Kyberturvallisuus seurakunnassa

- opas kyberturvalliseen työskentelyyn -

Kyberturvallisuus seurakunnassa

Jouni Lahtinen

Jyväskylän seurakunta

Jyväskylä 2024

Julkaistu Digiturvaviikolla 30.9.2024

Kuvat: Sami Saarenpää Kansikuva Jyväskylän kaupunginkirkko,

s. 12, s. 17, s. 30 ja s. 50 Luotu tekoälyn avulla

Tulostusohje PDF-tiedostolle:

Tulosta 19-sivuisena vihkona, taita keskeltä ja nido. Mikäli haluat tulostaa pelkästään täytettävän Kyberturvallisuus seurakunnassa -työkirjan (liite 7), valitse sivut 72-75 ja tulosta mustavalkoisena vihkona.

Sisällys

1. LUKIJALLE

Suomen evankelis-luterilaisen kirkon (2020) vuoteen 2026 ulottuvassa Ovet auki -strategiassa kehotetaan avaamaan seurakuntatilojen ovet ja kutsumaan ihmiset sisään jättämättä ketään ulkopuolelle.

Kyberturvallisuudessa lähtökohta on erilainen. Kyberturvallisuuteen liittyy vahvasti Zero Trust -malli, joka pohjautuu ajatukseen, että mihinkään tai kenenkään ei lähtökohtaisesti voi luottaa. Tästä olisi helposti tehdä vastakkainasettelua nykyiseen kirkon strategiaa toteamalla kyberturvallisuuden edellyttävän Suomen evankelis-luterilaisen kirkon noudattavan päinvastoin ”Ovet kiinni” -strategiaa.

Jotta tällaiselta vastakkainasettelulta vältytään, pitää enemmänkin ajatella tietoturvallisuuden ja kyberturvallisuuden olevan osa työkaluja ja mahdollistajia kirkon Ovet auki -strategian toteuttamiseen ja kirkon hengellisen perustehtävän hoitamiseen nykypäivänä. Kirkon strategiassa kehotetaan hengellisyyden ja avoimuuden lisäksi muun muassa jatkamaan digitalisaatiota kirkossa palveluja sähköistämällä. Tässä kokonaisuudessa kyberturvallisuudella on merkittävä rooli palvelujen turvallisuuden ja luotettavuuden näkökulmasta.

Kirkon Ovet auki -strategian pohjalta ollaan parhaillaan laatimassa Suomen evankelis-luterilaisen kirkon digitalisaatiostrategiaa. Digitalisaatiostrategian visioksi on päätetty ”*Ihmislähtöisiä kirkon palveluita digitaalisesti”*. Strategiassa määritellään tarkemmin kirkon digitalisaatiota koskevat strategiset linjaukset, tavoitteet ja päämäärä sekä keinot niiden saavuttamiseksi. Digitalisaatiostrategian avulla kirkko kehittää toimivampia ja joustavampia toimintamalleja huomioiden julkisyhteisölle asetetut vaatimukset kansalaisille tarjottavista helppokäyttöisistä ja turvallisista palveluista. Kyberturvallisuudella tulee olemaan siis merkittävä rooli kirkon digitalisaatiostrategiassa. (Suomen ev.lut. kirkko, 2024a.)

Tämä Kyberturvallisuus seurakunnassa -opas on tarkoitettu Suomen evankelis-luterilaisen kirkon, kirkkohallituksen, tuomiokapitulien, seurakuntien ja työntekijöiden käytettäväksi. Kirkon kyberturvallisuus koostuu kirkon oman toiminnan lisäksi myös seurakuntalaisista, seurakuntien asiakkaista, yhteistyökumppaneista ja palveluntarjoajista, joten opas on myös heidän luettavissa.

Oppaan tarkoituksena on muun muassa avata kyberturvallisuuden käsitettä ja mikä on kyberturvallisuuden rooli nykypäivän kirkossa. Lisäksi opas neuvoo, kuinka kirkon eri toimijoiden pitäisi huomioida kyberturvallisuus seurakuntatyössä. Oppaan pohjana toimivat muun muassa Kyberturvallisuuskeskuksen ja Digi- ja väestötietoviraston ohjeistukset, Suomen evankelis-luterilaisen kirkon tietoturvapolitiikka (2022a) ja kirkon yleiset tietoturvamääräykset (2022b.). Lisäksi on hyödynnetty kirkon IT-alueiden tietoturvaohjeistuksia voimassa olevaa lainsäädäntöä unohtamatta.

Suomen evankelis-luterilaisen kirkon seurakunnissa ja IT-alueilla voi olla poikkeavia ohjeistuksia ja/tai käytäntöjä tähän oppaaseen verrattuna. Tämän vuoksi on hyvä muistaa noudattaa aina ensisijaisesti oman työnantajan antamia ohjeistuksia. Kyberturvallisuuden tilannekuva ja kyberturvallisuutta uhkaavat riskit muuttuvat jatkuvasti, joten myös kyberturvallisuutta tukevia suojauskäytäntöjä ja kirkon ohjeistuksia sekä lainsäädäntöä on päivitettävä säännöllisesti.

Parhaillaan Suomen evankelis-luterilaisessa kirkossa on käynnissä kirkon tietoturvapolitiikan ja kirkon tietoturvamääräysten päivittäminen. Nämä muutokset tullaan huomioimaan viimeistään päivitetyssä oppaassa syksyllä 2025. Palautetta tästä oppaasta voi laittaa sähköpostilla allekirjoittaneelle.

Kyberturvallisuus seurakunnassa -opas on toteutettu osana Johtamisen ja yritysjohtamisen (JYET) -erikoisammattitutkintoa, jossa keskitytään erityisesti kyberturvallisuuden johtamiseen. Toivon, että opas otetaan seurakunnissa ahkeraan käyttöön ja että se auttaa kirkon työntekijöitä toimimaan entistä turvallisemmin digitaalisessa maailmassa.

Kiitokset Jyväskylän seurakunnalle opiskelujen mahdollistamisesta ja kiitos kaikille oppaan kirjoittamisessa mukana olleille.

Jyväskylässä Digiturvaviikolla 30.9.2024

Jouni Lahtinen

tietohallintopäällikkö, tietosuojavastaava

Jyväskylän seurakunta

jouni.lahtinen@evl.fi

2. SANASTO

Digitalisaatio

Digitalisaatio tarkoittaa sitä, että tietotekniikkaa hyödynnetään yhä enemmän arkielämän järjestämisessä. Suuntaus koskee kaikkea yhteiskunnan toimintaa aina pankkiasioista joukkoliikenteeseen ja tiedon hausta viestien lähettämiseen.

Kirkossa digitalisaatio tarkoittaa esimerkiksi jumalanpalvelusten striimausta nettiin, sähköistä rippikouluilmoittautumista tai kasteen varausta, chatin kautta tapahtuvaa asiakaspalvelua ja sähköisiä kokouksia.

Hakkeri (hacker)

Hakkerilla on erilaisia merkitystä. Aikaisemmin se on tarkoittanut taitavaa IT-alan osaajaa, mutta nykyisin sillä yleensä viitataan tietojärjestelmiin murtautujaa. Valkohattuhakkeri tai hyvä hakkeri sen sijaan etsii työkseen järjestelmistä aukkoja ja pyrki parantamaan järjestelmien kyberturvallisuutta.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkea tunnistettuun tai tunnistettavissa olevaan henkilöön sisältönsä, merkityksensä tai vaikutuksensa vuoksi liittyvää informaatiota.

Henkilötietoja voivat olla muun muassa henkilön nimi, henkilötunnus, osoite, puhelinnumero, sähköpostiosoite, auton rekisterinumero, kiinteistötunnus ja IP-osoite sekä kyseistä henkilöä koskevat terveystiedot, tulotiedot, hänelle annettuja kirkon palveluja koskevat tiedot ja hänen yksityiselämäänsä koskevat tiedot.

IT-yhteistyöalue eli IT-alue

IT-alue on kahden tai useamman seurakunnan sopimuspohjainen IT-yhteistyöalue. Tästä kirkkolain (652/2023) mahdollistamasta yhteistoiminnasta vastaa IT-alueen tehtävää hoitava seurakunta (isäntäseurakunta) tai Kirkon keskusrahasto. Kirkossa on neljätoista (14) IT-aluetta.

Kirkon yhteiset palvelut

Kirkon keskusrahasto tuottaa seurakunnille ICT-palveluluettelon mukaisesti sekä koko kirkon yhteisiä palveluja että sopimuspohjaisia palveluja. Seurakuntataloudet voivat ottaa käyttöönsä joko yksittäisen palvelun tai palvelukokonaisuuden.

Kyberturvallisuus

Kyberturvallisuus tarkoittaa tiedon, tietojärjestelmien ja tietoteknisten laitteiden ja käyttäjien turvallisuuden takaamiseen tietoverkossa. Tietoturvallisuus kattaa sen sijaan tiedon turvaamisen laajemminkin esimerkiksi paperiarkistossa eli kyberturvallisuus on osa tietoturvallisuutta.

Kyberuhka

Kyberuhalla tarkoitetaan tilannetta, tapahtumaa tai toimintaa, joka voi vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, järjestelmien käyttäjiä tai muulla tavoin vaikuttaa näihin haitallisesti.

Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä tuottaa kyberturvallisuuden valtakunnallista tilannekuvaa Suomessa.

Palomuuri (firewall)

Laite tai ohjelmisto, jonka tarkoitus on estää asiaton pääsy verkosta toiseen, erityisesti Internetistä lähiverkkoon. Lähiverkko voi olla esimerkiksi seurakunnan toimipisteen sisäinen verkko tai valtakunnallinen KIRKKO-verkko.

Pilvipalvelu

Pilvipalvelu on Internetissä toimiva palvelu, kuten sähköposti tai Microsoft Teams -järjestelmä. Ne ovat käytettävissä ajasta, paikasta tai laitteesta riippumatta.

Roskapostinsuodatin

Roskapostinsuodatin poistaa automaattisesti roskapostiksi määritellyt postit sähköposteista tai ohjaa ne työntekijän poistettavaksi tai säilytettäväksi. Roskapostinsuodatin poistaa suurimman osan haitallisista posteista, mutta ei kaikkea. Toisinaan suodatin poistaa myös sellaisia viestejä, joita ei pitäisi poistaa.

Saavutettavuus

Saavutettavuus tarkoitta sitä, että mahdollisimman moni erilainen ihminen voi käyttää digitaalisia palveluja mahdollisimman helposti. Saavutettavuus on ihmisten erilaisuuden ja moninaisuuden huomiointia verkkosivujen ja mobiilisovelluksien suunnittelussa ja toteutuksessa.

Salassapitositoumus (non-disclosure agreement eli NDA)

Salassapitositoumus on dokumentti, jolla sitoudutaan pitämään salassa saamansa luottamukselliset tiedot.

Kirkon salassapitositoumuksessa velvoitetaan työntekijää, luottamushenkilöä, vapaaehtoista tai muuta ulkopuolista tahoa pitämään salassa tehtävässään saamansa luottamukselliset tiedot. Salassapitositoumus on kaikille kirkon eri toimijoille pakollinen, mikäli he käsittelevät tehtävässään luottamuksellista tietoa. Salassapitositoumus allekirjoitetaan ja toimitetaan arkistoitavaksi omaan seurakuntaan.

Tietosuoja

Tietosuoja on perusoikeus, joka turvaa rekisteröidyn eli esimerkiksi seurakuntalaisen oikeuksien ja vapauksien turvaamista henkilötietoja käsiteltäessä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Tietosuoja-asetus

Yleinen tietosuoja-asetus (GDPR eli General Data Protection Regulation) on vuonna 2018 voimaan tullut EU-alueen yhteinen asetus tietosuojan osalta, jota kansallisella tietosuojalainsäädöllä tarkennetaan.

Tietoturva eli tietoturvallisuus

Tietoturva tarkoittaa tiedon turvaamista eri keinoin, kuten toimitilojen tilajärjestelyillä tai tietojärjestelmien teknisillä suojauksilla. Tietoturvan avulla huolehditaan siitä, että tieto on luottamuksellista, eheää ja käytettävissä sekä sähköisesti, että paperitulosteissa.

Tietoturvapolitiikka

Tietoturvapolitiikka on dokumentti, jossa määritellään muun muassa organisaation tietoturvallisuuden organisointi ja tietoturvallisuuden keskeiset linjaukset.

Kirkon tietoturvapolitiikassa on määritelty tietoturvatyön (ja kyberturvallisuuden) organisointi Suomen evankelis-luterilaisessa kirkossa ja tietoturvallisuuden keskeiset linjaukset. Seurakunnan tietoturvapolitiikassa linjataan, miten seurakuntatalouden tietoturvallisuudesta tarkemmin huolehditaan ja mitkä ovat eri toimijoiden roolit, vastuut ja oikeudet. Siinä linjataan myös sisäisen valvonnan järjestäminen tietoturvallisuuden osalta.

Kirkon tietoturvapolitiikkaa täydentävät Kirkon yleiset tietoturvamääräykset.

Tietoturvamääräykset

Kirkon yleisissä tietoturvamääräyksissä on yksityiskohtaisemmin ohjeistettu tietoturvallisuuden (ja kyberturvallisuuden) toteuttamista Suomen evankelis-luterilaisessa kirkossa. Kirkon tietoturvamääräykset ovat salassa pidettävä asiakirja Julkisuuslain (621/1999) mukaisesti.

