

Pientalorakentajan ja -asukkaan

DIGITURVA



PTT
PIENTALOTEOLLISUUS

Digiturvaopas

*Turvallisen rakentamisen
ja asumisen puolesta*





Kodin digiympäristö tarjoaa erinomaisia tuotteita ja palveluita, jotka tekevät asumisesta helpompaa ja turvallisempaa.

Digitaalisuus on tärkeässä roolissa myös energiansäästössä ja ilmastomuutoksen vähentämisessä.

Digitaalisuuteen liittyy myös riskejä, jotka on syytä ottaa huomioon rakentamisen suunnittelussa ja arjen toiminnassa.

Tämä opas on suunnattu pientalorakentajalle ja omakotitalossa asujalle helpottamaan digitaalisen turvallisuuden huomiointia talotekniikassa ja yleensä kodin tekniikassa. Oppaassa asiat esitetään helposti ymmärrettävällä tavalla, mutta ohjeen perusteella rakennuttaja voi myös tilata rakentamisen asiantuntijalta tarvittavia turvallisuusratkaisuja. Osa kuvatuista palveluista ja tekniikoista on jo tätä päivää, osa on vasta tuloillaan. Tarkempia digiturvallisuuden huomioivia ohjeita rakennushankkeeseen ryhtyvälle ja sen suunnittelijoille on tarjolla RT- ja ST-ohjeistoissa www.rakennustieto.fi



Käyttäjätunnukset

Käyttäjätunnus on nimi, josta sinut digimaailmassa tunnustetaan. Käyttäjätunnuksen avulla käyttämäsi palvelu tunnistaa sinut ja tietää, mitkä viestit ja tiedostot kuuluvat sinulle.

Vaihda oletusarvoisen "admin" käyttäjän ja mahdollisesti muiden valmiiden roolien käyttäjätunnukset korvaamalla ne omillasi sekä luo tavallista käyttöä varten oma käyttäjätunnus, jos se on mahdollista.

Hybridikoti

Talotekniikka ja kodin muu tekniikka nivoutuu yhä useammin palveluiden ja verkkojen hybridiksi, jota ohjataan vaivattomasti mobiililaitteilla. Samoja mobiililaitteita käytetään sähköposteihin, sosiaalisen median palveluihin, ruokatilauksiin, etätöihin jne. Mobiililaitte voi kommunikoida esim. auton tai latauspisteen kanssa, välittää maksutietoja ja sisältää vahvasti yksityisyyden suojaan kuuluvia tietoja.

Talotekniikan digiturvallisuus

Digitaalisella turvallisuudella tai lyhyemmin digiturvallisuudella tarkoitetaan riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen, kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojan liittyviä asioita. Talotekniikalla tarkoitetaan kaikkia niitä laitteita, toimintoja ja palveluita, joilla hallitaan sisäolosuhteita (lämpötila, valaistus, ilmanvaihto jne.), valvotaan turvallisuutta (murto- ja palo-ilmaisimet, kameravalvonta jne.) sekä rajoitetaan tai estetään vahinkoja (lukitusjärjestelmä, veden katkaisu oltaessa poissa, automaattinen sammutusjärjestelmä, katkoton jännitesyöttö jne.).

Myös kaikenlainen energian käyttö, tuotto ja muodon muuttaminen, energiayhteisöjen ratkaisut jne. ovat osa talotekniikkaa, joka ilmenee esim. aurinkopaneeleina ja -keräiminä, sähköisten kulkuneuvojen akustojen yksi- tai kaksisuuntaisena käyttönä jne.

Monivaiheinen tunnistautuminen

Henkilöllisyytesi varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä. Lähes kaikki käyttäjätilien kaappausyritykset voidaan estää monivaiheista tunnistautumista käyttämällä.

Vaikka rikollinen saisi tietoonsa käyttäjätunnuksesi ja salasanasasi, palveluun ei pääse kirjautumaan ilman lisätunnistetta.

Palvelut, joissa on henkilö- tai maksutietoja, kannattaa aina suojata monivaiheisella tunnistautumisella.

Salasanat

Verkkopankkiin kirjautuessasi käytät vahvaa kaksivaiheista tunnistautumista, mutta keskustelupalstalle kirjautu-essasi salasanasasi voi olla yksinkertaisempi.

