmän digitaaliseen turvallisuuteen voidaan vaikuttaa sekä fyysisin että ohjelmallisin suojauksin. Fyysisiä suojauksia ovat esimerkiksi lukitukset ja tilojen rakenteet, kuten ovet ja ikkunat. Ohjelmallisia suojauksia ovat esimerkiksi käyttäjäoikeudet. Merkittävä riski kulunvalvontajärjestelmissä voi myös olla on työasemien sijainti. Esimerkiksi toimistorakennusten aulapalvelupiste on usein julkisessa tilassa, jolloin työaseman suojaukseen tulee kiinnittää erityistä huomiota.

Huomioi ainakin nämä:
- palvelimet lukitusten takana
- mahdolliset muut suojaukset, kuten kamerat ja kuorihälytykset
- kytkennät näkymättömiin oven suojatulle puolelle, kun mahdollista, esimerkiksi alakaton yläpuolelle
- lukijat ja tunnisteet: nykyaikainen ja salattu lukutekniikka
- tietoliikenne- ja sähkökatkon turvatila ja turvasuunnat
- käyttöoikeusrajoitukset suojaustasojen mukaisesti
- henkilötietojen käsittely ja muu GDPR:n mukainen toiminta käytössä ja ylläpidossa
- elinkeinolupa ja turvasuojaajakortti asennuksessa ja ylläpidossa.

Murtoilmaisujärjestelmä

Murtoilmaisujärjestelmä on turvallisuusjärjestelmä, jonka avulla kiinteistön tonttialueella ja rakennusten sisätiloissa tapahtuva luvaton tunkeutuminen ja tiloissa liikkuminen voidaan havaita ja välittää tieto sovittuun paikkaan, esim. vartiointiliikkeen hälytyskeskukseen tarvittavan turvallisuushenkilöstön hälyttämiseksi paikalle. Murtoilmaisujärjestelmästä käytetään myös nimityksiä murtohälytysjärjestelmä ja rikosilmoitinjärjestelmä.

Murtoilmoitusjärjestelmä koostuu keskusyksiköstä ohjelmistoineen ja tietoliikenneyhteyksineen sekä siihen liittyvistä ilmaisimista (ulkoalueet, sisätilat, lämpö, savu, kaasut, kosteus jne.). Valvonta voidaan ohittaa hallitusti esimerkiksi avaimella, koodilla tai biometrisellä tunnistuksella toimivilla ohisulkijoilla. Murtoilmaisujärjestelmä toimii usein hälytysten välittäjänä integroituna osaksi muuta talotekniikkaa. Ja kuten kulunvalvonnassakin, luvaton pääsy murtoilmaisujärjestelmään antaa tunkeutujille mahdollisuuden poistaa järjestelmä aktiivitilasta ja täten pienentää merkittävästi kiinnijäämisriskiä murtovarkauksissa.

Murtoilmaisujärjestelmän tuottamat ilmoitukset siirretään lähes poikkeuksetta valvotulla ilmoituksensiirtopalveluntarjoajan siirtoverkolla tai langattomasti valvottavan kiinteistön ulkopuolelle, vartiointiliikkeeseen, yrityksen omaan valvomoon tai korkean turvallisuustason omaavissa kohteissa poliisille.

Huomioi ainakin nämä:
- oletuskäyttäjätunnukset ja -salasanat pois käytöstä
- elinkeinolupa ja turvasuojaajakortti asennuksessa ja ylläpidossa.

Kameravalvontajärjestelmä

Kameravalvontajärjestelmä on valvottavan kohteen kuvaamiseen sekä tapahtumien valvontaan ja tallentamiseen perustuva turvallisuusjärjestelmä, jota voidaan hyödyntää myös kaupallisiin tarkoituksiin, kuten liiketoiminnan kehittämiseen ja tehostamiseen esimerkiksi hyödyntämällä kameroiden tuottamaa dataa asiakasvirtojen hallinnassa.

Kameravalvontajärjestelmä koostuu erilaisista kamera-, tallennus- ja tarkkailulaitteista ja niihin liitetyistä ohjelmistoista sekä verkostosta, jota tarvitaan siirto- ja ohjaustarkoituksiin. Käyttö- ja hallintalaitteet voivat olla joko paikallisia, tai ne voivat olla pilvipalveluna tuotettua etäpalvelua.