Toimitusketju

Toimitusketjulla tarkoitetaan tuotteen tai palvelun kokonaisuutta valmistamisesta asiakkaan käyttöön ja mahdollisesti asiakkaan tietojen ja rahojen käsittelyä. Esimerkiksi tuotteen toimitusketjuun voi liittyä jälleenmyyjän lisäksi kuljetusliike, tukkuri ja tehdas. IT-palveluissa toimitusketjut voivat koostua esimerkiksi eri ohjelmistotoimittajista, tietoliikenneoperaattoreista, konesalipalvelujen tarjoajista yms. Kyberturvallisuuden näkökulmasta koko toimitusketjun pitää olla turvallinen.

Vahva tunnistautuminen eli MFA

Vahva tunnistautuminen (MFA eli Multi-Factor Authentication) on yksi tärkeimmistä tavoista parantaa työntekijän kyberturvallisuutta. Käytännössä vahva tunnistautuminen tarkoittaa kirjautumista sähköisiin palveluihin, kuten sähköpostiin, käyttäjätunnuksen ja salasanan lisäksi esimerkiksi puhelinta hyödyntäen.

Virustorjunta (antivirus)

Esimerkiksi tietokoneissa, matkapuhelimissa tai tableteissa olevan ohjelma, jonka tarkoitus on estää ja poistaa virukset ja haittaohjelmat. Tarkistaa myös, onko vierailemasi verkkosivut turvallisia.

Zero Trust

Zero Trust eli ”luottamattomuuden periaate”. Kyberturvallisuudessa lähtökohtana on ajatus, että lähtökohtaisesti mihinkään ei luoteta. Tämä koskee niin tietoliikenneverkkoja, siihen liitettyjä laitteita kuin palvelujen käyttäjiä.

3. KYBERTURVALLISUUS

Sanana kyberturvallisuus tai kyberturva on melko uusi. Eri yhteyksissä sille onkin annettu erilaisia määritelmiä. Se saatetaan ajatella tarkoittavan samaa kuin tietoturvallisuus. Näin ei kuitenkaan ole. Tietoturva turvaa tiedon turvallisuuden sekä verkossa että paperitulosteissa. Kyberturvallisuus on osa tietoturvallisuutta ja siinä keskitytään erityisesti verkkoympäristön ja käyttäjien turvallisuuteen. Kyberturvallisuudesta käytetään myös nimitystä digitaalisen ympäristön turvallisuus tai digitaalinen turvallisuus.

Tässä oppaassa kyberturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla Suomen evankelis-luterilainen kirkko ja sen seurakunnat voivat suojata toiminnassaan käytettävät sähköiset tiedot, järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet sekä niiden käyttäjät kyberuhkilta. Käyttäjät ovat tässä yhteydessä niin kirkon työntekijöitä, luottamushenkilöitä, vapaaehtoisia kuin seurakuntalaisia tai yhteistyökumppaneita.

Kirkolla ja sen seurakunnilla on oikeus käsitellä seurakunnan jäsenten henkilötietoja kirkon hengellisen perustehtävän toteuttamisessa sekä asiakkaiden henkilötietoja lakisääteisten tehtävien hoidossa. Kyberturvallisuus kirkossa tarkoittaa ensisijaisesti näiden sähköisessä muodossa olevien henkilötietojen suojaamista, mutta myös tietojärjestelmien turvallisuutta ja käytettävyyttä. Kyberturvallisuus on osaltaan tietoteknisiä ratkaisuja, mutta suurelta osin myös työkulttuuria, työntekijöiden kouluttamista, viestintää, ennaltaehkäisyä, riskien kartoittamista ja arviointia sekä johtamista. Kyberturvallisuus pitää huomioida niin päivittäisessä seurakuntatyössä kuin laajemmissa kirkon strategisissa linjauksissakin.

Kyberturvallisuuden uhat ovat viime vuosina kasvaneet niin globaalisti kuin Suomen evankelis-luterilaisessa kirkossa. Syynä tähän on, että kyberrikollisuus on valitettavasti tuottoisa bisnes rikollisille. Finanssialan mukaan pelkästään vuoden 2024 ensimmäisellä puoliskolla Suomessa 27,5 miljoonaan euroa päätyi kyberrikollisille. Määrä kasvoi lähes 30 % vuoteen 2023 verrattuna samalla ajanjaksolla. Isoimmat menetykset tulivat tietojenkalasteluhuijauksista, jossa rikollinen sai tietoonsa esimerkiksi uhrin verkkopankkitunnukset. Tiedot ovat peräisin pankeilta kerätyistä tiedoista, joten todellisuudessa määrät voivat olla moninkertaiset. (Finanssiala 2024.)

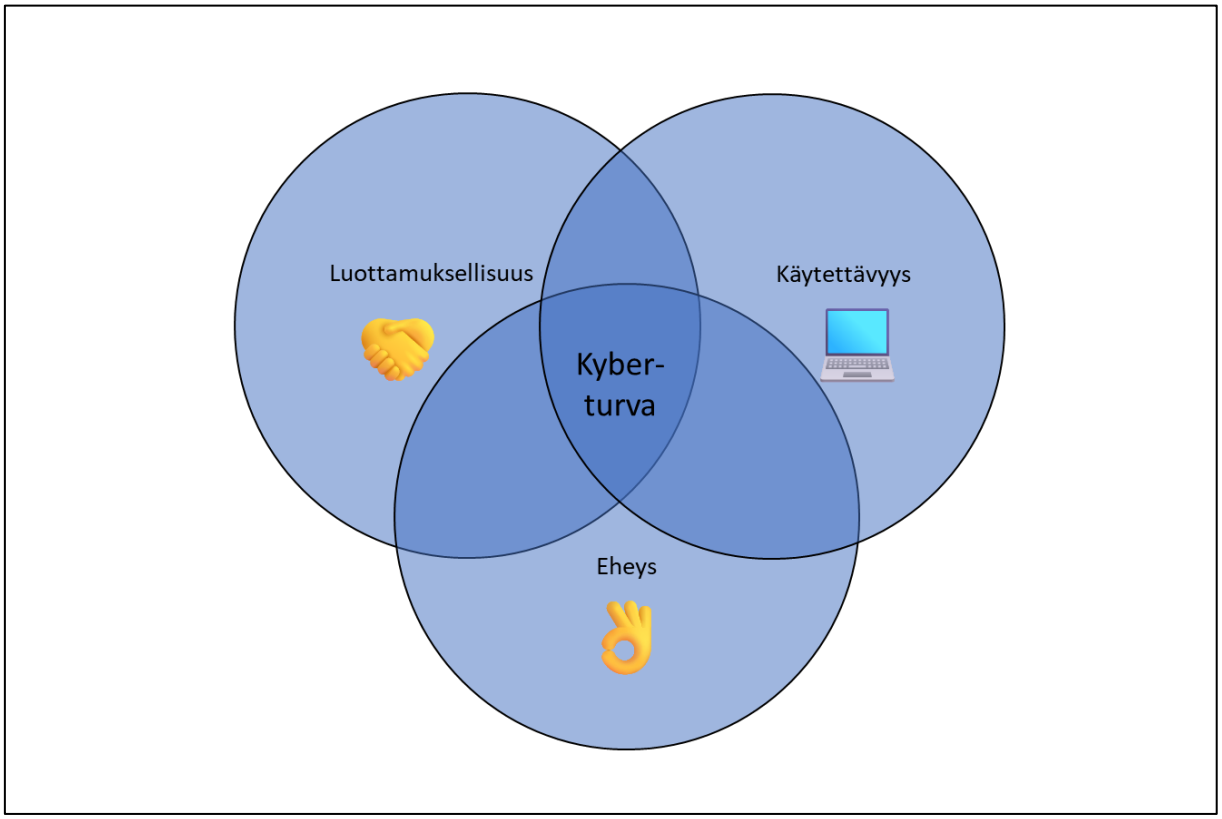
Digitalisaation laajentumisen myötä koko yhteiskuntamme on yhä enemmän riippuvaisia sähköisistä palveluista. Tämä tuo valitettavasti kyberrikollisille yhä enemmän mahdollisuuksia hyökkäyksille. Seurakunnissa esimerkiksi etätyön lisääntyminen on tarkoittanut myös sitä, että kyberturvallisuus pitää ulottaa myös seurakuntien toimipisteiden lisäksi myös etätyöpisteisiin.

Samalla kun kirkko lisää ja kehittää osana yhteiskuntaa sähköisten palvelujen tarjontaa asiakkailleen, myös mahdollisten hyökkäyskohteiden määrä kirkossa kasvaa. Esimerkiksi vuonna 2022 kansainvälisen tilanteen muuttuminen Ukrainan sodan myötä on lisännyt yleisesti ottaen Suomessa kyberuhkien riskiä ja edellyttänyt eri toimijoita entistä parempaan varautumiseen niitä vastaan. Näin on tehty myös Suomen evankelis-luterilaisessa kirkossa.

Lähtökohta kyberturvallisuudessa on Zero Trust eli luottamattomuuden periaate tai nollaluottamusmalli. Siinä kantava ajatuksena on, että mihinkään ei lähtökohtaisesti luoteta ja kaikkeen pitää vähintäänkin suhtautua epäilevästi. Tämä koskee niin tietoliikenneverkkoja, sähköisiä palveluja, verkkoon liitettyjä laitteita kuin palvelujen käyttäjiä. Samalla kirkolta ja muilta julkisen sektorin toimijoilta kuitenkin edellytetään avoimuutta toiminnassaan sekä helppokäyttöisiä ja saavutettavia sähköisiä palveluja, joita kaikkien on mahdollista käyttää.

3.1. Kyberturvallisuuden CIA-malli

Tietoturvallisuus koostuu tiedon käytettävyydestä, eheydestä ja luottamuksellisuudesta. Tietoturvallisuuden yhteydessä puhutaan myös CIA-mallista. CIA-lyhenne muodostuu englannin kielen sanoista confidentiality, integrity ja availability. CIA-mallilla voidaan kuvata myös kyberturvallisuutta. (Microsoft 2020.)



Kuva 1 Kyberturvallisuuden CIA-malli

Luottamuksellisuus (confidentiality) tarkoittaa sitä, että kukaan sivullinen ei saa tietoa tai ei voi käsitellä sitä. Tiedot ovat siis vain niiden käyttöön oikeutettujen saatavilla. Luottamuksellisuuden suurin uhka on kyberrikollisuus eri muodoissa.

Eheys (integrity) tarkoittaa sitä, että tieto on yhdenmukaista alkuperäisen tiedon kanssa. Eheyttä uhkaavat muun muassa inhimilliset virheet tai väärinkäsitykset tietokoneohjelmien rakentamisessa tai tietojen tallennuksessa. Eheyttä uhkaavat myös esimerkiksi rikollisten tarkoituksellisesti tekemät tietojen muuttamiset esimerkiksi rahaliikenteen käsittelyssä.

Käytettävyys (availability) tarkoittaa sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Käytettävyyttä uhkaavat muun muassa laitteiden, tietoliikenneverkkojen ja tietokoneohjelmien vikaantumiset sekä kyberrikollisten tekemät palvelunestohyökkäykset. Vikaantumiset voivat aiheutua esimerkiksi jonkin teknisen komponentin vikaantumisesta tai käyttäjän tekemästä inhimillisestä virheestä.

3.2. Kyberturvallisuus ja lainsäädäntö

Suomen evankelis-luterilaisen kirkon ja sen seurakuntien toimintaa säätelevät monet lait. Lainsäädännössä ohjeistetaan ja määrätään myös seurakuntien tietoturvallisuuden (ja kyberturvallisuuden) järjestämistä eri tavoin. Tietoturva on mainittu muun muassa kirkkolaissa (652/2023), tiedonhallintalaissa (906/2019), digipalvelulaissa (306/2019), valmiuslaissa (1552/2011) sekä EU:n yleisessä tietosuoja-asetuksessa (GDPR). Tietosuoja-asetuksen ja kansallisen tietosuojalain (1050/2018) lisäksi henkilötietojen käsittelystä on säädetty erikseen muun muassa laissa uskontokuntien jäsenrekistereistä (614/1998) sekä diakoniatyössä käsiteltävistä henkilötiedoista asiakaslaissa (703/2023).

Heinäkuussa 2023 voimaan tullut uudistettu kirkkolaki (652/2023) toi seurakunnille uusia lakisääteisiä velvoitteita tietoturvallisuuden osalta. Uuden kirkkolain myötä jatkossa kirkkoon sovelletaan soveltuvin osin tiedonhallintolakia. Lain mukaan tiedonhallintayksikön, kuten seurakunnan, on muun muassa selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Uudistettu kirkkolaki ottaa kantaa myös sähköisen kokouksen ja päätöksentekomenettelyn tietoturvallisuuteen. Lain mukaisesti seurakunnan, tuomiokapitulin tai kirkkohallituksen tulee huolehtia tietoturvallisuudesta ja siitä, että salassa pidettävät tiedot eivät ole ulkopuolisen saatavissa sähköisessä kokouksessa tai sähköisessä päätöksentekomenettelyssä. Sähköinen päätöksentekomenettely tarkoittaa tässä yhteydessä ajasta ja paikasta riippumatonta päätöksentekoa ennen varsinaista kokousta siihen tarkoitetussa tietojärjestelmässä.

Kirkkolain mukaisesti myös seurakunnan, hiippakunnan ja kirkkohallituksen tulee valmiussuunnittelulla ja sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. Tuomiokapituli johtaa ja valvoo hiippakunnan seurakuntien varautumista. Kirkkohallitus johtaa kirkon keskushallinnon varautumista.

Kirkon viranomaisten tiedonhallintaan, tietojärjestelmien käyttöön sekä tietojen sähköiseen luovutustapaan sovelletaan tiedonhallintalain 4 §:n 2 momenttia, jonka mukaisesti tiedonhallintayksiköllä (seurakunta, tuomiokapituli ja kirkkohallitus) on oltava ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta. Sama laki myös ohjeistaa tietojärjestelmien käyttöoikeuksien hallinnasta ja lokitietojen keräämisestä sekä asiarekisteristä.