Salasanoja kannattaa päivittää säännöllisesti, mutta hyvää salasanaa ei tarvitse vaihtaa yhtenään. Hyvät ja vahvasti suojatut salasanat saattavat joutua tietomurrossa ja -vuodoissa rikollisten haltuun, vaikka olet tehnyt asiat oikein.

Yksi hyvä tapa suojata salasanoja on salasanan-hallintatyökalu. Hallinta-sovelluksen avulla salasanat ovat tallessa yhden pääsalasanan takana.

Talotekniikan automaatio on pientaloissa usein kompakti kokonaisuus, jolla ohjataan mm. lämmitystä, ilmanvaihtoa ja usein myös turvallisuusjärjestelmien toimintaa.

Sähkönsiirron kaapelointi eri keskuksineen ja laitteineen ovat talotekniikan perusrakenteita, ja sitä täydentää tiedonsiirtoverkko, joka voi olla joko fyysinen tai langaton tai näiden yhdistelmä.

Pilvipalvelut

Pilvipalvelun avulla voidaan saada erilaisia skaalautuvia ja virtuaalisia palveluita (sovelluksia, tallennustilaa, laskentakapasiteettia) internetin välityksellä. Mobiililaite ja siihen linkittyneet pilvipalvelut sisältävät myös elämää helpottavan automaation kaipaamia tietoja mm. kalenterimerkintöinä, joiden avulla kehittyneet optimointipalvelut voivat huolehtia oikea-aikaisesti esim. asunnon lämpötilan mukauttamisesta tai eri energiavarastojen täydentämisestä tai hyödyntämisestä ilman, että käyttäjän pitää olla toistuvasti säätämässä mitä talotekniikka tai kodinkoneet milloinkin saavat ja eivät saa tehdä.

Älykodin sopimuskumppanit

Älykodissa on usein laitteita, jotka vaativat toimiakseen yhteyden niiden valmistajan verkkopalveluun. Tarvetta perustellaan vikavalvonnalla ja huoltomahdollisuuksilla, mutta useimmiten oikea syy on vain pyrkiä keräämään sellaista käyttäjätietoa, jonka voi myydä kolmannelle osapuolelle.

Siksi tulee selvittää huolella mitä sopimuksissa lukee ja käyttää vain luotettavaksi tunnettuja palveluntarjoajia. Markkinoilta on jo esimerkkejä, joissa älykodin laitteita valmistanut on poistunut markkinoilta mitään ilmoittamatta, jolloin hankitut laitteet ovat muuttuneet elektroniikkaromuksi. Pahimmillaan voi käydä niin, että älylukot eivät aukea tai ne ovat koko ajan auki. Tilanteen korjaaminen ei välttämättä onnistu halvalla ja nopeasti.



Kodinkone kaapattu?

*Laite muuttuu hitaaksi
tai toimii oudosti.*

*Televisio temppuilee
tai tietokone jumiutuu.*

*Verkkoyhteys muuttuu hitaaksi,
tai se toimii epäluotettavasti.*

*Verkko-operaattori ottaa
yhteyttä ja kertoo, että
koneelta lähtee epätavallisen
paljon liikennettä.*

Esineiden internet

Yhä useammassa kodinkoneessa on verkkoyhteys. Puhutaan esineiden internetistä eli IoT:stä (Internet of Things). Internet-yhteys voi olla televisiossa, jääkaapissa, kiukaassa, turvakamerassa, silitysraudassa tai vaikka pölynimurissa.

Kodin tietoverkkoon integroituneet kodinkoneet ovat digiturvallisuuden kannalta merkittävä riski.

IoT:stä muistettavaa

Internet-yhteyden omaavan IoT-laitteen voi kytkeä kodin langattomaan tietoverkkoon. Laitteella voi olla myös oma internet-yhteys, joka ei käytä kodin verkkoa, vaan on yhteydessä suoraan laitteen valmistajan palveluihin. Se voi lähettää valmistajalle esimerkiksi tietoja laitteen käytöstä ilman, että tiedät asiasta mitään.

Kodinkoneiden ohjauksessa nettiyhteydestä on hyötyä. Jos kiuas on kytketty kodin verkkoon, voit laittaa saunan lämpiämään kännykällä kotimatalla. Kaupassa voit kurkistaa jääkaappiisi ja katsoa, mitä ruokaa pitää ostaa. Voit ladata älytelevisioon lisäohjelmistoja kuten tablettiin tai matkapuhelimeen.

