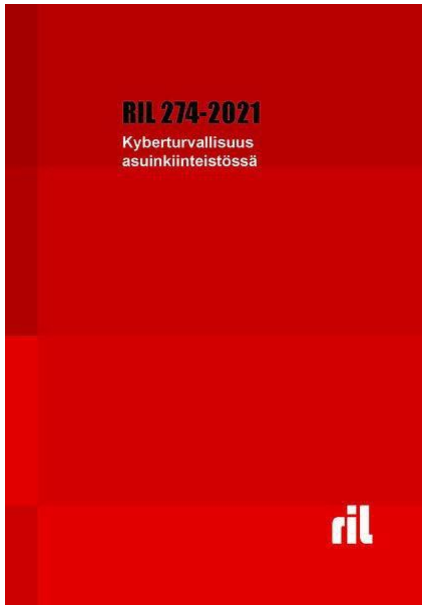
RIL 274-2021 Kyberturvallisuus asuinkiinteistössä



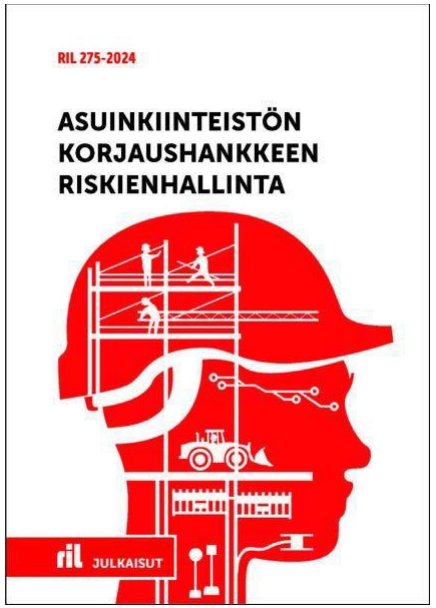
Älykkäiden järjestelmien suunnittelu, ohjaus ja automaatio
MOTIVA 8.10.2024
Pekka Talaskivi, RIL

RILin julkaisuja

RIL 274-2021 Kyberturvallisuus asuinkiinteistössä

Tietoa ja ohjeita kyberturvallisuuden vaikutuksista taloyhtiön strategiseen suunnitteluun ja sen huomioimisesta korjaushankkeen suunnitteluun, toteutukseen ja ylläpitoon. Sisältää myös Case-tapauksia sekä liitteinä mm. Astukri-ohjeistus.

Kyberturvallisuuden perusteet -osio on ladattavissa vapaasti.