Kirkkolain mukaisesti kirkkohallitus vastaa jäsenrekisteri Kirjurin tietoturvallisuudesta ja antaa tarkempia määräyksiä sen tietoturvallisuudesta. Kirjurissa on perustiedot jokaisesta seurakunnan jäsenestä sekä häntä koskevat kirkolliset toimitukset, kuten kaste, vihkiminen ja hautaaminen. Kirjurin jäsentietojen tietoturvasta ja henkilötietojen käsittelystä on tarkemmin ohjeistettu muun muassa kaikkia kirkon toimijoita velvoittavissa Kirkon yleisissä tietoturvamääräyksissä sekä kirkkohallituksen Virastonhoidon ohjeissa (2019).

Hallintolaissa (434/2003), joka myös kirkkoa osaltaan koskee, säädetään hyvän hallinnon perusteista ja hallintoasioiden käsittelystä. Tietoturvallisuutta ja kyberturvallisuutta voidaan pitää osana hyvää hallintotapaa.

EU:n yleisen tietosuoja-asetuksen soveltaminen alkoi vuonna 2018 kaikissa EU-maissa. Kansallinen tietosuojalaki astui voimaan 1.1.2019. Tietosuojalailla (1050/2028) täsmennetään ja täydennetään tietosuoja-asetusta. Rekisterinpitäjän eli esimerkiksi seurakunnan tulee toteuttaa tarvittavat tekniset ja hallinnolliset toimenpiteet, joilla varmistetaan ja osoitetaan tietosuojalainsäädännön noudattaminen. Tekniset toimenpiteet voivat tarkoittaa kyberturvallisuuden osalta esimerkiksi niitä toimenpiteitä, joilla tietojärjestelmät tai tietoliikenneverkot suojataan kyberrikollisuudelta.

Tietosuojalaissa määritellyt seuraamusmaksut tietosuoja-asetuksen rikkomisesta eivät tällä hetkellä koske julkista hallintoa tai evankelis-luterilaista kirkkoa. Ne koskevat yrityksiä ja voivat olla suuruudeltaan enintään 4 % liikevaihdosta tai 20 miljoonaa euroa. Nykyisessä Petteri Orpon hallitusohjelmassa tietosuojalainsäädäntöä ollaan uudistamassa ja muun muassa seuraamusmaksut tietosuojaloukkauksista ollaan säätämässä koskemaan julkista ja yksityistä sektoria yhtäläisesti. (Valtioneuvosto, 2023.)

Lisäksi kirkkoa koskevat muun muassa laki yksityisyyden suojasta työelämässä (759/2004) ja julkisuuslaki (621/1999). Kummassakin näissä on viittauksia henkilötietojen käsittelyyn, tietosuojaan tai tietoturvallisuuteen.

EU:n yleisen tietosuoja-asetuksen lisäksi Euroopan unionin laajuinen kyberturvallisuusdirektiivi on tulossa voimaan. NIS2-kyberturvallisuusdirektiivi on EU:n laajuinen kyberturvallisuutta koskeva lainsäädäntö, jonka tavoitteena on parantaa EU:n kyberturvallisuuden yleistä tasoa. Direktiiviä täydennetään kansallisella lainsäädännöllä, jota ollaan Suomessa parhaillaan valmistelemassa. Kansallisen lainsäädännön on tarkoitus astua voimaan syksyllä 2024. NIS2-direktiivi koskee valtion toiminnan kannalta kriittisiä toimialoja, kuten pankkeja, terveydenhuoltoa ja energia-alaa sekä tietoliikenneoperaattoreita tai suurimpia pilvipalvelujen tarjoajia. (Valtioneuvosto, 2022.)

Jatkossa näillä toimialoilla toimivien yritysten ja julkishallinnon toimijoiden pitää 24 tunnin kuluessa raportoida viranomaiselle havaitsemistaan tietoturvapoikkeamista. Myös mahdolliset seuraamusmaksut tietoturvapoikkeamissa ovat mahdollisia, mikä he eivät ole toteuttaneet kyberturvallisuusdirektiivin edellyttämiä toimenpiteitä, kuten kyberriskien hallintaa tai johdon koulutusvelvoitteita. (Valtioneuvosto, 2022.) Direktiivi ei koske suoraan kirkkoa tai sen seurakuntia, mutta se voi mahdollisesti tuoda uusia velvoitteita tai kyberturvakäytäntöjä myös seurakunnille näiden kriittisten palveluiden käyttäjänä tai yleisen tietoturva-, tietosuoja- ja/tai kyberturvalainsäädännön tai suositusten muuttuessa.

4. KYBERTURVALLISUUDEN ROOLIT JA VASTUUT KIRKOSSA

Suomen evankelis-luterilaisen kirkon tietoturvapolitiikassa (2022a) ja yleisissä tietoturvamääräyksissä (2022b) on määritelty kirkon tietoturvatyön roolit ja vastuut. Seurakunnilla tai seurakuntien eri työaloilla voi olla lisäksi omia tarkentavia ohjeita tietoturvallisuuteen ja kyberturvallisuuteen sekä niiden organisointiin ja vastuisiin. Nämä eivät kuitenkaan saa olla ristiriidassa kirkon yleisten tietoturvamääräysten tai voimassa olevan (tietoturva)lainsäädännön kanssa.

Kirkon ohjeissa ei oteta suoraan kantaa kyberturvallisuuteen, mutta roolit ja tehtävät on määritelty tietoturvallisuuden kautta. Kirkon tietoturvapolitiikan mukaisesti seurakunnissa pitää olla esimerkiksi nimettynä tietoturvan yhdyshenkilö(t). Hänellä pitää olla tarvittavat resurssit hoitaa kyseistä tehtävää. Yhdyshenkilön tehtävänä on tiedottaa seurakunnan työntekijöitä tietoturvallisuuteen ja kyberturvallisuutteen liittyvistä asioista ja olla esihenkilöiden tukena tietoturva-asioiden perehdyttämisessä.

Seurakunnan johdolla ja esihenkilöillä on viime kädessä vastuu seurakunnan kyberturvallisuudesta ja sitä kautta kokonaiskirkon kyberturvallisuudesta. Vastuuhenkilöiden tietoturvallisuuden liittyvät tehtävät pitää olla määriteltynä myös kyseisten henkilöiden tehtävänkuvissa.

Tietoturvan yhdyshenkilön ja seurakunnan johdon lisäksi tietoturvallisuus ja kyberturvallisuus on viime kädessä jokaisen kirkon työntekijän vastuulla. Työntekijöiden pitää tuntea Suomen evankelis-luterilaisen kirkon yleinen tietoturvaohjeistus sekä mahdolliset oman seurakunnan ja/tai IT-alueen tarkentavat ohjeet sekä noudattaa niitä työssään. Mikäli työntekijä havaitsee työssään puutteita tai poikkeamia tietoturvassa, on hän niistä myös velvollinen raportoimaan eteenpäin.

Liitteessä 1 on kuvattu yleisellä tasolla kirkon tietoturvallisuuden johtamisjärjestelmä. Kirkon tietoturvapolitiikan ja kirkon tietoturvamääräysten mukaisesti tietoturvan roolit, tehtävät ja vastuut ovat määritelty seuraavasti kirkossa:

Kirkolliskokous

Linjaa kokonaiskirkon ja seurakuntien tietoturva-asioita seuraavissa yhteyksissä:

- Kirkolliskokous tekee ehdotuksia eduskunnalle kirkkolain säätämisestä ja hyväksyy kirkkojärjestyksen. Näissä säädöksissä on myös tietoturvaa koskevia säännöksiä.
- Tietoturva-asioiden hoitamisessa on otettava huomioon yleinen lainsäädäntö, joka sisältää tietoturvallisuutta koskevia säännöksiä ja joka kirkkolain perusteella tai muutoin välittömästi koskee myös kirkollishallintoa.
- vahvistaa Kirkon keskusrahaston talousarvion ja käsittelee toiminta- ja taloussuunnitelman. Nämä sisältävät myös kokonaiskirkon tietoturvallisuuden kehittämiseen liittyviä asioita.

Kirkkohallituksen täysistunto ja virastokollegio

Kirkkohallituksen täysistunnon tehtävänä on

- asettaa **kirkon tietoturvan johtoryhmä**
- antaa kirkon tietoturvamääräykset.

Kirkkohallituksen virastokollegion tehtävänä on

- nimittää **kirkon tietoturvapäällikkö**
- antaa yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä sellainen kirkon tietoturvamääräys, joka on voimassa enintään neljä (4) kuukautta
- antaa kirkon tietoturvamääräyksiä täydentäviä yleisiä tietoturvaohjeita ja suosituksia sekä työalakohtaisiin tietojärjestelmiin ja perustietotekniikkaan liittyviä erityisiä tietoturvaohjeita.

Kirkon tietoturvapäällikkö

Kirkkohallituksen virastokollegion nimittämän kirkon tietoturvapäällikön tehtävänä on

- vastata KIRKKO-verkon ytimen ylläpidosta ja tietoturvallisuudesta
- toimia KIRKKO-verkon ytimen yhteisötilaajan vastuuhenkilönä, jolla on oikeus käsitellä tarpeellisia tunnistetietoja
- oikeus ryhtyä välittömiin suojelutoimenpiteisiin Suomen lainsäädännön määrittelemissä puitteissa
- nimetä yksittäistapauksessa tunnistamistietojen käsittelyssä mukana olevat henkilöt kirjallisesti etukäteen ja raportoita ilman aiheetonta viivytystä käsitellyistä tunnistetiedoista kirkkohallituksen tietohallintojohtajalle
- valmistella yllättävän tietoturvauhan tai poikkeamatilanteen yhteydessä tilapäisen tietoturvamääräyksen Kirkkohallituksen **virastokollegion** päätettäväksi
- vastata tietoturva-asioiden tiedottamisesta tai sen järjestämisestä seurakunnille sekä tiedotusvälineille ja muille kirkon ulkopuolisille tahoille
- järjestää seurakuntien toimittamien tietoturvallisuutta koskevien arviointi- ja tapahtumaraporttien vastaanoton ja käsittelyn
- koordinoida IT-alueiden välistä tietoturvatyötä.

Kirkon tietoturvan johtoryhmä

Kirkkohallituksen täysistunnon asettaman kirkon tietoturvan johtoryhmän tehtävänä on

- seurata tietoturvallisuuden tilannetta ja kehittämistarpeita koko kirkossa
- valmistella esityksen kirkon tietoturvapolitiikasta ja sen päivittämisestä
- valmistella esityksen kirkon yleisistä tietoturvamääräyksistä ja niiden päivittämisestä
- valmistella kirkon tietoturvapolitiikkaa ja yleisiä tietoturvamääräyksiä täydentäviä yleisiä ohjeita ja suosituksia
- ohjata ja tukea kirkon tietoturvapolitiikan, tietoturvamääräysten ja tietoturvaohjeiden koulutuksen järjestämistä ja muuta jalkautusta
- tehdä aloitteita työalakohtaisia tietojärjestelmiä ja niiden toimintoja tai perustietotekniikan eri osa-alueita koskettavien tarkempien tietoturvamääräysten ja -ohjeiden laatimisesta ja toimia yhteistyössä näiden laatimisprojektien kanssa

Seurakunta ja seurakunnan kirkkoneuvosto

Seurakunnalla tarkoitetaan tässä yhteydessä seurakuntataloutta, tuomiokapitulia tai kirkkohallitusta. Seurakunnan tehtäviä tietoturvallisuuden osalta on

- noudattaa tietoturvallisuutta koskevia määräyksiä ja ohjeita
- ylläpitää valmiussuunnitelmaa ja testata sen toimivuutta säännöllisesti.
- tuntea toimintaansa sääntelevät lait ja muut säädökset ja määräykset
- on rekisterinpitäjänä vastuussa henkilötietojen käsittelystä ja tietoturvan tasosta henkilörekistereissä.

Kirkkoneuvostolla tarkoitetaan tässä yhteydessä seurakunnan kirkkoneuvostoa tai seurakuntayhtymän yhteistä kirkkoneuvostoa. Kirkkoneuvoston tehtävänä on

- vastata **seurakuntataloudelle** annettujen tietoturvallisuutta koskevien määräysten ja ohjeiden noudattamisesta
- huolehtia, että seurakuntataloudelle on asetettu **tietoturvaryhmä**. Ryhmän on tarkoituksenmukaista olla yhteinen IT-alueen kaikkien seurakuntien kanssa
- huolehtia, että seurakuntataloudelle on nimetty **tietoturvavastaava**. Sen on tarkoituksenmukaista olla yhteinen IT-alueen kaikkien seurakuntien kanssa
- huolehtia, että seurakuntataloudelle on nimetty yksi tai useampia **tietoturvan yhdyshenkilöitä** siten, että kukin seurakuntatalouden työntekijä tuntee oman yhdyshenkilönsä
- hyväksyä seurakunnan tietoturvapolitiikka. Sen on järkevää olla yhteinen IT-alueen kaikkien seurakuntien kanssa. Siinä linjataan, miten seurakuntatalouden tietoturvallisuudesta tarkemmin huolehditaan ja mitkä ovat eri toimijoiden roolit, vastuut ja oikeudet. Siinä linjataan myös sisäisen valvonnan järjestäminen tietoturvallisuuden osalta.

Seurakunnan tietoturvan yhdyshenkilö

Kirkkoneuvosto huolehtii siitä, että seurakuntataloudelle on nimetty yksi tai useampia **tietoturvan yhdyshenkilöitä**. Seurakunnan tietoturvan yhdyshenkilön tehtävänä on

- huolehtia saamiensa tietoturvallisuuteen liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta kaikille työntekijöille.
- osallistua esihenkilöiden tukena uusien työntekijöiden perehdyttämiseen tietoturvallisuutta koskevissa kysymyksissä.
- ottaa vastaan ilmoituksia seurakunnassaan havaituista tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoida niistä IT-alueen **tietoturvavastaavalle** sekä oman seurakuntansa **esihenkilöille**.