Esineiden internetin ongelma on, että useiden kodinkoneiden ja laitteiden tietoturva on huono. Kaikissa laitteissa sitä ei ole ollenkaan. Etenkin halpojen mallien tietoturvassa on heikkouksia. Myös omat toimintatavat aiheuttavat riskejä, esim. etäohjattu

Puheohjauksen käyttö?

Puheohjaus on kiva, mutta haluatko, että Amazon, Google yms. kuuntelevat koko ajan ympäristöäsi?

Käytä kodinkoneen internetyhteyttä turvallisesti

Kirjaudu laitteen tai ohjekirjan kertomille internetsivuille ja yhdistä laite kodin verkkoon.

Vaihda laitteen salasana ja käyttäjätunnus. Rikolliset etsivät verkosta laitteita, joissa on valmistajan alkuperäiset tunnukset, esimerkiksi "admin" tai "root". Älä käytä laitetta, jonka salasanoja ja käyttäjätunnuksia ei voi muuttaa.

Jos laitteessa on palomuuuri, laita se päälle. Päivitä palomuuuri silloin tällöin.

Laita päälle ohjelmien automaattinen päivitys. Laitteessa on silloin aina uusin versio ohjelmasta. Se vähentää mahdollisuuksia hyödyntää vanhentuneiden ja turvallisuukseltaan puutteellisempien ohjelmien haavoittuvuuksia.

kiuas voi aiheuttaa palovaaran, kun se on kytketty päälle ilman tilan turvallisuudesta varmistumista.

Kaapattu kodinkone botti-verkon osaksi

Verkkoon kytkettyjen laitteiden määrä kasvaa pian sataan miljardiin. Siksi saamme todennäköisesti lukea jatkossa yhä enemmän uutisia hakkeroinnin kohteeksi joutuneista jääkaapeista, televisioista ja erilaisista tuotantolaitteista.

Botti-verkoilla toteutetaan lähinnä hajautettuja palvelunestohyökkäyksiä (DDoS, Distributed Denial of Service) keskeisiä palveluja tai organisaatiota kohtaan, jolloin suuret määrät verkossa olevia laitteita pakotetaan lähettämään toistuvasti lyhyitä sanomia hyökkäyksen kohteena olevaan palveluun.

Kotiverkosta voi löytyä kiristämiseen hyödynnettävää dataa tai mahdollisuus levittää johonkin muuhun tarkoitukseen soveltuvaa haittaohjelmaa.

Kaappauksen sivuvaikutuksena voi kodinkoneen toiminta häiriintyä, kun sen prosessori(t) tekevät muuta kuin niiden pitäisi, jolloin esim. pakastin voi sulaa tai valaistuksen säätö toimii omituisesti. Yleensä laite saadaan irti botti-verkosta laitteen uudelleen käynnistyksellä, mutta aina se ei riitä, vaan laiteohjelmisto pitää asentaa uudelleen, joissa tilanteissa laitteen konfiguraatietiedoston varmuuskopio nopeuttaa palautumista.

Korvaako vakuutus?

Kodinkoneisiin voi kohdistua myös kybervaikutusta, jolloin tavoitellaan jotain fyysistä vaikutusta, esim. laiterikon tai tulipalon aiheuttavaa ylikuumeenemistä. Kun otat käyttöön WiFi-verkkoon liitettyjä kodinkoneita, varmista vakuutusyhtiöltäsi korvaus ehdot mm. tilanteessa, jossa vahingon on aiheuttanut ulkopuolinen kybervaikutus.

Valvontakamera

Valvontakameroiden käyttöön ei ole kaiken kattavaa ohjetta. Laillisuuden kannalta olennaista on, mitä käyttöä varten ja millä tavalla valvontaa toteutetaan, informoidaanko siitä valvonnan kohteita ja miten kuvataallenteita (henkilötietoja) käsiteltäisiin. Kamera-valvonnan harjoittaja vastaa itse toimintansa laillisuudesta.

Yksityisyyden suoja

Digiriskeistä yksityisyyden suojaan liittyvät riskit ovat yksi huomioitava tekijä. Huonosti toteutettu kamera-valvonta tai ääntä ja kuvaa välittävä ovipuhelinjärjestelmä voivat olla tietosuojan kannalta riski. Myös huonekohtaisen olosuhteiden mittaussysteemin on täytettävä tietosuojavaatimukset, kuten kameravalvonnankin.