Kameravalvonta on houkutteleva kohde digitaaliselle vaikuttamiselle ja laitteiden kaappaamiselle muuhun käyttöön. Myös järjestelmän tuottama informaatio voi olla tärkeä tekijä suunniteltaessa esimerkiksi murtoa, mutta sitä voi hyödyntää myös muihin rikollisiin tarkoituksiin, kuten yritysvakoiluun. Kameravalvontajärjestelmän käytössä on huomioitava myös yksityisyyden suoja ja tietosuoja.

Huomioi ainakin nämä:
- luotettava valmistaja ja tunnettu toimittaja
- tiedon salaus: kamerat, tallentimet, kytkimet, palvelimet ja työasemat
- laitteiden turvallisuus: tunnistaminen ja varmennukset
- oletuskäyttäjätunnukset ja -salasanat pois käytöstä
- kytkennät näkymättömiin, esimerkiksi alakaton yläpuolelle
- laitetuki ja päivitykset
- lainsäädäntö, kuten rikoslaki, laki yksityisyyden suojasta työelämässä ja EU:n yleinen tietosuoja-asetus (GDPR).

Henkilöturvajärjestelmä

Henkilöturvajärjestelmän avulla voidaan hälyttää apua esimerkiksi työtapaturman sattuessa tai väkivallan uhatessa ja näin parantaa yksin tai muuten riskialttiissa oloissa työskentelevien henkilöiden turvallisuutta. Henkilöturvajärjestelmästä käytetään myös nimityksiä hätäkutsu- tai päällekarkaushälytysjärjestelmä.

Järjestelmä on hyvä toteuttaa siten, että se toimii asiakkaan sisäverkossa, jolloin se on jo yhden turvaverkon alla, esimerkiksi APN-palvelulla (Access Point Name), joka on matkapuhelinoperaattorin toteuttama yrityskohtainen ratkaisu mobiililaitteiden ja yritysverkon välille. Järjestelmän fyysinen suojaus tulee suunnitella siten, että keskuslaitteet sijoitetaan lukittuihin ja mahdollisuuksien mukaan kulunvalvottuihin laite- ja teletiloihin. Jos henkilöturvajärjestelmän paikannustietoja tallennetaan ja ne sisältävät henkilötietoja, joista henkilö on suoraan tai epäsuorasti tunnistettavissa, syntyy henkilörekisteri, jonka käsittelyssä tulee noudattaa tietosuojalakia ja -asetusta.

Huomioi ainakin nämä:
- sisäverkon käyttö
- keskuslaitteet lukittuihin ja valvottuihin tiloihin
- kaikki käytettävät protokollat salataan
- henkilötietojen käsittely ja GDPR.

Paikannusjärjestelmä

Paikannusjärjestelmää käytetään henkilöiden, kulkuneuvojen, laitteiden tai tavaroiden sijaintitiedon määrittämiseen. Tämä on toteutettavissa useilla erilaisilla paikannustekniikoilla.

Paikannusjärjestelmä ei saa heikentää digiturvallisuutta ollessaan osana esimerkiksi langatonta lähiverkkoa. Laitteiden fyysisestä turvallisuudesta sekä pääsynhallinnasta tulee huolehtia, ja keskuslaitteiden sekä palvelimien tulee sijaita valvotuissa laite- tai muissa vastaavissa tiloissa. Lisäksi tulee huomioida mahdollisten pilvipalveluiden digitaalinen turvallisuus.

Henkilöpaikannuksen käyttöönotosta on huolehdittava YT-menettelyin. Mikäli paikannuksen yhteydessä tallennetaan henkilötietoja ja jos henkilö on suoraan tai epäsuorasti tunnistettavissa tallenteista, syntyy tietosuoja-asetuksen mukainen henkilörekisteri. Rekisterinpitäjän on tällöin laadittava henkilörekisteristä tietosuojaseloste, jonka tulee olla rekisteröitävien saatavilla. Myös säännökset tietojen suojaamis- ja hävittämisvelvollisuudesta on huomioitava.

Huomioi ainakin nämä:
- YT-menettely henkilöpaikannuksen käyttöönotossa
- keskuslaitteet lukittuihin ja valvottuihin tiloihin
- salaukset ja käyttöoikeudet
- henkilötietojen käsittely ja GDPR.