IT-aluekeskus (IT-alueen isäntäseurakunta)

IT-aluekeskus hoitaa käytännön IT-asioita omalla IT-alueellaan. Sitä johtaa IT-alueen **tietohallintopäällikkö** tai vastaava viranhaltija. IT-aluekeskuksella tarkoitetaan IT-alueen isäntäseurakunnassa tai Kirkon keskusrahastossa toimivaa teknisen tuen yksikköä. IT-aluekeskuksen tehtävänä on

- vastata tietoturvapolitiikan ja tietoturvamääräysten täyttymisen omalta osaltaan IT-alueen seurakunnissa (KIRKKO-verkko ja siihen liitetyt laitteet ja palvelimet)
- varata riittävästi ammattitaitoista henkilöstöä, jotta turvallisuusvaatimusten käytännön toteuttaminen on realistisesti mahdollista ottaen huomioon mm. henkilöstön lomat ja muut poissaolot.
- velvollisuus auditoida säännöllisesti tietoturvan tason.

IT-alueen tietohallintopäällikkö

IT-alueen tietohallintopäällikön tehtävänä on

- vastata IT-alueen oman alueverkon tietoturvallisuudesta
- vastata tietoturvallisuuden toteuttamisen edellyttämistä käytännön toimista omalla IT-alueellaan kirkon tietoturvapolitiikan, yhteisten tietoturvamääräysten ja seurakunnan kirkkoneuvoston tai seurakuntayhtymän yhteisen kirkkoneuvoston päätösten pohjalta

IT-alueen/seurakuntatalouden tietoturvaryhmä

Seurakunnan kirkkoneuvosto huolehtii siitä, että IT-alueella on tietoturvaryhmä. Sen kokoonpano ja toimikausi voi vaihdella IT-alueittain ja siihen voi kuulua IT-alueeseen kuuluvien seurakuntien työntekijöitä ja luottamushenkilöitä. Pääsääntöisesti IT-alueen tietoturvaryhmän nimittää IT-alueen isäntäseurakunta. Tietoturvaryhmän tehtävänä on

- ylläpitää IT-alueen seurakuntatalouksien tietoturvapolitiikan ja tietoturvallisuuteen liittyviä määräyksiä, ohjeita ja suosituksia siten, että ne ovat linjassa kirkon yhteisen tietoturvapolitiikan ja kirkon yhteisten tietoturvamääräysten kanssa
- valvoa tietoturvamääräysten, ohjeiden ja suositusten noudattamista
- käsitellä ajankohtaisia tietoturvallisuutta koskevia kysymyksiä
- suunnitella ja järjestää tietoturvallisuuteen liittyvää koulutusta yhteistyössä **IT-alueen tietoturvavastaavan** ja seurakuntien **tietoturvan yhdyshenkilöiden** kanssa.

IT-alueen tietoturvavastaava

IT-alueen tietoturvavastaava työskentelee IT-alueen IT-aluekeskuksessa. Tietoturvavastavan nimittää pääsääntöisesti IT-alueen isäntäseurakunta. Tietoturvavastaavan tehtävänä on

- kehittää jatkuvasti ja aktiivisesti IT-alueen seurakuntien tietoturvallisuutta
- vastata tietoturvallisuuteen liittyvien ohjeiden, suositusten ja määräysten tiedottamisesta tietoturvan yhdyshenkilöille, esihenkilöille ja kaikille työntekijöille
- ottaa vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja poikkeamista ja raportoi ne säännöllisesti IT-alueen **tietoturvaryhmälle** ja kirkon **tietoturvapäällikölle**
- osallistua kirkon tietoturvapäällikön koordinoimaan IT-alueiden väliseen tietoturvatyöhön.

Esihenkilö

Esihenkilön tehtävänä on

- välittää tietoa tietoturvallisuuteen liittyvistä määräyksistä, ohjeista ja suosituksista omille työntekijöilleen
- järjestää uusien työntekijöiden perehdytys tietoturvallisuuden määräyksistä, ohjeista ja suosituksista ja on velvollinen huolehtimaan siitä, että työntekijät ovat tiedostaneet ja oppineet kyseiset asiat
- huolehtia, että työntekijät noudattavat annettuja määräyksiä ja ohjeita
- on velvollinen tilaamaan alaisilleen tarpeelliset tunnukset sekä käyttöoikeudet seurakunnan käyttämiin tietojärjestelmiin
- vastata omien työntekijöidensä osalta siitä, että tietojärjestelmien käyttöoikeudet vastaavat työtehtävien tarpeita
- huolehtia tarpeettomien tunnusten poistamisesta ajallaan.
- järjestää omaa toimialaansa koskevien tietoturvamääräysten ja -ohjeiden laatimisen, jos asioita ei ole vielä ohjeistettu
- puuttua kaikkiin tietoturvaa koskettaviin havaitsemiinsa epäkohtiin
- ottaa työntekijöiltään vastaan havaintoja tietoturvallisuuteen liittyvistä tapahtumista ja (tietoturva)poikkeamista ja raportoi ne seurakunnan **tietoturvan yhdyshenkilölle** ja IT-alueen **tietoturvavastaavalle**

Työntekijä

Työntekijällä tarkoitetaan tässä yhteydessä kirkon kaikkia työntekijöitä, luottamushenkilöitä, vapaaehtoistyöntekijöitä tai ostopalveluna hankittuja työntekijöitä. Jokaisen kirkon työntekijän vastuulla on

- tuntea seurakuntansa **tietoturvan yhdyshenkilö**
- perehtyä häntä koskeviin tietoturvamääräyksiin ja ohjeisiin ja noudattamaan niitä päivittäisessä työssään sekä muutoinkin toimimaan huolellisesti erityisesti henkilötietoja käsitellessään
- osallistua tietoturvallisuuteen liittyviin säännöllisiin koulutuksiin
- raportoida **esihenkilölleen** ja seurakunnan **tietoturvan yhdyshenkilölle** sekä IT-alueen **tietoturvavastaavalle** havaitsemansa tietoturvallisuuteen liittyvät epäkohdat ja (tietoturva)poikkeamat
- vastata käytössään olevista laitteista, käyttöoikeuksista ja tiedoista sekä vastata huolimattomuudestaan johtuvista seurauksista

Muut tietoturvallisuuden ja kyberturvallisuuden roolit ja tehtävät

Kirkkohallituksen tietohallintoyksikkö toimii Suomen evankelis-luterilaisen kirkon evl.fi-tenantin eli teknisen ICT-ympäristön omistajana. Tietohallintoyksikkö vastaa kirkon yhteisen tenantin kyberturvallisuudesta ja sen kehittämisestä. Kirkkohallituksen tietohallintoyksikkö vastaa myös lukuisista kirkon yhteisistä palveluista, kuten Microsoft M365-palvelut ja infrapalvelut. Kirkon Digiverkosto eli digitalisaation ja projektihallinnan verkosto tarjoaa kirkon henkilöstölle tietoa digitalisaatioon ja projektihallintaan liittyvissä asioissa sekä järjestää muun muassa kyberturvallisuuteen liittyviä tietoiskuja.

Kirkkohallituksen virastokollegion nimeämän **Kirkon tietohallinnon johtoryhmän** tehtävänä on selvittää ja arvioida nykyisen kirkon tietohallinnon kokonaiskuva, laatia toimenpide-ehdotuksia, seurata käynnistettyjen kehitysehdotusten etenemistä, seurata ICT-palveluiden palvelutasoa, seurata ICT-kustannuksia, koordinoida yhteisten ICT-toimintojen viestintää ja laatia kannanottoja, jotka vaikuttavat ICT-palveluiden tuottamiseen kirkossa. Johtoryhmän puheenjohtaja on Kirkkohallituksen tietohallintojohtaja ja siihen kuuluvat IT-alueiden tietohallintopäälliköitä ja kirkkohallituksen tietohallintoyksiköstä tietojärjestelmäpäällikkö. ICT-hankkeisiin liittyy vahvasti myös tietoturvallisuus, joten johtoryhmän tehtävä on osaltaan ottaa kantaa myös hankkeiden tietoturvallisuuteen ja kyberturvallisuuteen.

Suomen evankelis-luterilaisen kirkon tulee turvata kaikissa tilanteissa hengellisen elämän hoito ja hengellinen toiminta sekä huolehtia seurakunnan palveluista. Valmius toimia häiriötilanteissa rakennetaan normaalioloissa. Kyberturvallisuuteen liittyy osana myös häiriö- ja poikkeusolot, näihin varautuminen sekä kyberuhkien kartoittaminen ja arviointi. Tämän vuoksi seurakuntien, tuomiokapitulien ja kirkkohallituksen **valmiusryhmillä** on merkittävä rooli myös kyberturvallisuudessa. Tarkemmin seurakunnan valmiussuunnittelusta ja seurakunnan valmiusryhmästä on ohjeistettu Seurakunnan valmiussuunnitelman laatimisohjeessa. (Suomen ev.lut. kirkko, 2019.)

Seurakunnan valmiussuunnitteluun, tietosuojaan ja tietoturvallisuuteen otetaan kantaa myös **piispantarkastuksessa**. Piispantarkastuksen käydään läpi seurakunnan valmiussuunnittelua ja henkilötietojen käsittelyä sekä tietoturvallisuutta muun toiminnan ohella. Tarkastettavia asioita ovat muun muassa, kuinka henkilötietoihin liittyvät tietoturvaloukkaukset on hoidettu ja mitä niistä on opittu. Tarkastuksessa käydään myös läpi, kuinka seurakunnassa noudatetaan kirkon yleisiä tietoturvamääräyksiä. (Suomen ev.lut. kirkko, 2024b.)

Tietosuojatyön roolit ja tehtävät

Seurakunnan kirkkoneuvosto nimeää seurakunnan **tietosuojan yhdyshenkilön** tai tietosuojaryhmän sekä tietosuojalainsäädännön edellyttämän **tietosuojavastaavan**. Yhdellä tai useammalla seurakunnalla voi olla yhteinen tietosuojavastaava.

Seurakunnan tietosuojan yhdyshenkilö

Seurakunnan tietosuojan yhdyshenkilön tai seurakunnan tietosuojaryhmän tehtävänä on

- huolehtia tietosuojaan liittyvien määräysten ja -ohjeiden tiedottamisesta kaikille työntekijöille
- osallistua **esihenkilöiden** tukena uusien työntekijöiden perehdyttämiseen tietosuojaa koskevissa kysymyksissä
- ottaa vastaan ilmoituksia seurakuntataloudessaan havaituista tietosuojaan liittyvistä tapahtumista ja poikkeamista ja raportoida niistä tietosuojavastaavalle ja oman seurakuntataloutensa esihenkilöille.
- toimia yhteyshenkilönä seurakunnan ja **tietosuojavastaavan** välillä.

Tietosuojavastaava

Jokaisella seurakunnalla pitää olla nimettynä EU:n tietosuoja-asetuksen edellyttämä tietosuojavastaava. Seurakunnat voivat nimittää yhteisen tietosuojavastaan. Tietosuojavastaavan tehtävänä on

- neuvonta ja valvonta
- toimia rekisteröidyn eli henkilön, jonka henkilötietoja seurakunnan rekistereissä on, yhteyshenkilönä tietosuojaan liittyvissä kysymyksissä
- toimia tietosuojavaltuutetun toimiston yhteyshenkilö ja tehdä yhteistyötä tietosuojavaltuutetun toimiston kanssa.

Tehtävänimikkeestä huolimatta, tietosuojavastaava ei ole vastuussa seurakunnan henkilötietojen käsittelystä tai käsittelyn lainmukaisuudesta. Tämä vastuu kuuluu seurakunnalle itselleen ja erityisesti sen johdolle. Tietosuojavaltuutetun toimisto on julkaissut ohjeen tietosuojavaltuutetun nimittäneelle organisaatiolle ja sen johdolle, jossa ohjeistetaan tarkemmin tietosuojavastaavan tehtävistä ja asemasta organisaatiossa (Tietosuojavaltuutetun toimisto, 2024.). Ohjeeseen on seurakuntienkin hyvä tutustua ja se löytyy tietosuojavaltuutetun toimiston verkkosivuilta osoitteesta https://tietosuoja.fi/-/julkaisimme-paivitetyt-ohjeet-tietosuojavastaavan-nimittaneelle-organisaatiolle.

Tarkemmin kirkon tietosuojatyöstä on kerrottu lisää kirkon tietoturvapolitiikassa, tietoturvamääräyksissä sekä vuonna 2021 ilmestyneessä Tietosuoja seurakunnassa –oppaassa. Päivitetty versio oppaasta on tarkoitus julkaista vielä vuoden 2024 aikana huomioiden muun muassa uusi kirkkolaki. Opas on ladattavissa veloituksetta Kirkon julkaisut -verkkopalvelusta osoitteessa https://julkaisut.evl.fi.