Kameravalvonta

Hyvin toteutetulla kameravalvonnalla parannetaan mahdollisuuksia selvittää tapahtumia ja niihin liittyviä tekijöitä jälkikäteen. Joissakin tilanteissa niistä voi olla hyötyä myös vahingon rajaamisessa. Mutta on myös mahdollista, että kameroiden tallentamaa kuvaa ja ääntä päätyy luvattomaan käyttöön, joka vaarantaa yksityisyyden suoja. Varmistu siis kameravalvonnan turvallisuudesta ja lainmukaisesta käytöstä.

Kameravalvonta laissa

*Suomessa kameravalvon-
nasta on määritelty rikoslain
(39/1889) 24. luvussa. Siinä
on kameravalvontaa rajaavia
säädöksiä, jotka koskevat
yksityiselämää loukkaavan
tiedon levittämistä, sala-
katselua sekä salakuuntelua.*

*38. luvussa otetaan kantaa
tieto- ja viestintärikoksista,
joita voidaan soveltaa nyky-
ajan kameravalvontajärjes-
telmiin. Laissa myös linjataan
oikeudettoman sijainnin mää-
reitä eli kotirauhan suojaamaa
paikkaa sekä julkisrauhan
lainsäädännöllistä piiriä.*

Ovipuhelinjärjestelmä

On hyvä, kun ovikello hälyttää myös kännykässä, jolloin näkee, kuka ovella on ja voi kertoa milloin on kotona. Ovipuhelinjärjestelmään voi kuitenkin liittyä salakuuntelun ja -katselun mahdollisuus teknisestä toteutuksesta riippuen. Suositus on, että salakuuntelun ja -katselun estämiseksi ovipuhelinjärjestelmän huoneistossa oleva mikrofoni olisi oikosuljettu, kun siihen ei puhuta ja kameran optiikan edessä olisi läppä tms. estämässä kuvaamisen, kun sitä ei haluta. Tällöin ei järjestelmään murtautuja pääse seuraamaan eikä tietotekninen vika levittämään yksityisyyden suojaan liittyviä tietoja.

Etäterveydenhoito

Digitaaliset ratkaisut laajentavat erityisryhmien ja iäkkäiden mahdollisuuksia asua kotonaan. Sovellukset lähettävät verkon kautta terveystietoja ja hälyttävät tarvittaessa apua sen lisäksi, että tekniikka mahdollistaa vaivattoman kommunikoinnin asunnon ulkopuolisten sosiaalisten yhteyksien kanssa. Teknisesti asumisturvallisuuteen liittyvät sensorit yms. voivat olla osa integroitua talotekniikka, jonka myötä talotekniikan digiturvallisuuden vaatimukset ovat yleensä tavanomaista kovemmat.

A man is relaxing in a wooden lounge chair on a patio. In the background, there is a house with solar panels installed on the roof. The entire image has a green tint.

Energia

Älykkäiden digitaalisten ratkaisujen avulla omakotiasuja voi säästää energiakuluissa. Erilaiset sovellukset mahdollistavat energiankäytön hallinnan ja seurannan vaivattomasti omasta mobiililaitteesta. Automaation lisääntymisen myötä myös digiturvaa uhkaavat riskit kasvavat, joka on huomioitava suunnitelmissa, toteutuksessa ja ylläpidossa.

Älykäs energiankäyttö

Älykäs energiankäyttö edellyttää monia mittaus-tietoja ja ennusteita energian käytöstä, tuotosta ja hinnoista. Nykyisin sähköenergian markkinoilla on nopeasti vaihtelevaa hinnoittelua kysynnän ja tuotannon vaihtelun mukaan. Kaukolämpöön ja -kylmään voi tulla myös suurtakin hintavaihtelua energiamarkkinan muutosten myötä. Älykäs ja kapasiteetiltaan merkittävä jousto ei toteudu ilman investointeja ja luotettavaa tiedonvaihtoa. Kuluttajan ja myyjän tulee keskustella ja sopia eduista ja kustannuksista esimerkiksi eBUS:n käytön yhteydessä.