Paloilmoitinjärjestelmä

Paloilmoitin antaa automaattisesti ilmoituksen alkavasta palosta ja laitteiston toimintavalmiutta vaarantavista vioista sekä paikallisesti että hätä-, hälytys- tai palvelukeskukseen tai valvomoon. **Automaattisen paloilmoittimen** ilmoituksensiirto paloilmaisusta tapahtuu hätäkeskukseen ja muihin edellä mainittuihin paikkoihin, mutta vikailmoitukset siirretään vain hälytys- tai palvelukeskukseen tai valvomoon. Kummankin laitteisto on toteutettu SFS-EN 54 -standardisarjan mukaisesti sertifioiduista komponenteista.

Paloilmoitin muodostuu ilmoitinkeskuksista, teholähteistä, paloilmaisimista, paloilmoituspainikkeista, hälyttimistä ja ilmoituksensiirtojärjestelmästä tai paikallisesta valvontajärjestelmästä. Paloilmoittimeen voi liittyä palonrajoitus- ja sammutuslaitteistoihin sekä savunhallintaan liittyviä ohjauksia ja pelastustöitä helpottavien laitteiden toimintailmoituksia ja/tai henkilöturvallisuutta ja palonilmaisua palvelevien laitteistojen ohjaustoimintoja.

Vanhoissa paloilmoitinjärjestelmissä ei yleensä ole liityntää kiinteistön digitaaliseen toimintaympäristöön. Uudet järjestelmät voivat olla osa laajasti verkottunutta kiinteistön talo- ja turvatekniikan toimintaympäristöä.

Huomioi ainakin nämä:
- paloilmoittimen hoitaja varahenkilöineen on nimetty ja koulutettu
- kunnossapito-ohjelma on laadittu
- akusto on mitoitettu toteutuskohtaisesti ja oikein
- ilmoituksensiirtoyhteys hätäkeskukseen on jatkuvasti valvottu ja käytettävissä
- asennus- ja huoltotöitä tekevät paloilmoitinliikkeet täyttävät Turvallisuus- ja kemikaaliviraston (Tukes) vaatimukset.

Palovaroitinjärjestelmä

Palovaroitinjärjestelmä ei ole sama kuin paloilmoitinjärjestelmä. Palovaroitinjärjestelmä koostuu keskusyksiköstä sekä siihen yhdistetyistä palovaroittimista tai palovaroitinryhmistä. Järjestelmän palovaroittimet ja keskus hälyttävät paikallisesti. Lisäksi keskusyksikkö voi välittää hälytyksen esimerkiksi hälytysvalvomoon. **Hälytystä ei kuitenkaan saa liittää hätäkeskukseen.** Järjestelmän suunnittelusta, asentamisesta ja tarkastamisesta ei ole säädöksiä.

Savunhallinnan ohjaus- ja valvontajärjestelmä

Sammutus- ja pelastustoiminnan tehostamiseksi rakennukseen on tarpeen mukaan suunniteltava ja rakennettava sen eri tiloihin soveltuva mahdollisuus savunpoistoon. Savunpoiston suunnitteluperusteet määrittää palotekninen suunnittelija. Savunhallintajärjestelmää saa käyttää myös muihin tarkoituksiin, kuten ilmanvaihtoon.

Savunhallinnan ohjausjärjestelmä voi olla kytkettynä kiinteistön verkotettuun ohjausjärjestelmään, jolloin osana ilmanvaihtoa voidaan savunpoistoa käyttää esim. kesällä yöajan viilennykseen, joka puolestaan on otettava huomioon mm. murtoilmaisujärjestelmässä. Kuitenkaan nämä kytkennät tai niiden vika eivät saa palotilanteessa vaikuttaa savunhallinnan ohjausjärjestelmään.

Poistumishälytys- ja turvakuulutusjärjestelmä

Poistumishälytys- ja turvakuulutusjärjestelmien ensisijaisena tehtävänä on ohjata ja varoittaa kiinteistössä tai sen ulkotiloissa olevia henkilöitä ja henkilökuntaa niin, että ihmisten ohjaaminen voidaan hoitaa järjestelmällisesti ennalta laadittujen suunnitelmien ja ohjeiden mukaisesti.