5. KYBERUHAT

Tässä luvussa esitellään erilaisia kyberuhkia eli tilanteita, tapahtumia tai toimintaa, jotka voivat vahingoittaa tai häiritä verkko- ja tietojärjestelmiä, järjestelmien käyttäjiä tai muulla tavoin vaikuttaa näihin haitallisesti. EU:n kyberturvallisuusviraston (2022) mukaan suurimmat kyberuhat Euroopassa ovat kyberrikollisuus eri muodoissa:

- kiristysohjelmahyökkäykset
- palvelunestohyökkäykset
- haittaohjelmat
- käyttäjän manipulointi
- dataan kohdistuvat hyökkäykset
- Internetiin kohdistuvat hyökkäykset
- Disinformaatio – misinformaatio
- Toimitusketjuun kohdistuvat hyökkäykset

Kiristysohjelmahyökkäysten kautta varastetaan yli 10 teratavua dataa kuukausittain. Tällaisten hyökkäysten yleisimpänä alkutekijänä on tietojenkalastelu eri tavoin. Kyberrikollisuuden vuosittaisen kustannuksen maailmantaloudelle on arvioitu saavuttaneen vuoden 2020 loppuun mennessä 5,5 biljoonaa euroa. Tämä on kaksinkertainen määrä vuoden 2015 arvioon verrattuna. (EU:n kyberturvallisuusvirasto 2022.)

Samat kyberuhat uhkaavat myös Suomen evankelis-luterilaista kirkkoa. Ensisijaisesti kyberrikollisuus eri muodoissa, mutta myös järjestelmien vikaantuminen tai työntekijöiden inhimilliset virheet. Toteutuessaan kyberuhat voivat aiheuttaa merkittäviä taloudellisia ja toiminnallisia vahinkoja kirkolle ja sen seurakunnille. Taloudellisten ja toiminnallisten vahinkojen lisäksi mainehaitta kirkolle voi tietosuojan, tietoturvallisuuden tai kyberturvallisuuden vaarantuessa olla merkittävä. Mainehaitta taas voi johtaa seurakunnan jäsenten eroamiseen kirkosta, jolloin vaikutukset ovat myös taloudellisia.

5.1. Kyberrikollisuus

Kyberrikollinen voi olla yksittäinen henkilö tai kansainvälisen rikollisjärjestön tai valtiollisen toimijan tukema. Kyberrikollisuudessa maantieteellisillä rajoilla ei ole juurikaan merkitystä. Rikollinen voi iskeä Suomesta tai ulkomailta. Yhteistä näille tietomurroille tai niiden yritykselle on kuitenkin se, että tarkoituksena on viime kädessä taloudellinen hyöty. Myös mainehaitan tuottaminen - erityisesti kirkolle, voi olla motiivina tällä rikolliselle toiminalle.

Toisaalta uhan voi myös aiheuttaa alan osaaja tai opiskelija, joka haluaa esimerkiksi testata (kirkon) tietojärjestelmien suojausta. Hän voi ymmärtämättömyyttään ilman taloudellisen hyödyn tavoittelukin aiheuttaa kirkolle merkittävät toiminalliset ja taloudelliset vahingot järjestelmiin murtautumisella. Riippumatta motiivista tai tekijästä, uhkiin pitää suhtautua samalla tavalla.

Suomessa tietomurto on rikoslaissa (39/1889) määritelty rangaistava teko ja myös tietomurron yritys on rangaistavaa. Sisäministeriön mukaan suurin osa kyberrikollisuudesta jää tulematta poliisin tietoon ja rikokset, joista poliisi käynnistää esitutkinnan, jäävät usein selvittämättä tai selviävät vain osittain.

Tietojenkalastelu eli phishing

Rikolliset pyrkivät tietojenkalastelun avulla saamaan käyttöönsä (kirkon) työntekijöiden käyttäjätunnuksia ja salasanoja tai muita henkilötietoja. Tällöin puhutaan myös identiteettivarkaudesta.

Tietojenkalastelu tapahtuu pääasiassa sähköpostin välityksellä, mutta myös puhelimitse ja tekstiviestein. Yleensä viestit sisältävät linkkejä verkkosivuille, joihin pyydetään kirjautumaan. Näillä luotettavilta näyttäviltä verkkosivuilta käyttäjät huijataan antamaan tietonsa rikollisille. Viestejä saatetaan lähettää esimerkiksi kirkon työntekijän, pankin, Poliisin tai Microsoftin nimissä. Myös seurakuntien sosiaalisen median palveluihin on tullut yhteydenottoja, joista voi päätellä niiden olleen huijauksia. Liitteessä 2 on esimerkkejä erilaisista huijausviesteistä, jotka ovat saapuneet sähköpostitse, tekstiviestillä tai pikaviestisovellus Whatsappiin.

Tietojenkalastelun kautta saaduilla tunnuksilla rikollinen voi kirjautua (kirkon) järjestelmiin ja pyrkii löytämään tietoja, joilla voidaan tehdä uusia rikoksia. Huijari voi esimerkiksi esiintyä kirkon työntekijänä lähettämällä työntekijän sähköpostista lisää tietojenkalastelu- tai huijausviestejä. Mikäli tietojenkalastelun kautta rikollinen on saanut tietoonsa pankki- tai luottokorttitietoja, niillä voi tehdä ostoksia verkkokaupoista tai tehdä rahansiirtoja työntekijän nimissä.

Erilaisia tietojenkalasteluviestejä kirkon sähköpostiosoitteisiin tulee päivittäin, vaikka käytössä on tehokas roskapostinsuodatus. Kyseessä on siis valitettavasti hyvin yleinen ilmiö, johon työntekijöiden pitää osata varautua päivittäisessä työssään. Liitteessä 3 on ohje, kuinka tunnistaa tietojenkalasteluviesti.

Huijausviestit ja haittaohjelmat

Huijausviesteissä voidaan pyytää esimerkiksi seurakunnalta rahansiirtoja esiintymällä seurakunnan työntekijänä tai kiristämällä rahaa eri tavoin. Kuten tietojenkalasteluviesteissä, huijausviesteissä vedotaan yleensä kiireeseen ja nopeaan reagointiin. Sähköpostin välityksellä voidaan lähettää myös haittaohjelmia työntekijöiden laitteisiin. Haittaohjelmien kautta rikollinen voi sitten murtautua järjestelmiin.

Aiemmin tietojenkalasteluviestit tai muut huijausviestit pystyttiin tunnistamaan selkeästi huijauksiksi esimerkiksi huonon suomen kielen vuoksi. Nykyään on toisin. Viestit saattavat sisältää erittäin hyvää kieltä ja ovat muutenkin taidokkaasti väärennettyjä. Huijausviestien tunnistaminen on nykyään entistä vaikeampaa.

Kuten tietojenkalasteluviestejä, myös erilaisia huijausviestejä lähetetään kirkon sähköpostiosoitteisiin päivittäin. Roskapostinsuodatin poistaa myös valtaosan huijaus- ja haittaohjelmaviesteistä, mutta tietojenkalasteluviestien tapaan työntekijöiden rooli näiden tunnistamisessa on erittäin tärkeää.

Palvelunestohyökkäykset

Myös palvelunestohyökkäykset kirkon järjestelmiin tai palveluntarjoajien järjestelmiin ovat mahdollisia. Palvelunestohyökkäyksessä tarkoituksena on estää tai hidastaa verkossa olevan palvelun käyttö. Palvelunestohyökkäyksiä on viime vuosina tehty usean eri viranomaisen esimerkiksi Kelan ja eduskunnan sähköisiin palveluihin sekä suomalaisten pankkien verkkopalveluihin.

Palvelunestohyökkäyksessä valjastetaan suuri määrä Internetiin liitettyjä laitteita ottamaan eri puolilta maailmaa yhteyttä tiettyyn järjestelmään saman aikaisesti. Laitteina voidaan hyödyntää esimerkiksi tietokoneita tai Internetiin liitettyjä kameravalvontajärjestelmiä, jotka on aiemmin hakkeroitu. Palvelunestohyökkäys hidastaa palvelun käyttöä hetkellisesti. Se voi myös lamauttaa koko palvelun tai pahimmassa tapauksessa estää koko järjestelmän käytön useaksi viikoksi. Palvelunestohyökkäysten tarkoitus on ensisijaisesti vaikuttaa palvelujen käytettävyyteen.

Hakkerointi eli tietomurto

Hakkeroinnissa järjestelmiin murtaudutaan käyttämällä esimerkiksi tietojenkalastelun kautta saatuja tunnuksia tai hyödyntämällä järjestelmässä havaittuja haavoittuvuuksia. Hakkeroinnin tuloksena rikollinen voi poistaa järjestelmästä tietoja tai ladata niitä itselleen ja käyttää niitä kiristyksen välineenä. Nykyisin tietomurtojen seurauksena on hyvin yleistä, että rikollinen salaa eli kryptaa järjestelmissä olevat tiedot. Salatut tiedot eivät ole enää organisaation käytettävissä ja salaus on mahdollista purkaa ainoastaan rikollisen tietämällä avaimella. Tätä salausavainta tietomurron kohteeksi joutuneelle organisaatiolle sitten pyritään myymään. Yleinen ohje on, että rikolliselle ei koskaan pidä maksaa mitään.

Hakkerointi voi kohdistua seurakunnan tietoliikennelaitteisiin, tietokoneisiin, matkapuhelimiin, info-näyttöihin tai vaikkapa kiinteistöautomaatiojärjestelmiin. Periaatteessa kaikki laitteet, jotka ovat yhdistetty Internetiin, ovat mahdollisia hakkeroinnin kohteita. Ellei tietoliikenneverkkoa tai laitteita ole suojattu asianmukaisesti, yhden hakkeroidun laitteen kautta voidaan murtautua seuraavaan laitteiseen ja siitä taas eteenpäin etsien tietoja, joita voidaan käyttää rikokselliseen tarkoitukseen. Hakkeroitujen laitteiden kautta voidaan toteuttaa myös laajoja palvelunestohyökkäyksiä sähköisiin palveluihin tai tietoliikenneverkkoihin.

Loppuvuodesta 2023 Ruotsin kirkossa koettiin laaja tietomurto, jonka seurauksena Ruotsin kirkon ja sen seurakuntien tietojärjestelmiin hyökättiin. Tarkemmin tapauksesta on kerrottu luvussa 6.

Misinformaatio ja disinformaatio

Dis- ja misinformaatio ovat väärän tiedon levittämistä tahattomasti tai tahallisesti, joka yleensä tapahtuu Internetin keskustelupalstoilla tai sosiaalisessa mediassa. Misinformaatiossa saatetaan huomaamatta esimerkiksi jakaa esimerkiksi valeuutinen, jonka lähteitä ei ole tarkastettu. Disinformaatio sen sijaan on tarkoituksella levitettyä väärää tietoa. Disinformaatiota voidaan levittää esimerkiksi politiikasta, ilmastonmuutoksesta tai uskonnosta.

Kirkon toiminnan kannalta disinformaatiota voidaan jakaa esimerkiksi siten, että pyritään liittämään jollain tapaa kirkollinen toiminta negatiivisiin uutisiin, vaikka kirkolla ei ole mitään tekemistä asian kanssa. Näin pyritään saamaan kirkko näyttäytymään huonossa valossa ihmisten silmissä ja vaikuttamaan yleiseen mielipiteeseen kirkon toiminnasta tai sen opetuksesta. Väärää tietoa voidaan jakaa myös seurakunnan virallisilla sosiaalisen median kanavilla tekaistujen tilien kautta, murtautumalla seurakunnan some-tilille tai verkkosivuille ja julkaisemalla siellä haitallista sisältöä tai luomalla kopioita seurakunnan somesivuista väärän tiedon levittämiseen.

Väärän tiedon tahallista levittämistä on käytetty esimerkiksi eri puolilla maailmaan vaaleissa vaikuttamisen välineenä. Tämä voi olla todellinen uhka tulevaisuudessa myös kirkon eri vaaleissa.

Uudet uhat

Kyberrikollisuus kehittyy ja monimutkaistuu koko ajan. Esimerkiksi tekoälyn hyödyntäminen tuo rikollisille uusia kehittyneempiä mahdollisuuksia hyökkäyksille. Tietojenkalasteluviesteistä ja haittaohjelmista voidaan tehdä entistä vaikeammin tunnistettavia.

Tekoäly mahdollistaa myös syväväärennösten (deepfake) tekemisen. Niissä tekoälyä hyödyntämällä kuvaan tai videoon liitetään esimerkiksi toisen henkilön kasvot tai puhe. Näin voidaan saada henkilö tekemään tai sanomaan asioita, joita he eivät todellisuudessa ole tehneet tai sanoneet. Syväväärennöksen tarkoitus on erityisesti vaikuttaa tiedon luottamuksellisuuteen.

Hyökkäykset voivat tapahtua yhtä tai useampaa edellä mainitutta tapaa hyödyntäen. Tämän vuoksi kyberturvallisuutta pitää jatkossakin kehittää niin kirkossa kuin muissa organisaatioissa. Erityisen tärkeää on tiedostaa ja ymmärtää nykyiset ja tulevat uhat sekä varautua niihin.

5.2. Työntekijän virheet

Kyberrikollisuudessa pyritään hyödyntämään ihmisen osaamattomuutta, kiirettä, inhimillisyyttä ja/tai hyväntahtoisuutta. Kyse on sosiaalisesta vaikuttamisesta (social engineering). Merkittävä uhka kyberturvallisuudelle on lopulta ihminen eli tässä yhteydessä jokainen kirkon työntekijä luottamushenkilöt ja vapaaehtoiset mukaan lukien.

Selvää on, että kukaan ei tahallaan tee virheitä. Työntekijään kohdistuu nykyään valtava määrä erilaisia huijausyrityksiä niin töissä kuin vapaa-ajallakin. Valitettavasti joskus huijaukset onnistuvat ja yksittäisen työntekijän virheestä voi koitua koko kirkolle merkittäviä ongelmia.

Kuten hakkeroinnissakin, yhteen laitteiseen murtautuminen voi antaa pääsyn muihin järjestelmiin ja johtaa isompiin ongelmiin. Sama kaava on mahdollinen työntekijöiden osalta. Yksittäisen työntekijän käyttäjätilin kautta voi päästä käsiksi toisen työntekijän tietoihin, kirjautumaan kirkon eri järjestelmiin tai esiintymään kirkon työntekijänä esimerkiksi lähettämällä työntekijän sähköpostista viestejä eri tahoille.