Kysyntäjousto

Sähkömarkkinoihin liittyy kysyntäjousto, jossa kyse on tuotannon ja kulutuksen välisestä tasapainotuksesta. Jos sähkön tuotantoa on enemmän kuin kulutusta, taajuus nousee, jolloin kulutusta täytyy lisätä. Jos sähköä tuotetaan vähemmän kuin kulutetaan, taajuus laskee, jolloin kulutusta täytyy vähentää. Sähkön tuotannon ja kulutuksen on oltava jatkuvasti



Aurinkopaneelit ja -keräimet

Aurinkopaneelit ovat osa sähköjärjestelmää ja parhaimmillaan, kun ne liitetään joko omaan tai energiayhteisön akustoon, jolla voi tasata tuotannon ja kulutuksen ajallisia ja tehollisia eroja.

www.energiatehokaskoti.fi

tasapainossa, eikä tuotannon nopea säätely ole mahdollista kuin tietyillä tekniikoilla. Lisäksi siirtoverkon kuormitushuiput voivat aiheuttaa lisäkustannuksia, ja ylikuormitustilanteelta suojaavat katkot jakelussa monia muita ongelmia.

Lämmitys ja ilmastointi

Tyypillinen kulutusjouston kohde on kiinteistön lämmitys ja jäähdytys. Niiden toteutuksesta riippuen energian syötön katkos voi olla kymmenistä minuuteista muutamaan tuntiin ilman, että sisäolosuhteet muuttuvat käyttäjien kannalta vielä liikaa. Älykäs jousto edellyttää tietoisuutta kohteen energia-varannoista sekä varaus- ja purkaustehoista, ennusteen energian kulutuksesta ja sopimuksellisia tietoja energian hinnasta eri ajankohtina ja tehoilla. Vähemmän älykäs jousto vain olettaa joustovaraa olevan, ja antaa sähköön myyjän katkoa jännitettä esim. lämmitysjärjestelmästä.

Kulkuneuvojen lataus ja akut

Ajoneuvoliikenteen sähköistymisen myötä lisääntyvä akustojen lataus ja purkaminen (kaksisuuntainen lataus) on jouston kannalta jatkossa hyvin merkittävä tekijä. Kun akustojen varaus- ja purkaussyklien vaikutus elinkaarikustannuksiin saadaan kohtuulliseksi, niin akustojen hyödynnettävyys kasvaa merkittävästi. Älykäs hyödyntäminen vaatii edellä kuvatusti paljon tietoa, joten järjestelmien ja palveluiden digiturvallisuudelta on myös syytä vaatia riittävää kyvykkyyttä.

Kodinkoneet

Kodinkoneiden energian käyttö on yksi kulutusjouston mahdollisuus. Kaikkien kodinkoneiden kohdalla ei joustoa voi tehdä, mutta esim. pesukoneissa ohjelman aloitusta voidaan siirtää ja siten ajoittaa pesuveden lämmityksen ajankohta kulutuksen kannalta paremmin. Sähköhellan ja -kiukaan teho on moninkertainen pesukoneeseen nähden, mutta vaikuttaminen käytön ajankohtaan on haasteellista, jolloin saavutettavat hyödyt jäänevät vähäisiksi.

Ohjeita ja turvallisuus-ratkaisuja

Rakentamisen ja asumisen digitaalista turvallisuutta parantavia ratkaisuja, joista toiset ovat useimmilla jo luonnostaan käytössä ja osa sellaisia, joiden käyttöönotto vaatii joko hieman lisää omaa panostusta tai sopivan kumppanin käyttöä.

Internet-yhteyden suojaus, VPN

Selaimen ja sähköpostin tiedonsiirto yleensä salaataan sovelluksessa automaattisesti, mutta kaikkien laitteiden kaikenlaisen tietoliikenteen salaaminen on helpointa toteuttaa reitittimen VPN-palvelun avulla, jolloin kaikki sitä käyttävät kodin internet-yhteydet kulkevat salattuna. Hyvälaatuisen kotireitittimen suorituskky riittää VPN-asiakasohjelman ajoon ilman, että tiedonsiirtonopeus kärsii liikaa, mutta tarjolla on myös muitakin toteutusmalleja. VPN:n etuna on lisäksi se, että kotipaikkaasi ei voida tunnistaa enää IP-osoitteen perusteella, joskin se voi onnistua varsinaisen palvelun muuten saaman tiedon perusteella.