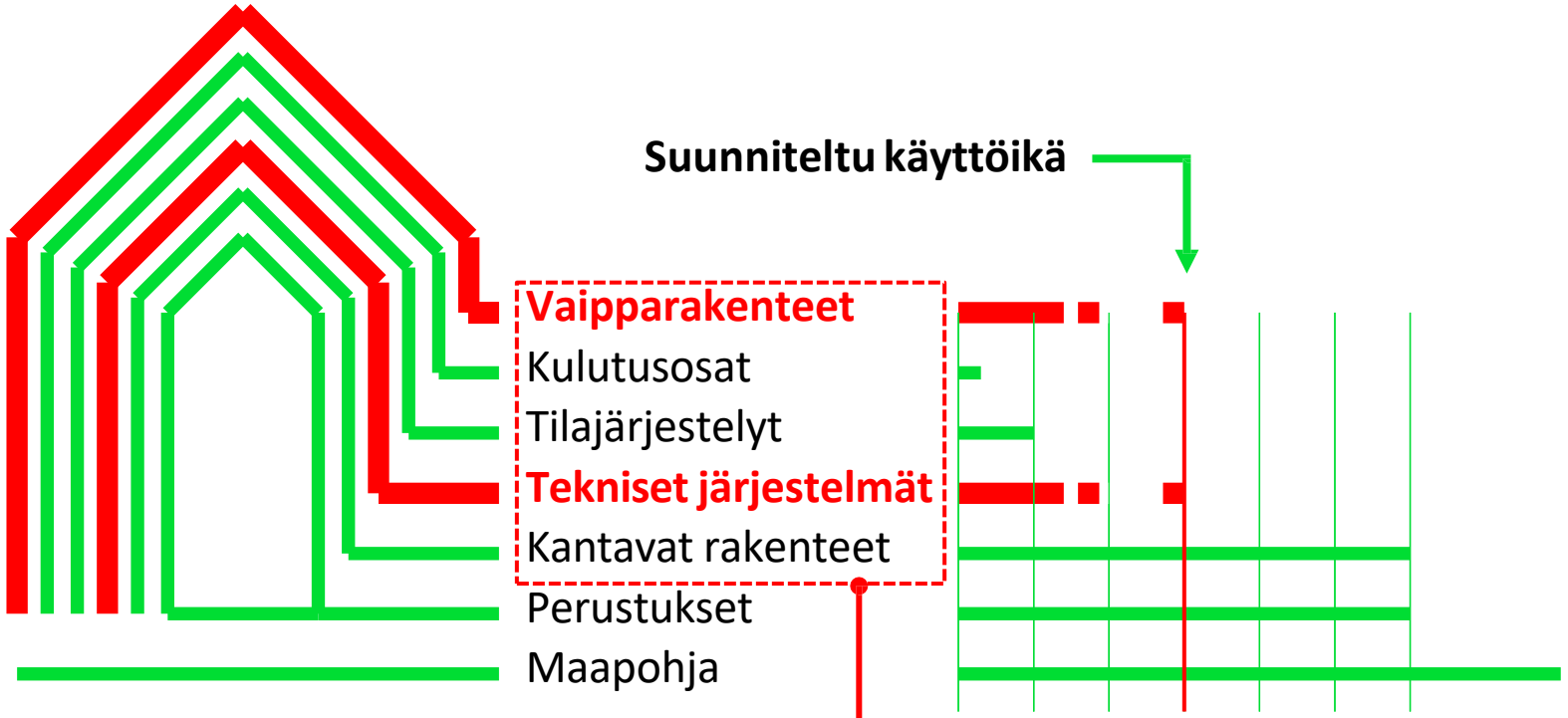


TULOSSA

RIL 275 Asuinkiinteistön korjaushankkeen riskienhallinta

Ohje on tarkoitettu korjaushankkeen tilaajan käyttöön. Tavoitteena on auttaa taloyhtiötä korjaushankkeen eri toteutusvaihtoehtojen mahdollisuuksien ja riskien hahmottamisessa, tukea taloyhtiön päätöksentekoa sekä kehittää korjaushankeprosessia ja taloyhtiöviestintää.

RIL 274-2021 Kyberturvallisuus asuinkiinteistössä



Rakennusosia tai järjestelmiä, joita on huollettava, ylläpidettävä tai uusittava

➔ **yhteys ulkomaailmaan**

Lämmitys
(esimerkki)