Työntekijä saattaa tehdä työssään myös inhimillisiä virheitä. Kiire, vahinko, osaamattomuus tai piittaamattomuus annettuja ohjeita kohtaan altistavat inhimillisiin virheisiin kuten huijauksissakin. Esimerkiksi väärien tietojen kirjaaminen järjestelmiin, tietojen poistaminen järjestelmistä, liian laajojen käyttöoikeuksien antaminen tietoihin tai väärin tehdyt järjestelmäpäivitykset voivat aiheuttaa järjestelmiin tai niiden tietoihin isoja ongelmia. Nämäkin uhat on syytä tunnistaa ja luoda toimintatavat seurakunnissa siten, että myös inhimilliset virheet olisivat minimoitavissa tai korjattavissa. Mitä laajemmat käyttöoikeudet työntekijällä on, sitä suuremmat vahingot virheestä voi koitua. Kyberturvallisuuden näkökulmasta työntekijään ei voida automaattisesti luottaa.

Tiedossa on ainakin muutamia tapauksia viime vuosilta, jossa kirkon työntekijä on vahingossa lähettänyt luottamuksellista tietoa sisältävän sähköpostin väärälle henkilölle, poistanut tärkeitä tiedostoja verkkoasemalta ja antanut käyttäjätunnuksensa ja salasanansa tietojenkalasteluviestiin. Tapaukset on selvitetty yhteistyössä asianosaisten kanssa ja niistä on tehty tarvittavat ilmoitukset viranomaisille. Lisäksi korjaavia toimenpiteitä on tehty ja ohjeistusta päivitetty, jotta vastaavalta voitaisiin jatkossa välttyä.

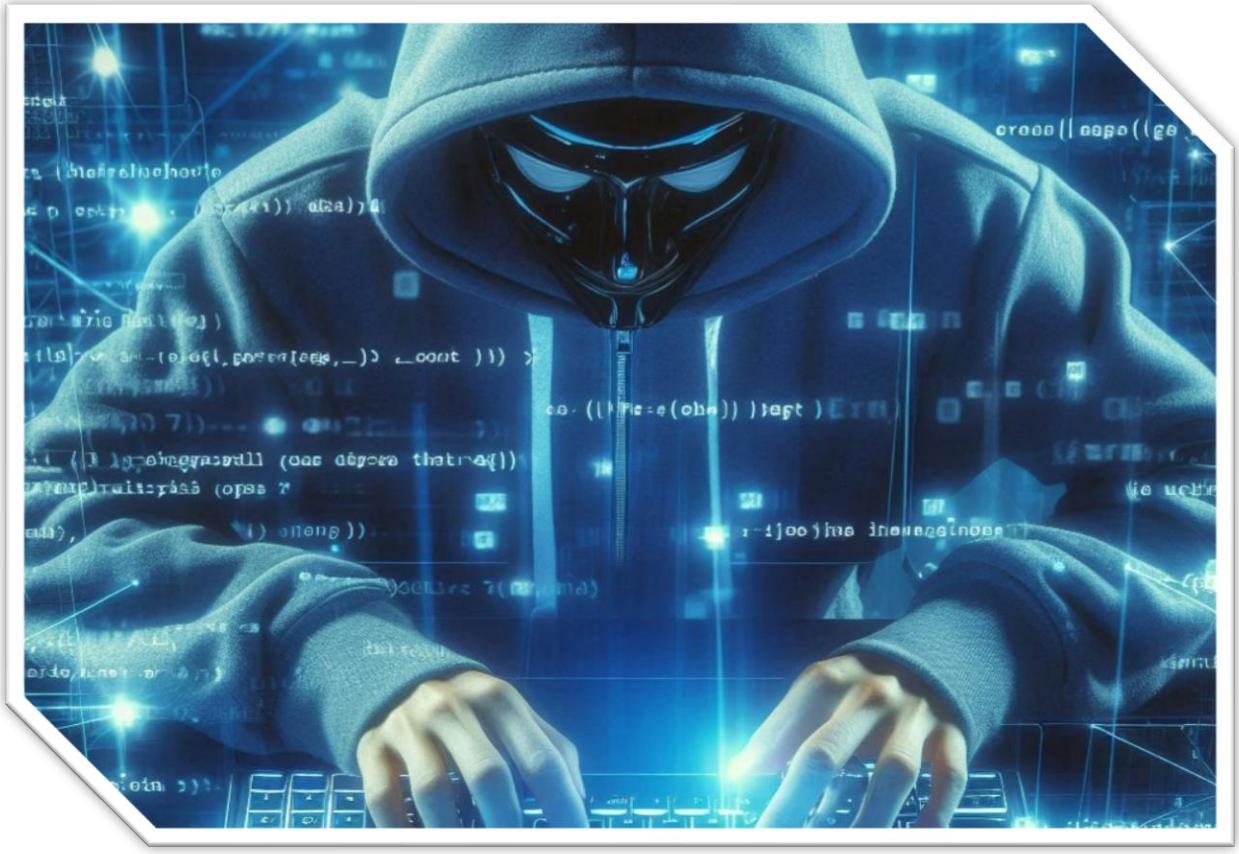
Työntekijä voi tuntea virheen tehdessään häpeää, osaamattomuutta tai mennä paniikkiin. Hän ei uskalla kertoa asiasta eteenpäin tai ei tiedä kenelle tilanteesta pitäisi kertoa. Tämän vuoksi on tärkeää, että koko Suomen evankelis-luterilaisessa kirkossa on avoin ja keskusteleva ilmapiiri tietoturvallisuudesta ja kyberturvallisuudesta.

5.3.Järjestelmävirheet ja vikatilanteet

Toisinaan myös tietojärjestelmissä tai tietoliikenneverkoissa on ongelmia. Erilaiset automaattisesti asentuvat päivitykset saattavat aiheuttaa järjestelmien toimimattomuutta tai hitautta. On ollut myös tapauksia, jossa järjestelmän päivitys tai järjestelmän korvaaminen toisella järjestelmässä on aiheuttanut myös järjestelmään tallennettuihin tietoihin muutoksia. Nämä ovat nykyisin harvinaisia tapauksia, mutta mahdollisia.

Ongelmat voivat johtua esimerkiksi ohjelmisto- tai palvelutoimittajien laajemmista ongelmista myös Suomen rajojen ulkopuolella, jotka sitten heijastuvat myös kirkon järjestelmiin. Nykyisin kun kirkossa hyödynnetään laajasti esimerkiksi pilvipalveluita palveluntuotannossa, järjestelmien toimivuus on yhä enemmän riippuvainen myös kyberturvallisuudesta Suomen rajojen ulkopuolella. Tämän vuoksi kokonaiskirkon kyberturvallisuus on viime kädessä osa maailmanlaajuista kyberturvallisuutta ja toisinpäin. Kirkon kyberturvallisuus koostuu siis laajoista toimitusketjuista, joista jokainen toimitusketjun osa voi joutua niin kyberrikollisuuden kohteeksi kuin oman työntekijän tai järjestelmän virheen kohteeksi.

Oli kyseessä sitten huijauksen kohteeksi joutuminen tai inhimillinen virhe, näistä tietoturvapoikkeamista pitää aina ilmoittaa eteenpäin. Kuten Kyberturvallisuuden roolit ja vastuut kirkossa -luvussa todetaan, jokaisella seurakunnan työntekijällä on velvollisuus raportoida havaitsemistaan tietoturvallisuuteen liittyvistä epäkohdista ja poikkeamista esihenkilölle ja seurakunnan tietoturvan yhdyshenkilölle. Näin vältetään suurempien ongelmien synty. Tarkemmin tietoturvapoikkeamien ilmoittamisesta on kerrottu luvussa 8.



6. KYBERHYÖKKÄYKSET JA -HUIJAUKSET USKONTOKUNTIIN

Tässä luvussa esitellään joitakin huijauksia ja kyberhyökkäyksiä, jotka ovat kohdistuneet eri uskontokuntiin Suomessa ja maailmalla. Suurin osa näistä on tuoreita tapauksia vuosilta 2023 ja 2024. Rikoksista on ilmoitettu paikalliselle poliisille ja tietoturva- tai tietosuojaviranomaisille sekä uskontokunnat ovat tiedottaneet niistä avoimesti eri medioille. Tutkinta on näissä vielä kesken.

- Jyväskylän seurakunnan pääkirkkoon murtauduttiin kesällä 2024. Kyseessä ei ollut varsinainen kyberhyökkäys tai -huijaus, mutta murrossa varastettiin muun muassa kirkossa säilytetty tietokone ja muuta elektroniikkaa. Seurakunnan tietoturvallisuus tai tietosuoja ei kuitenkaan vaarantunut murrossa käytössä olevien tietoturvaratkaisujen vuoksi. (Jyväskylän seurakunta, 2024.)

- Ruotsin kirkkoon kohdistui loppuvuodesta 2023 laaja kyberhyökkäys. Kohteena oli useat kirkon eri järjestelmät, joihin haittaohjelmalla hyökättiin. Haittaohjelmalla hakkeriryhmä sai salattua osan kirkon järjestelmistä ja kiristi sillä kirkkoa. Hyökkäyksen myötä useat kriittiset Ruotsin kirkon järjestelmät olivat poissa käytöstä jopa kuukauden. Hyökkäyksessä ei tiedettävästi seurakunnan jäsenten henkilötiedot vaarantuneet, mutta Ruotsin kirkon työntekijöitä varoitettiin heidän omien henkilötietojen vaarantumisesta. (Ruotsin kirkko, 2023.)

- Luterilaisten kirkkojen yhteistyöjärjestö Luterilainen maailmanliitto (LML) joutui verkkohyökkäyksen ja -kiristyksen kohteeksi loppuvuodesta 2023. Verkkohyökkäyksessä hakkeriryhmä murtautui Luterilaisen maailmanliiton järjestelmiin ja kiristi maailmanliittoa kaappaamallaan tiedoilla. Osa kaapatuista tiedoista julkaistiin hakkeriryhmän toimesta nettiin ja ne koskivat muun muassa tietoja ihmisten passeista ja maailmanliiton talousasioita. Hakkeriryhmä myi myös kaappaamaansa aineistoa eteenpäin muille rikollisille. (Iltasanomat, 2024.)

- Sama hakkeriryhmä iski loppuvuodesta 2023 myös maailman kristillisten kirkkokuntien ekumeeniseen järjestöön Kirkkojen maailmanneuvostoon (KMN). Verkkohyökkäyksessä hakkeriryhmä hakkeroi KMN:n järjestelmät ja kiristi maailmanneuvostoa käsiinsä saamallaan aineistolla. Hyökkäyksessä myös maailmanneuvoston tietojärjestelmät kaatuivat. (Kirkkojen maailmanjärjestö, 2023 ja Iltasanomat, 2024.)

- Jyväskylän ortodoksisen seurakunnan kirkkoherran nimissä lähetettiin joulukuussa 2023 huijausviestejä. Lähettäjänä näkyi kirkkoherran etu- ja sukunimi ja ne olivat allekirjoitettu hänen nimellään ja virka-asemallaan. Todellisuudessa sähköpostit olivat tulleet väärennetystä sähköpostiosoitteesta. (Jyväskylän ortodoksinen kirkko, 2023.) Vastaavia tapauksia ilmenee Suomen evankelis-luterilaisessa kirkossakin säännöllisesti.

- Suomen evankelis-luterilaiseen kirkkoon ja muihin suomalaisiin organisaatioihin kohdistui laaja tietojenkalastelukampanja loka-marraskuussa 2023. Kampanjan aikana useiden eri organisaatioiden työntekijöiden käyttäjätileihin onnistuttiin murtautumaan Suomessa. Kyberturvallisuuskeskus julkaisi tietomurtoaallosta vakavan varoituksen, joka sittemmin poistettiin. (Kyberturvallisuuskeskus, 2023b.)

- Loppuvuodesta 2020 seurakuntien Kauneimmat Joululaulut -tapahtumailmoituksiin Facebookissa (nykyisin Meta) kohdistui laaja huijauskampanja. Kampanjassa muun muassa luotiin Facebookiin huijaustapahtumia, jossa tilaisuuden osallistumisen yhteydessä kalasteltiin luottokorttitietoja. (Kirkon viestintä, 2020.)

- Kangasalan seurakunta joutui vuonna 2019 maksupetoshuijauksen uhriksi. Petoksessa seurakunta kärsi huomattavaa taloudellista vahinkoa. (Kangasalan seurakunta, 2019.)

Kyseisten tapausten lisäksi muihinkin organisaatioihin Suomessa ja maailmalla on vuosien varrella kohdistunut erilaisia kyberuhkia ja tietomurtoja. Esimerkiksi yksi poikkeuksellisen laaja tapaus Suomessa tuli ilmi julkisuuteen vuonna 2020 Psykoterapiakeskus Vastaamoon kohdistuneen tietomurron osalta. Tapaus ei liity Suomen evankelis-luterilaiseen kirkkoon, mutta se aiheutti huolestuneita yhteydenottoja myös seurakuntiin kirkon tietoturvallisuuden tasosta

Vastaamon tietomurrossa varastettiin yli 30000 ihmisen henkilö- ja potilastietoja ja julkistettiin ne osittain verkossa. Varastetuilla tiedoilla kiristettiin aluksia Vastaamoa ja myöhemmin henkilöitä, joiden tietoja oli tietomurroissa saatu käsiin. Tietomurtoja tapahtui useampana kertana vuosien 2018–2019 aikana, mutta ensimmäinen kiristysviesti Vastaamoon lähetettiin vasta syksyllä 2020. Tämän jälkeen Vastaamo teki tietomurrosta ilmoituksen viranomaisille ja samalla se tuli ilmi myös julkisuuteen. (Wikipedia, 2024.)