Palomuuuri (Firewall)

Yksinkertaisimmillaan palomuuuri estää uuden yhteyden avaamisen internetin suunnasta kotiverkon laitteille ja palveluihin. Kun yhteys on aina avattava kotiverkosta, on kontrolli verkon käyttäjällä (henkilö tai ohjelma). Kehittyneempiin palomuuritoteutuksiin liittyy myös suodattimet haittaohjelmien pyrkimyksille avata yhteyksiä kotiverkosta ulospäin, sekä erilaiset hallitut menettelyt sallimaan palomuurin läpi mm. etähallinnan vaatimat yhteydenotot.

Suojaus haittaohjelmilta

VPN ja palomuuuri eivät estä haittaohjelmien pääsyä kotiverkon laitteille internetin käytön yhteydessä. Haittaohjelmat pitää ensin tunnistaa, jotta ne voidaan eristää ja poistaa saastuneista laitteista, ja tähän tarkoitukseen on tarjolla useita eri vaihtoehtoisia tuotteita ja palveluita, nk. virusskannereita. Kaikkiin verkon laitteisiin suojausta haittaohjelmia vastaan ei saa jälkikäteen, vaan monissa IoT -laitteissa sekä viihdelaitteissa toiminnallisuus tulee olla jo sisään-rakennettu.

Pidä huoli haittaohjelmilta suojaavien ohjelmistojen ml. IoT- ja viihdelaitteiden laiteohjelmat (Firmware, FW) ajantasaisuudesta sallimalla niiden automaattiset päivitykset ja tarkista aika ajoin ovatko ne raportoineet mistään pienestäkään havainnosta tai päivityksiin liittyvistä ongelmista. Käytä vain tunnettujen palveluntarjoajien VPN- ja palomuuriratkaisuja.

Langattomat verkot ja reitittimien palvelut

Vaikka lähes kaikki Wi-Fi/WLAN-laitteet tarjoavat oletusarvoisesti salaavaa tiedonsiirtoa radiotielle, niin varmistu laitteiden asetuksista salatun tiedonsiirron olemassaolo. Voit vaihtaa salausavaimen omaksesi, mutta vaihda ainakin laitteiden hallintaan tarvittavan käyttäjätunnuksen salasana. Kotiverkoissa langattoman verkon tukiasema voi olla myös reititin internet-yhteydelle, joten varmistu laitteen asetuksista ainakin em. palomuurin ja osoitteen käännön (NAT) päällä olo.

Kotiverkon segmentointi

Astetta vaativampi suojaustapa on osittaa tai segmentoida kotiverkko useisiin aliverkkoihin. Aliverkkojen tarkoituksena on pakottaa aliverkon laitteen tai laiteryhmän tiedonsiirto kulkemaan myös verkon sisällä sen toisissa aliverkoissa oleville laitteille ja palveluille palomuurin kautta, jolloin tiedonsiirron luvallisuus voidaan tarkistaa ja sallia vain hyväksyttävä liikenne. Tällöin esim. haittaohjelmasta saastuneen tai jotenkin muuten vioittuneen laitteen verkkoliikenne ei pääse helposti leviämään verkossa aiheuttaen laajempia vahinkoja. Aliverkot toteutetaan rajaamalla tarvittavat osoitteet tai osoitealueet kuulumaan samaan segmenttiin. Segmentoinnin toteuttaminen kannattaa antaa alan osaajan hoidettavaksi.

Varmuuskopiot

Laiterikko, haittaohjelma tai myös inhimillinen virhe voivat aiheuttaa tietojen häviämisen tai niihin pääsyn estymisen. Tietojen palauttaminen varmuuskopiosta on helpompaa ja halvempaa kuin niiden alkuperäisen tallennusmedian korjaus käyttäen kalliita erikoismenettelyjä. Varmuuskopioistakaan ei ole hyötyä, jos ne ovat kovin vanhoja (tietoja puuttuu) tai ne on salattu siten, että salausta ei saa purettua. Tuorekin varmuuskopio voi sisältää haittaohjelmia, joten palautuksen tehostamiseksi varmuuskopioita on hyvä olla hieman eri ikäisiä ja eri tavoin toteutettuna. Arvioi eri varmuuskopioinnin vaihtoehtoja siltä kannalta, mikä merkitys tietojen katoamisella tai niihin pääsyn estymisellä on, ja valitse sen perusteella tarpeisiisi sopivat varmuuskopioinnin menettelyt. Pilvipalvelu on yksi melko vaivaton vaihtoehto verrattuna omaan verkosta irrallaan olevaan kovalevyyn, mutta siinä varmuuskopiointi on täysin omassa hallinnassa.