Käyttövesi

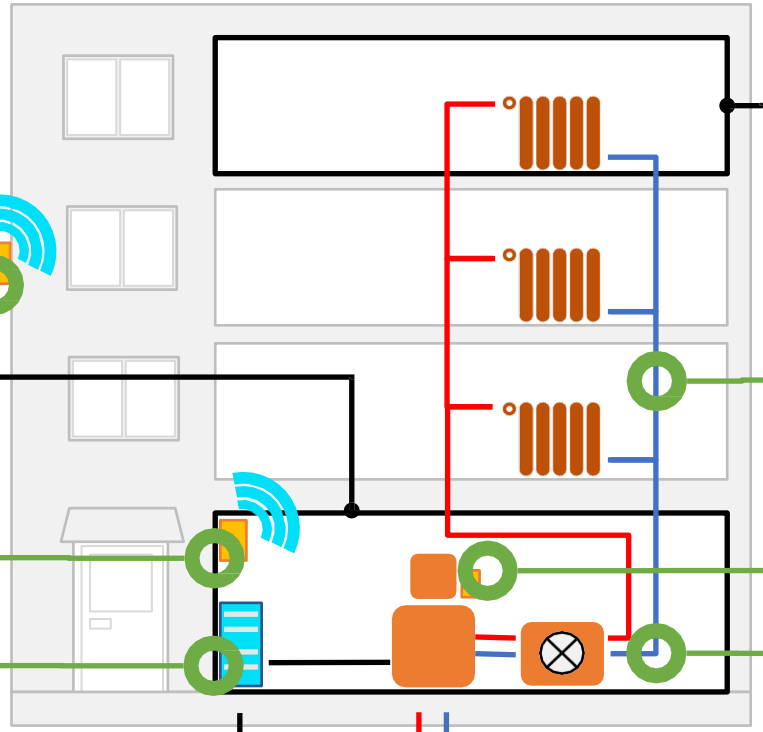
Ilmanvaihto

Sähkö

Jätevesi

Hälytys jne.