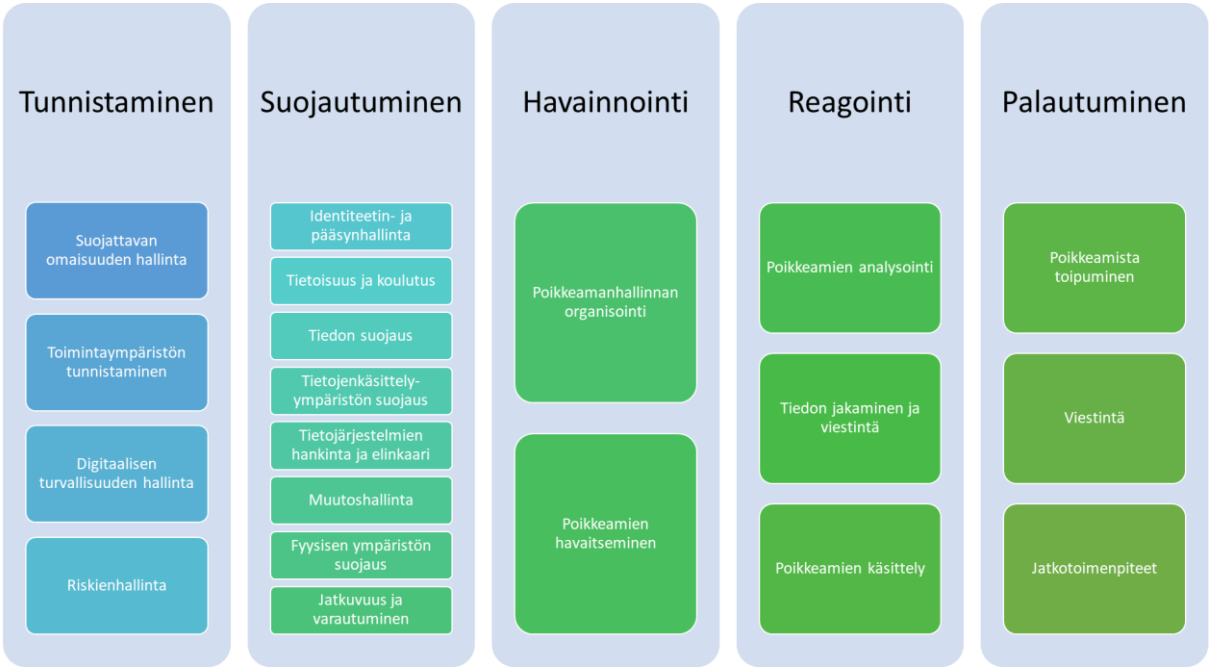
Vastaamo-tapauksen lisäksi keväällä 2024 uutisoi laajasta tietomurrosta Helsingin kaupungin kasvatuksen ja koulutuksen toimialan henkilötietoihin. Tietomurron tekijä saattoi saada haltuunsa tietoja kaikista helsinkiläisistä oppivelvollisista kaupungin verkkoasemaan murtautumalla. Tietomurto koski noin 150000 oppijaa ja heidän huoltajiansa sekä kaupungin työntekijöitä. Henkilötietoja ei ole Helsingin kaupungin mukaan väärinkäytetty. (Helsingin kaupunki, 2024.)

7. KYBERUHKIEN TORJUNTA

Kyberuhkilta suojautumisessa ja torjunnassa on paljon erilaisia keinoja. Usein ne ovat teknisiä välineitä, mutta jo pelkästään henkilöstöä kouluttamalla asioihin voidaan varautua. Seuraavassa luvussa käydään läpi tarkemmin, mitä kirkon ja sen seurakuntien on hyvä huomioida kyberturvallisuudessa ja kyberuhkien torjunnassa.

Digi- ja väestötietoviraston (DVV) mukaan digitaalisen turvallisuuden arkkitehtuuri koostuu viidestä kokonaisuudesta. Nämä ovat *tunnistaminen*, *suojautuminen*, *havainnointi*, *reagointi* ja *palautuminen*. Tätä arkkitehtuurimallia voidaan hyödyntää myös kirkon kyberturvallisuudessa ja sen kehittämisessä. Digi- ja väestöviraston malli sisältää erilaisia työkaluja, jolla seurakunnat voivat tarkemmin selvittää kyberturvallisuuden tasonsa.

Tässä luvussa esitellään yleisellä tasolla mallin eri kokonaisuudet ja mitä ne esimerkiksi tarkoittavat Suomen evankelis-luterilaisessa kirkossa. Tarkemmin arkkitehtuuriin ja sen työkaluihin voi tutustua Digi- ja väestötietoviraston verkkosivuilla osoitteessa https://wiki.dvv.fi/display/DTARK/Digitaalisen+turvallisuuden+arkkitehtuuri.



Kuva 2 Digitaalisen turvallisuuden arkkitehtuuri (DVV 2022.)

7.1. Kyberuhkien tunnistaminen

Arkkitehtuurimallissa tunnistaminen koostuu suojattavan omaisuuden hallinnasta, toimintaympäristön tunnistamisesta, digitaalisen turvallisuuden hallinnasta ja riskienhallinnasta. Lähtökohta kirkon kyberturvallisuudelle on tunnistaa, mitä suojattavaa kirkossa on. Esimerkiksi seurakunnat käsittelevät toiminnassaan seurakuntalaisten henkilötietoja toteuttaessaan kirkon lakisääteistä perustehtävää. Tietosuojalainsäädännön näkökulmasta kyseessä on erityisten henkilötietoryhmien käsittely, koska henkilötiedoista ilmenee usein myös henkilön uskonnollinen vakaumus. Näitä erityisiä henkilötietoryhmiä seurakuntien on suojeltava erityisen tarkasti.

Lisäksi seurakunnat hoitavat monia kirkon yhteiskunnallisia tehtäviä kuten hautaustoimea ja väestörekisteriin liittyviä tehtäviä. Henkilötietoja ja muita kriittisiä tietoja sekä asiakirjoja säilytetään ja käsitellään sitten erilaisissa seurakuntien tietojärjestelmissä, tietoliikenneverkoissa ja laitteissa sekä tarjotaan sähköisinä palveluina käyttöön asiakkaille ja yhteistyökumppaneille.

Henkilötietoja sisältäviin tietojärjestelmiin kohdistuu aina kohonnut kyberuhkien riski. Mitä enemmän tietoja on järjestelmässä, sitä tiukemmat suojaustoimet järjestelmässä tulee olla. Kyberrikolliset myyvät varastettuja henkilötietoja eteenpäin verkossa tai kiristävät organisaatioita tai tietomurron uhreja julkaisemalla tietoja verkkoon. Varastetuille henkilötiedoilla voidaan esimerkiksi tehdä ostoksia verkossa, luoda valeprofiileja eri verkkopalveluihin tai tehdä muita petoksia. Varastettuja henkilötietoja voidaan käyttää myös dis- tai misinformaatioon eli väärän tiedon levittämiseen verkossa.

Kirkko vastaa myös kulttuurihistoriallisesti rakennusten ja irtaimiston ylläpidosta. Kiinteistöihin liittyy usein erilaisia kiinteistöautomaatio-, kulunvalvonta sekä kameravalvontajärjestelmiä. Erityisesti etävalvottajat ja internetiin liitetyt laitteet ovat alttiita tietomurroille. Mikäli näiden järjestelmien kyberturvallisuus vaarantuu, voi seuraukset rakennuksille ja irtaimistolle olla taloudellisesti ja toiminnallisesti merkittävät.

Myös talous- ja henkilöstöhallinnon järjestelmien toimivuus ja turvallisuus on ensiarvoisen tärkeää. Järjestelmissä käsitellään henkilötietojen lisäksi seurakuntien rahaliikennettä, joten tämän vuoksi näihin järjestelmiin kohdistuu kohonnut kyberuhkien riski. Mikäli rikollinen taho pääsee näihin tietoihin käsiksi tietomurron seurauksena, seurakunnan taloudelliset menetykset voisivat olla merkittäviä. Rikollinen voisi tiedon eheyteen vaikuttamalla esimerkiksi muuttaa pankkitilitietoja rahansiirroissa ja ohjata ne väärälle tilille.

Seurakuntavaaleihin tai muihin kirkollisiin vaaleihin voidaan myös yrittää vaikuttaa väärän tiedon kautta. Jakamalla esimerkiksi sosiaalisen median kanaviin ehdokkaasta väärää tietoa, voidaan saada ehdokas näyttäytymään äänestäjille huonossa valossa. Väärän tiedon jakamisella voi olla suurikin merkitys äänestyskäyttäytymisessä ja sitä kautta vaalien lopputuloksessa. Erityisesti seurakuntavaaleissa jokaisella annetulla äänellä on merkitystä, koska äänestysaktiivisuus on ollut vuosikymmenet alhainen. Esimerkiksi vuoden 2022 seurakuntavaalien äänestysprosentti oli 12,7 %. Väärän tiedon levittämisen lisäksi vaalijärjestelmiin voidaan yrittää murtautua tai häiritä niiden toimintaan vaalien aikana.

Kyberuhat voivat kohdistua myös toimitusketjun eri toimijoihin. Tietomurrot tai palvelunestohyökkäykset palveluntarjoajien tai heidän alihankkijoiden tietojärjestelmiin, tietoliikenneverkkoihin tai laitteisiin vaarantaa myös seurakuntien kyberturvallisuuden. Tämän vuoksi kyberturvallisuuden riskien hallinta pitää ulottaa myös seurakuntien yhteistyökumppaneihin ja eri toimitusketjuihin.

Lisäksi seurakunnilla on paljon käytössä erilaisia tietojärjestelmiä, joiden kriittisyys osana isompaan kokonaisuutta pitää tunnistaa ja tehdä tarvittavat suojaustoimet. Kaikkia tietoja, järjestelmiä, tietoliikenneverkkoja, laitteita tai käyttäjiä ei tarvitse kuitenkaan suojata samalla tavalla – riittää, että kyberturvallisuuden perustaso on kaikkialla kunnossa Zero Trust -periaatetta unohtamatta.

Esimerkkejä seurakunnan suojattavista kohteista kyberuhilta:

- kirkon jäsentiedot
- talous- ja henkilöstöhallinto ja rekrytointi
- hankinnat ja sopimukset
- hautarekisteri
- vaalijärjestelmä
- asian- ja dokumenttihallinta ja päätöksenteko
- kiinteistöautomaatio ja kulunvalvonta
- seurakunnan verkkosivut ja intranet
- sosiaalisen median palvelut
- toiminnanohjausjärjestelmät
- sähköposti ja muut sähköisen viestinnän järjestelmät
- asiakastiedot ja sähköiset leiri- ja tapahtumailmoittautumisjärjestelmät
- muut sähköisen asioinnin palvelut
- laitteet, työntekijät, järjestelmät ja tietoliikenneyhteydet, jotka mahdollistavat tietojen käsittelyn
- järjestelmien tekniset rajapinnat, jotka siirtävät tietoa järjestelmien välillä

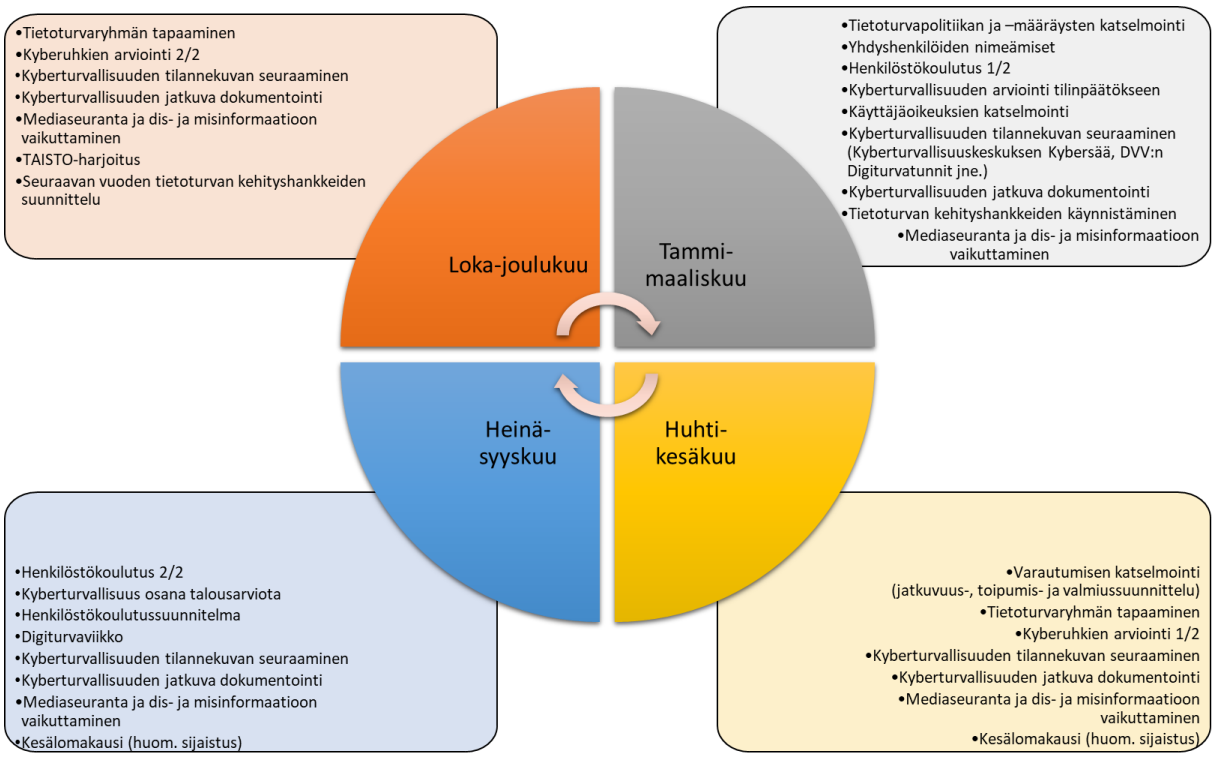
Suomen evankelis-luterilaista kirkkoa ja sen seurakuntia uhkaavia kyberriskejä ja toimenpiteitä niiden torjumiseksi on kuvattu esimerkein liitteeseen 5. Pohjana on käytetty Seurakunnan valmiussuunnitteluohjeen Riskien arviointi -liitettä. Sitä on täydennetty CIA-analyysi-sarakkeella, joka kuvaa tarkemmin sen, mihin tietoturvan osa-alueeseen kyberriski toteutuessaan erityisesti vaikuttaa. Osa-alueita ovat luvun 2 mukaisesti käytettävyys, eheys ja luottamuksellisuus.