Rakentamisen suunnitelmätiedot

Rakentamista edeltää suunnitteluvaihe, jonka lopuksi on käytössä usein monien versioiden myötä muovautunut kokonaisuus asema-, julkisivu- ja pohjapiirroksia, rakennepiirroksia, talotekniikan suunnitelmia ja piirroksia yms. Suunnitelmat ovat hyvin harvoin salassa pidettäviä, mutta jos kohteeseen toteutetaan tilaturvallisuusjärjestelmiä, ovat niiden suunnitelma- ja toteumatiedot luottamuksellisia. Suunnitelmätiedot voivat olla teksteinä, kuvina ja piirroksina ja yleensä pdf-muodossa toteuttajien käytettävissä, vaikka suunnittelijoilla ne olisivat natiiveissa tiedostomuodoissa. Tietomallikin (Building Information Model, BIM) voi olla käytössä, jolloin icf-muotoisten tiedostojen käsittelyyn kykenevät ohjelmat voivat visualisoida

tavoiteltavat rakenteet. Ainakaan toistaiseksi ei suunnitteluohjelmissa ole mahdollisuutta palauttaa tietomallia natiiviksi, joten kiinteistöön sen elinkaaren aikana tehtävät muutokset on dokumentoitava jollain muulla tavalla, esim. alkuperäisiin suunnitelmiin niiden kanssa yhteensopivan ohjelmiston avulla. Menettely rajoittaa selvästi mahdollisuuksia valita toimittaja, jollei alun perin ole sovittu suunnitelmatietojen luovutuksesta myös natiivissa muodossa. Vaikka natiivit muodot olisivat käytössä, niin sekin rajoittaa jatkotyöskentelyä, sillä talotekniikan eri suunnitteluohjelmistot eivät ymmärrä toistensa tiedostomuotoja. Lisäksi on hyvä muistaa, että 20 vuotta vanhaa natiiviakaan ei välttämättä enää tueta suoraan, vaan tiedostoille on tehtävä välikonvergointi tai välikonvergointeja ennen kuin niitä pääsee hyödyntämään uudelleen suunnittelussa. Suunnitteludokumenttien saatavuus on yksi osa tietoturvallisuutta, ja sitä voi yrittää parantaa sopimalla pelkkien pdf-muotoisten suunnitelmatietojen luovutuksen lisäksi myös suunnitelmatietojen saamisesta natiivissa tiedostomuodossa, tietomallina (icf) sekä jossain yleisessä CAD-muodossa, kuten esim. DXF, jota yleensä voi lukea ja muokata ilmaisohjelmillakin toisin kuin DWG-tiedostoja voi yleensä vain lukea ilmaisohjelmilla. Kaikki suunnitelmatiedot on syytä varmuuskopioida ja säilyttää huolella.

Talotekniikka

Talotekniikka ja etenkin sen automaatio on pientaloissa usein kompakti kokonaisuus, johon voi hyvin soveltaa samoja periaatteita, kuin kodinkoneisiin ja muihin IoT-laitteisiin. Poista oletusarvoisen "admin" käyttäjän ja mahdollisesti muiden valmiiden roolien salasanat käytöstä ja korvaa ne omillasi sekä luo tavallista käyttöä varten oma käyttäjätunnus, jos se on mahdollista.

Laitteiden päivittäiseen hallintaan on yleensä käytössä niiden pienet näytöt muutamane painikkeineen, mutta laajempaa tarkastelua, konfigurointia tms. varten voi laitteissa olla oma web-palvelu, jonka avulla selaimeen tuodaan tarvittava käyttöliittymä erilaisine tietoineen. Myös valmistajien omat mobiiliapplikaatiot ovat yleistyneet, ja niissä toimintojen laajuudet voivat vaihdella hyvinkin paljon. Käyttöliittymäpalvelun ei tarvitse olla osa kotiverkkoa, mutta jos laite on liitetty kotiverkkoon, niin toimi digiturvallisuuden kannalta sen mukaisesti.