KIINTEISTÖN (TIETO)JÄRJESTELMÄ



HUONEISTO
Ei yhteyttä kiinteistön tietojärjestelmiin

Olosuhdeseuranta

KIINTEISTÖ
Suojattu laitetila

Tietoliikennelaitteet ja ohjelmistot

Talotekniikkakeskus

Lämmönsiirtoverkosto

Lämmönvaihtimen ohjaus

Pumput ja toimilaitteet

Etävalvonta ja -ohjaus

Verkostot ja muu infra

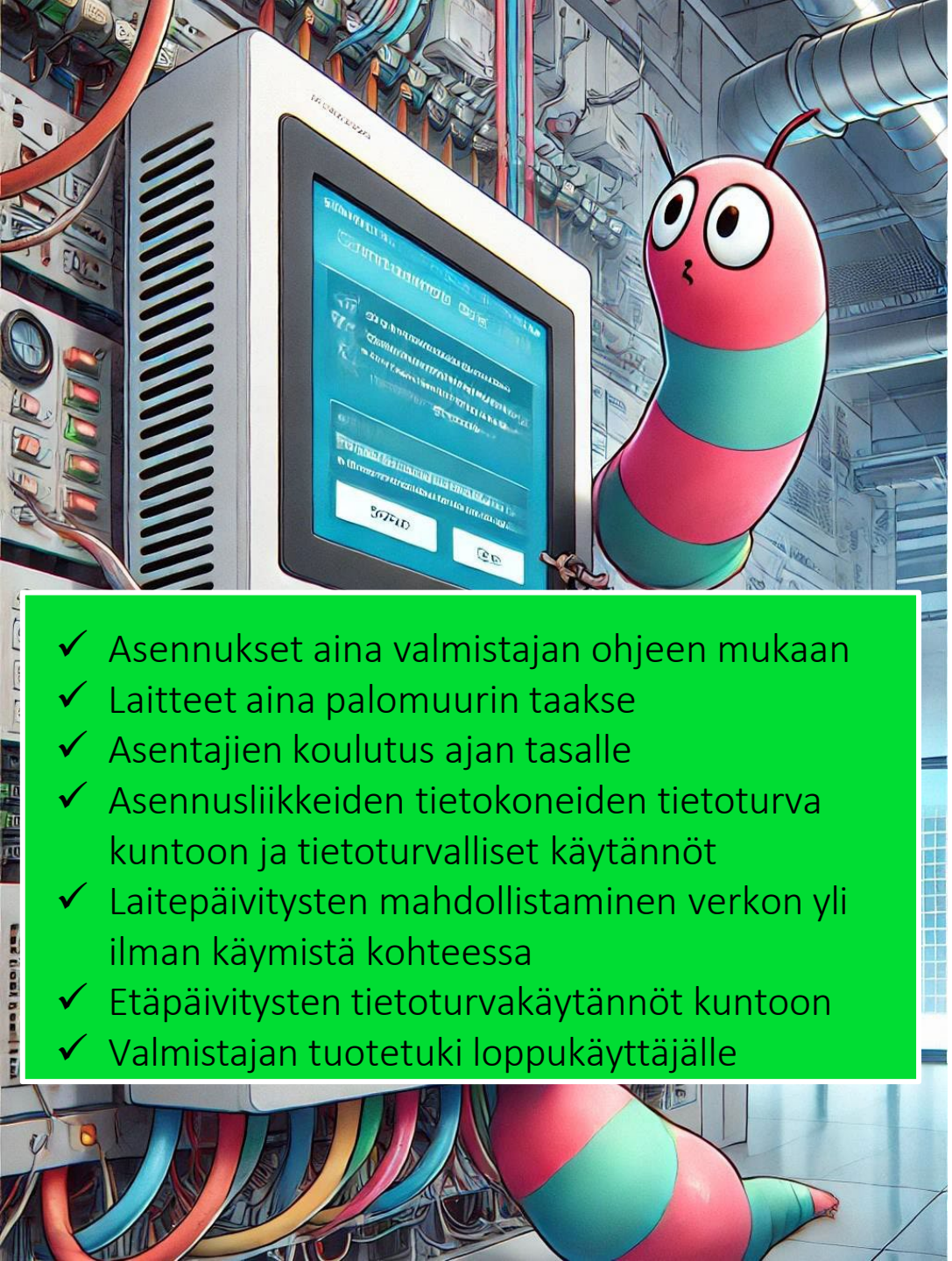
Henkilöstö

Tietoliikenneyhteydet ja laitetilat

SOFT-WARE + App

Ohjelmistot

KYBERYMPÄRISTÖ



- ✓ Asennukset aina valmistajan ohjeen mukaan
- ✓ Laitteet aina palomuurin taakse
- ✓ Asentajien koulutus ajan tasalle
- ✓ Asennusliikkeiden tietokoneiden tietoturva kuntoon ja tietoturvalliset käytännöt
- ✓ Laitepäivitysten mahdollistaminen verkon yli ilman käymistä kohteessa
- ✓ Etäpäivitysten tietoturvakäytännöt kuntoon
- ✓ Valmistajan tuotetuki loppukäyttäjälle

Case

Windows-mato julkiseen verkkoon kytketyissä säätimissä

Valmistajalle ilmoitettiin rakennusautomaatiossa käytettävistä säätimistä, jotka jumiutuivat toistuvasti ilman näkyvää syytä.

Valmistajan tuotekehitys otti etäyhteyden yhteen oudosti toimivaan säätimeen. Todettiin, että säätimeen oli ladattu Windows-mato, joka vei kyseisen säätimen vapaan muistin ja sai sen tämän vuoksi ajoittain jumiin. Mato ei kyennyt leviämään säätimestä eteenpäin. Kyberturvakeskusta informoitiin heti tapahtumasta.

Säätimet oli kytketty julkiseen internetverkkoon ilman palomuuria, jolloin mato oli päässyt sisään TCP-protokollaa käyttävästä FTP-portista.

Vaihtoehtoisesti mato oli päässyt säätimiin asentajan kannettavasta tietokoneesta, joka oli ollut suojaamattomana yleisessä verkossa.

Korjaavat toimenpiteet

Valmistaja ajoi kaikkiin verkossa olevin säätimiin massapäivityksenä uudet ohjelmat, jotka sulkivat FTP-portin.

Tapauksen vuoksi valmistaja on ottanut säätimiin käyttöön palomuurin, jossa oletuksena kaikki portit ovat suljettuna ja vain tarvittavat avattu. Lisäksi laitteen ja verkossa olevien palvelimien välisessä tietoliikenteessä on otettu käyttöön etäkäyttöyhteyden TLS-salaus.

- ✓ Huolellisuus järjestelmien hallinnassa ja verkkoon liittämisessä
- ✓ Järjestelmien hallinnan ja ylläpidon selkeä vastuuttaminen
- ✓ Vastuu ei saa jäädä ainoastaan järjestelmän omistajan (taloyhtiö) harteille

➔ **TALOYHTIÖN STRATEGIA**

Case

Verkkohyökkäys katkaisi talojen lämmityksen Lappeenrannassa

Verkkohyökkäys aiheutti häiriöitä lämmitysjärjestelmien toiminnassa kahdessa kiinteistössä marraskuussa 2016. Tapaus oli ensimmäinen mediassa näkyvästi esille tuotu tapaus.