Poistumishälytys- ja turvakuulutusjärjestelmä voi olla osa kiinteistön verkottunutta talotekniikkaa. Liityntä paloilmoittimeen voidaan toteuttaa käyttäen potentiaalivapaita kärkiohjauksia tai dataväylän kautta tapahtuvaa, valvottua ohjausprotokollaa, mikäli se on sertifioitu. Järjestelmä voi toimia paloilmoitinjärjestelmän täydentävänä osana (käyttöluokka 3) tai palohälyttimet korvaavana osana (käyttöluokka 4). Lisäksi poistumishälytys- ja turvakuulutusjärjestelmä voi toimia itsenäisenä

turvajärjestelmänä hätätilanteissa, muttei tulipalon sattuessa (käyttöluokka 2). Näiden lisäksi sitä voidaan käyttää yleisäänentoistojärjestelmänä (käyttöluokka 1).

Kun rakennukseen asennetaan paloilmoittimen ohjaama poistumishälytys- ja turvakuulutusjärjestelmä, paloilmoitinliike vastaa laitekokonaisuuden toteutuksesta. Järjestelmän voi asentaa äänentoistoalan yritys, mutta kokonaisuuden toiminnasta ja dokumentoinnista vastaa paloilmoitinliike.

Huomioi ainakin nämä:
- on käytetty paloilmoittimen suunnitteluperusteita
- on huolehdittu siitä, ettei mikään vika poistumishälytys- ja turvakuulutusjärjestelmässä estä paloilmoittimen toimintaa.

LIITE: TARKISTUSLISTAT

Tähän on koottu aiemmissa luvuissa esitetyt tarkistuslistat aihealueittain.

Turvallisuusjärjestelmien hallinta

- yrityksen toimitilojen turvajärjestelmien asiat on nimetty tietyn henkilön tehtäviin kuuluviksi
- turvajärjestelmille on nimetty elinkaaren eri vaiheissa vastuuhenkilö
- on olemassa kirjallinen ja hyväksytty turvallisuuskäytäntö, joka kattaa myös turvajärjestelmät
- käytössä on kirjoitettu ja hyväksytty turvallisuusohje tai turvallisuuden suunnitteluperusteet, jotka määrittävät turvatekniikan digitaalisen turvallisuuden tasot.

Turvallisuustaso uhka-arvion perusteella

- rakennushankkeen asiakirjoille tehdään luottamuksellisuusluokittelu
- käytössä on turvajärjestelmän digitaaliseen turvallisuuteen kohdistuva uhka-arvio
- toimitilojen turvatekniikka on huomioitu riskienhallintamenettelyssä riittävän yksityiskohtaisesti
- toimitilojen kriittisyysluokat tunnetaan ja haavoittuvuudet on kartoitettu
- turvatekniikan toiminnot on sijoitettu riskiarvion edellyttämälle turvallisuusvyöhykkeelle
- turvajärjestelmien data säilytetään EU:n alueella ja sen käsittelyssä noudatetaan tietosuojasta annettuja lakeja ja asetuksia
- kaikki toimitilan turvajärjestelmiin liittyvät tehtävät ovat tiedossa ja niihin liittyvät riskiarviot on tehty
- järjestelmäkohtaiset kunnossapito-ohjelmat on laadittu.

Palvelusopimukset

- toimitilojen turvajärjestelmien ylläpitäjät mukaan lukien urakoitsijat ja kolmannet osapuolet on tarkistettu ja valtuutettu tehtäviinsä
- turvajärjestelmien ulkoistetut ylläpitäjät toimivat valvotusti
- ylläpidon reagointi- ja palautumisajat turvajärjestelmien häiriöihin on määritetty.

Laitevalinnat

- käytetään luotettavia laitevalmistajia
- laitevalmistajilla on dokumentoitua näyttöä laitteiden ja järjestelmien turvallisuudesta.