Laitteista on syytä tietää miten, minne ja missä tilanteissa ne yrittävät ottaa yhteyttä kotiverkkoon ja etenkin internetin palveluihin. Laitteissa voi olla myös joku muu ulkoisen yhteyden toteuttava palvelu esimerkiksi laitevalmistajan tai huoltosopimuksen tarpeisiin liittyen, joka on huomioitava arvioitaessa digiturvallisuustoimenpiteitä.

Talotekniikan laitteista ei välttämättä saa aina varmuuskopioita, eikä edes niiden asetuksista, joten arvot on syytä dokumentoida paperille mahdollisia palautustilanteita varten. Ohjelmistopäivitysten suhteen tilanne vaihtelee, joihinkin päivityksiä tulee, toisiin ei.

Talotekninen toteutus ja sen automaatio voi olla hyvinkin laaja kokonaisuus. Laajemmassa toteutuksessa voi olla esim. kahdesta neljään erilaista kenttäväylää käytössä eri tarkoituksiin. Näitä voi käyttää erilaiset mittarit ja anturit, ilmanvaihtokoneet, lämpöpumput, lämpötilan säätimet, valaistus, sähköinen lukitus jne. Lisäksi eBUS ja sähköauton lataus tai kaksisuuntainen lataus sekä oma sähköntuotanto esim. aurinkopaneelein voivat lisätä automaation laajuutta ja digitaaliseen turvallisuuteen kohdistuvia riskejä. Talotekninen toteutus tulee nähdä systeemisenä kokonaisuutena, johon digitaalinen turvallisuus on sisäänrakennettu ominaisuus. Rakennusten digitaalisen turvallisuuden huomiointiseksi on RT- ja ST-ohjeistoissa tarjolla tilaajalle, suunnittelijalle ja ylläpidolle tarkempia ohjeita.

Tarkempia digiturvallisuuden huomioivia ohjeita rakennushankkeeseen ryhtyvälle ja sen suunnittelijoille on tarjolla RT- ja ST-ohjeistoissa www.rakennustieto.fi

Tarkistuslista

Käytä internet-palveluita virtuaalisen yksityisverkon (VPN) avulla.

Käytä palomureja (Firewall) ja osoitteen kääntöä (NAT) internet-yhteyksillä.

Käytä haittaohjelmien tunnistus- ja esto-ohjelmia kaikissa mahdollisissa verkon laitteissa.

Pidä ohjelmistot ajan tasalla, myös laiteohjelmistot kaikissa verkon laitteissa.

Ota säännöllisesti varmuuskopiot ja säilytä niistä ainakin osa irti verkosta.

Vaihda kaikista verkon laitteista niiden oletuksena tulevat salasanat ja salausavaimet.

Segmentoi kotisi verkko sopiviin kokonaisuuksiin ja luo niiden välille toimivat palomuurisäännöt, jos vain mahdollista tukeudu asiantuntijaan.

Lue myös pienellä painettu teksti eri palvelusopimuksista ja pyri ymmärtämään, mihin olet sitoutumassa.

Estä salakatselu ja -kuuntelu, noudata määräyksiä kameravalvonnasta.

Varmista ja ylläpidä kotisi sähköisen dokumentaation ajan tasaisuus ja saatavuus.

Varmistu, mitä kotisi vakuutusehdoissa todetaan kybervaikutuksen vahinkojen korvaamisesta.

Käytä vain luotettavia suojaus- ja turvallisuuspalveluja ja -ratkaisuja sekä kumppaneita. Älä käytä verkossa tarjolla olevia ilmaisia ratkaisuja.

Pientalorakentajan ja -asukkaan DIGITURVA

Hyvän rakentamisen ja asumisen puolesta

Tämän oppaan on toteuttanut ja rahoittanut
Rakennuspooli yhteistyössä
Pientaloteollisuus PTT ry:n kanssa.

Rakennuspooli on rakennusteollisuuden ja
viranomaisten välinen yhteistyöelin häiriötilanteiden ja
poikkeusolojen rakennustoimintaa koskevissa asioissa.

PTT on puu-, kivi- ja hirsitalovalmistajien
etujärjestö, jonka tavoitteena on edistää
pientalorakentamista ja -asumista.
PTT on osa Rakennusteollisuus RT:tä.



www.pientaloteollisuus.fi