Laitteet olivat verkkohyökkäyksen takia sammuneet tai niitä ei pystytty hallitsemaan etäyhteyden kautta. Laitteen ohjelmisto toimi oikein. Laite havaitsi häiriön verkkopalvelimen puolella ja pyrki poistamaan häiriön käynnistämällä säätimen uudestaan. Uudelleenkäynnistys ei luonnollisestikaan poistanut ongelmaa, koska verkkohyökkäys oli jatkuvaa ja erittäin voimakasta. Säädin siis pyrki turvaamaan toimintansa käynnistämällä itseään uudelleen ja uudelleen. Uudelleenkäynnistyksen aikana lämmityksen säätö ei toiminut.

On todennäköistä, että muitakin kohteita joutui verkkohyökkäyksen vaikutuksen alaiseksi, mutta johtuen muutamasta tekijästä (mm. missä asennossa lämmitysverkon venttiilien toimilaitteet olivat, kun uudelleenkäynnistyssykli alkoi), näissä kohteissa ei huomattu ongelmaa.

Kohteet itsessään eivät olleet palvelunestohyökkäyksen kohteena, vaan niiden internetiin suojaamattomana liitettyihin laitteisiin lähetettiin väärennettyä http-liikennettä. Vaikka datamäärä ei ollut suuri, taloyhtiön lämmitystä ohjaavien laitteiden normaali toiminta häiriintyi.

Laitteiden vastaus peilautui Englantiin vedonlyöntipalveluun, joka oli hyökkäyksen varsinainen kohde.

Korjaavat toimenpiteet

Rakennusautomaatiojärjestelmä toimii lähtökohtaisesti ilman verkkoyhteyttä. Suurimmassa osassa verkkoliitäntää hyödynnetään etäseurantaan tai etähallintaan.

Kyberuhkiin varautuminen 1/2

Kriittisiä järjestelmiä

- ✓ Automaatiojärjestelmät
- ✓ Sähkönjakeluun ja käyttöön liittyvät järjestelmät ja kojeet.
- ✓ Vesipumput
- ✓ Valaistuksen ohjaus
- ✓ Lämpöpumput
- ✓ Sähköinen lukitus
- ✓ Jälkikäteen lisätyt mm. etäohjaukseen liittyvät lisälaitteet tms.
- ✓ Tate-järjestelmien reitittimet ja palvelimet
- ✓ Wifi-verkot ja niiden yhteydet taloyhtiön verkkoon
- ✓ Operaattoreiden kytkimet/reitittimet ja niiden suojaus
- ✓ Sähköiset informaatiotaulut.

Joitakin perussyitä häiriöille

- ✓ Tietoturvapäivitykset vuotavat
- ✓ Käyttäjä ei vaihda oletussalasanoja
- ✓ Salasanoja hallitaan taitamattomasti
- ✓ Salasanasuojaus puuttuu kokonaan
- ✓ Automaatiokeskukset tai järjestelmät, voidaan ohjata etänä
- ✓ Vanhat järjestelmät, joihin ei enää saa päivityksiä.

Taulukko 7.2. Asuinkiinteistön käytön ja ylläpidon kyberturvallisuuden perusperiaatteet.

– Piilotetaan laitteet niin, että ne eivät näy avoimesti internetissä. – Käytetään turvallisia käyttäjätunnuksia ja salasanoja. – Ajantasaistetaan ja digitoidaan dokumentointi. – Otetaan lokitiedostot talteen. – Sovitaan kirjallisesti vastuukysymyksistä – myös yhteistyökumppanien kanssa. – Ohjeistetaan huolto ja ylläpito yksinkertaiseksi, mutta turvalliseksi. – Otetaan käytännöksi, että ei käytetä samaa tunnusta ja salasanaa eri palveluille. – Hankitaan turvalliset ja salatut etäyhteydet.

Taulukko 7.3. Asuinkiinteistön ohjelmistojen päivityksen perusperiaatteet.