Kaapelointi ja laitesuojaus

- turvallisuusstrategia huomioi turvajärjestelmien fyysisen suojaamisen
- turvatekniikan kaapelien ja verkkojen fyysisessä suojauksessa noudatetaan rakennusten sisäverkoista annettuja määräyksiä esimerkiksi lukituksessa
- fyysistä pääsyä kaikkiin turvatekniikan järjestelmiin ja niiden laitteistoihin ja ohjelmistoihin hallitaan ja valvotaan
- turvatekniikan ohjaimet, reitittimet ja verkkokytkimet on fyysisesti suojattu
- turvatekniikan verkkolaitteet ja ohjaimet on sijoitettu valvottuihin tai kahdella toisistaan riippumattomalla tavalla valvottuihin tiloihin
- turvatekniikan laite- ja kytkentäkotelot ovat turvallisella ja suojatulla alueella / lukittu
- käytössä on turvatekniikan vaatimien tilojen fyysisten avainten hallinnan käytännöt ja menettelyt mukaan lukien palauttamisen valvonta
- turvatekniikan laitteissa on ilmaisu niiden peukaloinnille / kotelot ovat tunkeutumisen kestäviä / koteloissa on ilmaisu luvattomalle tunkeutumiselle / säilytys on toteutettu siten, että niitä ei voi siirtää tiloista pois
- toimitilojen turvatekniikan tietoliikennekaapelit on suojattu
- turvajärjestelmien kenttätason laitteet on yhdistetty sabotaasin ilmaisevia kaapeleita käyttäen
- kaapelien valvonta ilmaisee häiriön ja laitteiden peukaloinnin myös laitteen ollessa poissa käytöstä
- fyysinen suojaus tarjoaa todisteita turvatekniikan järjestelmien ja laitteiden luvattomasta käytöstä, peukaloinnista tai niiden yrityksestä.

Salaus

– turvatekniikan kenttätason yhteydet on toteutettu kaksisuuntaisesti pollaavasti ja vähintään 128-bittisellä AES-avaimella (Advanced Encryption Standard) salatusti.

Pääsynhallinta

– tehdas- tai oletussalasanat ja muut vastaavat kirjautumistunnukset on poistettu käytöstä
– turvajärjestelmiin kirjautumisten valvonta asettaa epäonnistuneille kirjautumisyrityksille rajoitteita, esimerkiksi automaattinen lukitus tai muita toimenpiteitä
– turvajärjestelmien salasanoilla on monimutkaisuussääntöjä ja kirjautumisaikaa on rajoitettu automaattisella istunnon lopetuksella
– tiedetään, kenellä on pääsy turvajärjestelmiin, pääsy on rajoitettu ja vaatii valtuutuksen
– käytössä ovat käyttöoikeuksien hallinnan käytännöt ja menettelyt sekä auditoitavissa oleva menettely turvatekniikan järjestelmien pääsyoikeuksien hallintaan
– operaattoreiden ja ylläpitäjien käyttöoikeudet turvajärjestelmiin ovat tiedossa ja minimoitu
– turvatekniikan ylläpitäjän tunnistaminen ja todentaminen vaaditaan ennen pääsyä turvallisuusjärjestelmiin ja kirjautumisia valvotaan lokien avulla
– turvajärjestelmiä ylläpitävien pääsyoikeudet tarkastetaan säännöllisesti
– henkilön käyttöoikeudet turvajärjestelmistä poistetaan hänen lähtiessään organisaatiosta tai vaihtaessaan tehtävää.

Verkon valvonta

– turvajärjestelmien tietoverkoissa ja laitteissa on kyky havaita tunkeutuminen
– tiedonkulku talo- ja turvatekniikan eri osien sisällä ja välillä on valtuutettua ja valvottua
– turvajärjestelmien toiminta ja konfiguraatio tarkastetaan säännöllisesti siihen oikeutettujen toimesta
– turvajärjestelmien digitaalisen turvallisuuden valvonnan auditointeja tehdään vahvistetun, mutta satunnaisen aikataulun mukaisesti.

Rajapinnat muihin järjestelmiin ja integraatio

– verkon kapasiteetti on riittävä
– integraatioita varten avattu vain niin vähän oikeuksia kuin on tarpeellista
– järjestelmien rajapinnoissa on palomuurit
– kukin osajärjestelmä pystyy toimimaan myös itsenäisesti.