– **Varmuuskopioidaan** mahdolliset asetustiedostot ja kirjoitetaan ylös ohjelmistojen versionumerot ennen päivitystä. Päivityksen jälkeen varmistetaan, että versionumerot ovat muuttuneet odotetusti. – **Varaudutaan palauttamaan** aiempi ohjelmisto takaisin käyttöön, mikäli uuden toiminnassa ilmenee ongelmia. – **Varataan riittävästi aikaa** päivitykseen. Asentaminen ja uudelleenkäynnistyminen sekä mahdollisten toiminta-asetusten säätäminen voi viedä tunteja, jos kohteita on useita. Prosessia ei voi kiirehtiä. – **Ajoitetaan päivitykset** hetkiin, jolloin niistä aiheutuu mahdollisimman vähän haittaa asukkaille. Päivitysten ajaksi laitteen normaali toiminta lakkaa. – **Varmistetaan sähkönsyöttö** ennen päivityksen aloittamista. Sähköjen katkeaminen kesken päivitysprosessin voi asettaa laitteen tilaan, josta toipuminen on mahdotonta. – **Ladataan päivitystiedostoja** vain valmistajan omalta sivulta. Usein tiedostoon liittyy tieto sen koosta, päiväyksestä ja tarkistussummasta. Ne täytyy tarkistaa ja verrata päivitystiedoston todellisiin tietoihin ennen asennuksen aloittamista. – **Dokumentoidaan päivitykset** esimerkiksi merkitsemällä lokikirjaan tieto versiosta, päiväyksestä ja työn suorittaneesta asentajasta onnistuneen päivityksen jälkeen. – **Seurataan automaattipäivitysten toteutumista** dokumentoimalla säännöllisesti verkon yli tapahtuneiden päivitysten versiotiedot.

Yleisiä kyberturvallisuusperiaatteita

Kyberuhkiin varautuminen 2/2

PILVIPALVELUT

Pilvipalvelujen turvallisuus.
Käytetään ainoastaan luotettavia palveluntarjoajia.

SOVELLUKSET

Päivityspolitiikka.
Sovellusten ja laiteohjelmistojen päivitykset tehdään ajallaan ja suunnitelmallisesti.

DATATURVALLISUUS

Tiedon salaus.
Pääsy tietoihin sallitaan vain tunnistetuille käyttäjille tai järjestelmille.

ASUKKAAN TOIMINTA

Asukkaan ja taloyhtiön erottaminen.
Taloyhtiön ulkoiset yhteydet priorisoidaan ja eristetään asukkaan yhteyksistä.

TALOYHTIÖN STRATEGIA

PÄÄSYNHALLINTA

Turvalliset yhteydet ja fyysiset tilat.
Estetään luvaton pääsy järjestelmiin ja mahdollistetaan tekniikan ylläpito ja hallinnointi.

HUOLTO JA YLLÄPITO

Turvallisuuden johtaminen.
Nimetään kyberturvallisuuden vastuuhenkilö ja varmennetaan ulkoisten toimijoiden osaaminen.

RISKIENHALLINTA

Riskien aktiivinen ennakointi.
Seurataan yleistä kybertilannetta ja varaudutaan torjumaan tunnistetut riskit ennalta.

INFRASTRUKTUURI

Pahimman seurauksen rajaaminen.
Suojataan taloyhtiön perusinfra pahimmilta kyberhäiriöiden seurauksilta.

Kyberturvallisuus ja taloyhtiön strategia

Strategian laadintaprosessi

Asuinkiinteistön strategian mukaisen korjaustason valinta

Rakennusten korjaustasoluokitus talotekniikan osalta olemassa oleville rakennuksille

- Luokka A Parannetaan, kiinteistö ja ulkomaailma ovat älykkäässä ja vuorovaikutteisessa yhteydessä
- Luokka B Parannetaan, talotekniikan osajärjestelmillä on yhteinen käyttöliittymä
- Luokka C Parannetaan, talotekniikan hajautettuja osajärjestelmiä optimoidaan
- Luokka D Peruskorjataan, mutta talotekniikan perustasoa ei paranneta
- Luokka E Kiinteistö ajetaan hallitusti alas, investointeja ei tehdä