Käyttäjähallinta

– tietokalastelusta tai muusta henkilövaikuttamiseen pyrkivästä epäilyttävästä toiminnasta ilmoittamisen käytännöt ja menettelyt ovat käytössä
– henkilöstön muut turvallisuuskäytännöt ja -menettelyt ovat käytössä ja ajantasaiset, ja niihin sisältyy työlainsäädännön mukaisten työntekijän oikeuksien, sopimuksien ja velvollisuuksien huomioiminen
– henkilöstön taustat ja turvallisuustekijät tarkistetaan ennen työhön ottoa, myös turvajärjestelmiä ylläpitävien urakoitsijoiden ja kolmansien osapuolien henkilöstöltä ennen työn aloitusta
– turvallisuuteen liittyvät tarkistuskäytännöt ja -menettelyt ovat käytössä henkilön vaihtaessa tehtävää
– toimitilojen turvajärjestelmien operaattoreille ja ylläpitäjille tehdään lähtöhaastattelut
– kulunvalvonnan turvakäytännöt ja -menettelyt ovat käytössä ja ajantasaiset
– käytössä on jatkuva arviointi tehtävään soveltuvuudesta.

Koulutus

– käytössä on dokumentoitu turvallisuustietoisuuden ja sen kouluttamisen ohjelma
– turvatekniikka on osana turvallisuustietoisuuden koulutuspakettia
– turvatekniikan digiturvakoulutuksen kokonaisuus on testattu, tulokset dokumentoidaan ja osaamisen kehitystä seurataan
– myös etäkäyttäjien koulutus on huomioitu.

Etäkäyttö

- turvajärjestelmien etäkäyttöyhteys on tarpeellinen
- turvajärjestelmien langatonta etäyhteyttä käytetään vain rajoitettujen ja hallittujen liityntäpisteiden kautta
- operaattoreiden ja ylläpitäjien käyttöoikeudet turvajärjestelmiin ovat tiedossa ja minimoitu.

Lokitus ja lokiseuranta

- käytössä on kaikkien yksittäisten turvajärjestelmiä operoivien kirjautumiset tunnistettavasti tallettava loki, josta henkilöt voidaan tunnistaa ja todentaa
- kaikki turvajärjestelmien laitteisto- ja ohjelmistomuutokset sekä korjaukset voidaan tarkistaa lokeista
- turvatekniikan vika- ja/tai tunkeiluhälytyksiä seurataan reaaliaikaisesti
- pääsyä turvajärjestelmiin tiloja käyttävien yritysten verkoista seurataan
- turvatekniikkaan kohdistuneet turvallisuuspoikkeamat raportoidaan ja tutkitaan asianmukaisesti
- ohjelmistopäivityksissä huomioidaan lokien käytettävyys.

Varmuuskopiointi

- turvajärjestelmien pääkäyttäjien tunnukset, PIN-koodit ja tunnisteet säilytetään turvallisessa paikassa
- turvajärjestelmien ja laitteiden ohjelmistojen, asetusten ja kokoonpanotietojen tallenteet säilytetään suojatusti toimitilan ulkopuolella ja niiden asennusta on harjoiteltu ja testattu
- ohjelmistopäivityksissä huomioidaan varmuuskopioiden käytettävyys.

Ohjelmisto- ja laitepäivitykset

- turvajärjestelmät ovat osana toimitilan omaisuuden seurantajärjestelmää
- järjestelmissä on uusimmat ohjelmistopäivitykset
- turvajärjestelmille on korvaussuunnitelmia niiden vanhentuessa.

Poikkeustilanteet ja niistä palautuminen

- turvajärjestelmät on varustettu katkottomalla jännitesyötöllä ja ne pystyvät ylläpitämään vähintään hätätilan digiturvatoimintoja kaikissa poikkeustilanteissa
- poikkeustilanteen jälkeen tehdään tilanteen purku ja analyysi
- toimitilan turvatekniikka huomioidaan sitä käyttävän toimijan jatkuvuuden hallinnan suunnitelmissa ja poikkeustilanteiden hallinnan harjoituksien strategioissa
- poikkeustilanteiden ja jatkuvuuden hallinnan suunnitelmat testataan sovituin aikatauluin järjestettävillä työpöytäharjoituksilla ja käytännön harjoituksilla.

Purku ja poisto

- tehdään purkusuunnitelma, valitaan toteuttaja ja toteutusta valvotaan
- valitaan oikeat poistotavat ja jätelajit
- myös tiedot poistetaan
- tuhoamista tai loppusijoitusta valvotaan.