Talotekniikan suojaustason valinta

Kyberturvallisuuden suojaustasoluokitus (RT 103206)

- DT1 Suojauksen perustaso
- DT2 Parannettu suojaustaso *

* *Suositellaan A ja B korjaustasoilla*

Kyberturvallisuuden todentaminen

Asuinkiinteistön kyberturvallisuuskriteeristö

- Turvallisuuden johtaminen (TJO)
- Henkilöstöturvallisuus (HT)
- Fyysinen turvallisuus (FT)
- Tietoturvallisuus (TT)

Astukri - Asuinkiinteistön kyberturvallisuuskriteeristö

Vaatimukset on kuvattu vaatimuskorttiin, jossa on vakiorakenne.

Vaatimuksen osa-alue ja numero	**Vaatimuksen nimi tai kuvaus**
Suojaustavoite	Vaatimusten täyttämisen avulla tavoitettava tilanne.
Soveltuvuus	Vaatimuksen soveltamisalue tai sen rajaus.
Vaatimus	Yksi tai useampia vaatimuksia, joiden avulla pyritään todentamaan kohteen tilannetta.
Tietotyypit	Vaatimuksen kohteena oleva tieto.
Lisätietoja	Vaatimukseen toteuttamiseen liittyvää lisätietoa tai perusteita sekä lähdetietoja.

Neljä osa-aluetta

- ✓ Turvallisuusjohtaminen (TJO)
  - *TJO 1 Turvallisuusperiaatteet*
  - *TJ0 2 Turvallisuuden vastuut*
  - *TJ0 3 Turvallisuusriskien hallinta*
  - ***TJ0 4 Turvallisuuspoikkeamien hallinta***
  - *TJ0 5 Alihankkijoiden ja toimittajien turvallisuus*
- ✓ Henkilöstöturvallisuus (HT)
- ✓ Fyysinen turvallisuus FT)
- ✓ Tietoturvallisuus (TT).

Astukri TJO 4	**Turvallisuuspoikkeamien hallinta**
Suojaustavoite	Turvallisuuspoikkeamien hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa – minimoi vahingot ja palauttaa tilanteen normaaliksi. Ilmoitusvelvollisuus asiakkaalle tukee asiakkaan riskienarviointia ja muun muassa vahinkojen minimointia.
Soveltuvuus	Kiinteistölle tuotettavan palvelun turvallisuus kokonaisuudessaan.
Vaatimus	1) Palveluntarjoajalla tulee olla menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn. 2) Palveluntarjoajalla tulee olla käytössään selkeät prosessit turvallisuuspoikkeamien ilmoittamisesta. 3) Turvallisuuspoikkeamien määrää ja tyyppejä tulee seurata. 4) On oltava menetelmä, joilla toteutuneiden poikkeamien uusiutuminen pyritään estämään. 5) Asiakastiedon käsittelyyn liittyvät poikkeamat tai niiden epäilyt tulee ilmoittaa kyseiselle asiakkaalle.
Tietotyypit	Kaikki ne tietotyypit, jotka palvelun elinkaaren aikana ovat siirtyneet palveluntarjoajan haltuun.
Lisätietoja	Vaatimuksen täyttämisessä voi hyödyntää esimerkiksi seuraavaa toimintamallia: Turvallisuuspoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu ja koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, 4) harjoiteltu, ja erityisesti 5) viestintäkäytännöt ja vastuut on sovittu. Erityisesti henkilö ja käyttövaltuustietojen käsittelyyn liittyvistä poikkeamista, tietomurroista tai sellaisten yrityksistä suositellaan ilmoittamaan Kyberturvallisuuskeskukselle. Tunnistetusta rikollisesta toiminnasta suositellaan ilmoittamaan myös poliisille.

Esimerkki Astukri -vaatimuskortista

KIITOS

pekka.talaskivi@ril.fi

RIL Suomen Rakennusinsinöörien liitto – Finnish Association of Civil Engineers

@RILInsinoorit

@rakennusinsinoorienliitto

@rilinsinoorit