Kyberturvallisuuden näkökulmasta seurakuntien toimintaa uhkaavat samat riskit maantieteellisestä sijainnista tai seurakunnan koosta riippumatta. Osa tietojärjestelmistä ja palveluntarjoajista ovat kuitenkin seurakuntakohtaisia ja osalla seurakunnista on vastuu joidenkin toimintojen tuottamisesta toisille seurakunnille. Myös seurakuntalaisille tarjotut sähköiset palvelut voivat olla laajuudessaan hyvinkin erilaisia seurakuntien kesken. Tämän vuoksi kyberturvallisuuden tarkempi riskien arviointi pitää tehdä seurakunnittain. Tarkemmassa riskien arvioinnissa pitää huomioida seurakunnan eri toiminnot ja työalat sekä niihin liittyvät toimitusketjut.

7.2. Kyberuhkilta suojautuminen

Kun suojattavat kohteet ja tiedot on tunnistettu seurakunnassa ja määritelty niihin liittyvät riskit, on selvitettävä, kuinka uhkilta voidaan suojautua. Kaikkia riskejä ei koskaan voida poistaa, mutta niitä voidaan oikeaoppisella suojautumisella merkittävästi vähentää. Kyberturvallisuuden pitää näkyä niin kokonaiskirkon ja seurakuntien strategioissa kuin työntekijöiden päivittäisessä toiminnassa. Kyberturvallisuudelle pitää varata riittävät resurssit ja kyberturvallisuus pitää huomioida seurakunnan vuosisuunnittelussa. Suunnittelussa voidaan hyödyntää esimerkiksi kyberturvallisuuden vuosikelloa, jota seurakunta voi tarvittaessa täydentää ja muokata omiin tarpeisiinsa sopivaksi. (kuva 3).

Vuosikellon mukaisesti alkuvuodesta tulisi vähintään katselmoida kirkon tietoturvapolitiikka ja tietoturvamääräykset, nimetä tietoturvan (kyberturvan) yhdyshenkilöt ja arvioida edeltävää vuotta sekä järjestää henkilöstölle kyberturvallisuuteen liittyvää koulutusta. Keväällä on vuorossa varautumisen katselmointi, johon kuuluu muun muassa jatkuvuus-, toipumis- ja valmiussuunnitelmien testaaminen ja päivitys. Syksyllä vuorossa olisi esimerkiksi valtakunnalliseen Digiturvaviikkoon osallistuminen, kyberturvallisuuden huomioiden seuraavan vuoden toimintasuunnitelmassa ja talousarviossa sekä loppuvuodesta Taisto-harjoitukseen osallistuminen. Jatkuvaa työtä on muun muassa kyberturvallisuuteen liittyvien tietoturvapoikkeamien dokumentointi sekä jatkuva kehittäminen sekä mediaseuranta.



Kuva 3 Esimerkki seurakunnan kyberturvallisuuden vuosikellosta

Kyberturvallisuus pitää olla sisäänrakennettuna kaikessa seurakunnan toiminnassa. Kyberturvallisuus ei ole pelkästään teknisiä ratkaisuja, joita IT-aluekeskukset tai kirkkohallituksen tietohallintoyksikkö seurakunnille tarjoavat. Se on myös jatkuvaa kehittämistä, johtamista, henkilöstön kouluttamista, kyberturvallisuutta parantaviin harjoituksiin osallistumista ja kyberturvallisuuden yleisen tilannekuvan ylläpitämistä myös seurakunnissa.

7.2.1. Kyberturvallisuuden johtaminen

Kuten kirkon muutakin toimintaa, myös tietoturvallisuutta ja kyberturvallisuutta pitää johtaa. Vaikka kyberturvallisuus on jokaisen työntekijän vastuulla, on se viime kädessä esihenkilöiden ja johdon asia. Suomen evankelis-luterilaisen kirkon ja seurakuntien ylimmän johdon pitää ymmärtää roolinsa ja vastuunsa kyberturvallisuudessa kuten luvussa 4 on kerrottu. Johtamiseen kuuluu tiedostaa ja ymmärtää kyberuhat ja tunnistaa erityisesti omaan seurakuntaan kohdistuvat erityiset riskitekijät. Näitä voivat olla esimerkiksi rajalliset henkilöstöresurssit, henkilöstön osaaminen, tai laajempi vastuu jonkin toiminnan, kuten aluekeskusrekisterin, järjestämisestä toisten seurakuntien puolesta.

Johdon pitää myös määrittää keinot ja resurssit kyberuhkien torjumiseen. Seurakunnan kirkkoneuvostolla on vastuu hyväksyä seurakunnan tietoturvapolitiikka, mutta myös määrittää tarvittavat henkilöstö- ja taloudelliset resurssit tietoturvallisuuden osalta. On hyvä ymmärtää, että seurakunnan tietoturvallisuuteen liittyvillä päätöksillä on aina vaikutusta myös koko kirkon tietoturvallisuuteen. Mikäli seurakunta panostaa esimerkiksi työntekijöille tarjottavaan tietoturvallisuuteen liittyvään koulutukseen, sillä on positiivinen vaikutus koko kirkon tietoturvaan. Toisaalta, mikäli yksittäisessä seurakunnassa suhtaudutaan välinpitämättömästi tietoturvallisuuteen, se vaarantaa koko kirkon tietoturvallisuuden.

7.2.2. Kyberturvallisuuden kouluttaminen ja perehdyttäminen

Jotta jokainen kirkon työntekijä, luottamushenkilö ja vapaaehtoinen osaisi toimia oikein, on tärkeää kouluttaa henkilöstöä säännöllisesti. Sitä voidaan toteuttaa seurakunnissa monella eri tavalla ja eri yhteyksissä. Suomen evankelis-luterilaisessa kirkossa on tuotettu kaikille työntekijöille avointa koulutusmateriaalia esimerkiksi tietojenkalastelusta. Osa seurakunnista tarjoaa työntekijöilleen ja luottamushenkilöilleen verkkokursseja liittyen tietoturvallisuuteen ja tietosuojaan. Kyberturvallisuutta kannattaa pitää esillä myös seurakuntien omissa henkilöstöinfoissa ja tiimikokouksissa sekä tietyn työalan valtakunnallisilla neuvottelupäivillä. Esimerkiksi Kyberturvallisuuskeskuksen verkkosivuilta löytyy ajankohtaista tietoa ja ohjeistusta kyberturvallisuudesta työntekijöille ja johtohenkilöille, joita seurakunnan kannattaa hyödyntää. Myös Digi- ja väestötietovirasto järjestää verkossa kuukausittain kaikille avoimia Digiturvatunteja, jossa käydään läpi ajankohtaisia uhkia ja tarjoaa vinkkejä niiltä suojautumiseen.

Jokaisen työntekijän pitäisi vähintään tuntea kirkon tietoturvapolitiikka ja kirkon yleiset tietoturvamääräykset sekä ymmärtää niiden tavoitteet oman työn kannalta. Työntekijöiden pitää tietää myös keneen ottaa yhteyttä, kun havaitsee tietoturvapoikkeamia työssään. Tarkemmin tietoturvapoikkeamisen ilmoittamisesta on kerrottu luvussa 8.

Kouluttamisessa pitää huomioida myös tarvittavan osaamisen ylläpitäminen. Seurakuntien siirtäessä palveluitaan verkkoon, vaatii se myös uusien työtapojen ja välineiden omaksumista ja osaamista. Kyberuhkiin vastaaminen vaatii myös työntekijältä ymmärrystä ja osaamista. Esimerkiksi monivaiheisen tunnistautuminen käyttö edellyttää työntekijältä uutta osaamista. Monivaiheisesta tunnistautumisesta ja sen hyödyistä on tarkemmin kerrottu seuraavissa kappaleissa.

Uusien työntekijöiden osalta kyberturvallisuus pitää olla osa perehdyttämistä. Työntekijän siirtyessä tehtävästä toiseen, on varmistettava, että työntekijä tietää omat vastuut ja velvollisuudet myös uudessa tehtävässä. Jokaisen työntekijän pitää myös allekirjoittaa salassapitositoumus. Siinä työntekijä velvoitetaan pitämään salassa tehtävässään saamansa luottamukselliset tiedot. Vaitiolo- ja salassapito on voimassa myös palvelussuhteen päättyessä.

Seurakuntaliitoksissa työntekijöillä voi olla erilaisia ohjeistuksia ja käytänteitä liittyen tietoturvallisuuteen. Tämän vuoksi on tärkeää, että tietoturvallisuus, kyberturvallisuus ja tietosuoja huomioidaan myös seurakuntaliitoksissa. Tässä yhteydessä on hyvä valita ja tiedottaa uudelle organisaatiolle ne yhteisesti valitut parhaat käytännöt. Seurakuntaliitoksissa luottamushenkilöorganisaatio ja maantieteelliset etäisyydet kasvavat sekä uusia seurakuntalaisia ja yhteistyökumppaneita tulee mukaan toimintaa se. Myös nämä muutokset on hyvä huomioida niin kyberturvan johtamisessa, mutta myös kouluttamisessa ja perehdyttämisessä.

7.2.3. Kyberturvallisuuden huomioiminen hankinnoissa

Kirkon eri toimijat hankkivat tuotteita ja palveluita sadoilla miljoonilla euroilla vuosittain. Monet hankinnoista liittyvät tietoliikenneverkkoihin, tietojärjestelmiin, laitteisiin, henkilötietojen käsittelyyn ja sitä kautta kyberturvaan. Kaikissa hankinnoissa pitäisi huomioida kyberturva esimerkiksi liittämällä kilpailutusvaatimuksiin Kirkon yleiset tietoturvamääräykset, seurakunnan tietoturvapolitiikka sekä mahdolliset seurakuntakohtaiset tietoturvavaatimukset toimittajille, alihankkijoille ja tarvittaessa koko toimitusketjulle sekä tarjotuille tuotteille ja palveluille.

Seurakunnat hyödyntävät paljon eri julkishallinnon yhteishankintayksikköjen, kuten Hansel Oy, yhteishankintoja. Yhteishankintayksikköjen kilpailuttamissa puitejärjestelyissä on yleensä hyvin huomioitu yleiset tietototurvavaatimukset kyberturva huomioiden sekä henkilötietojen käsittelyn ehdot. Riippuen puitejärjestelystä, seurakunnat voivat vielä omissa kilpailutuksissaan tarkentaa näitä vaatimuksia halutessaan. Mitä kriittisemmästä toiminnasta on kyse, sitä tarkemmin pitää myös tieto- ja kyberturva ottaa huomioon hankinnan vaatimuksissa.

Hankintojen tietoturvavaatimuksissa voidaan esimerkiksi vaatia toimittajan henkilöstöltä tietosuoja- ja tietoturvaosaamista, tarjottujen tuotteiden osalta tietoturvapäivityksistä huolehtimista koko sopimuksen elinkaaren ajalta, palveluiden tietoturvallisuutta koskevaa valvontaa toimittajan toimesta sekä korvausvelvollisuutta toimittajan aiheuttamista tietoturvapoikkeamista.

Vaikka hankinnat tehtäisiinkin yhteishankintayksikköjen kautta, seurakunnan pitää joka tapauksessa käydä säännöllisesti keskusteluja toimittajan kanssa kyberturvallisuudesta ja sen kehittämisestä sopimuskauden aikana. Mitä pidempi sopimuskausi, sitä enemmän kyberturvallisuus ja sen uhat voivat muuttua sopimuskauden aikana. Esimerkiksi lainsäädännön kautta voi tulla uusia velvoitteita seurakunnille tai palveluntarjoajille, joita ei ole osattu alkuperäisessä kilpailutuksessa ottaa huomioon. Myös maailmanpoliittinen tilanne vaikuttaa hankintoihin. Mikäli tarpeet muuttuvat merkittävästi alkuperäisestä kilpailutuksesta, voi olla välttämätöntä tehdä uusi kilpailutus sopimuksen niin mahdollistaessa.

Viime vuosina hankintoihin ja toimitusketjuihin on liittynyt paljon epävarmuuksia, jotka ovat välillisesti vaikuttaneet myös kyberturvallisuuteen. Esimerkiksi vuonna 2020 alkaneen koronapandemian vuoksi Aasiassa monet IT-laitteita tai -komponentteja valmistavat tehtaat suljettiin ja tavarat eivät kulkeneet maailmalla. Samalla pandemian vuoksi työpaikoissa siirryttiin etätöihin ja IT-laitteiden, kuten kannettavien ja videoneuvotteluvälineiden, tarve kasvoi merkittävästi ympäri maailmaa. Tuotteiden valmistusongelmat ja samalla kysynnän kasvu merkitsivät toimitusaikojen merkittävää pidennystä.

Seurakunnissa se näkyi esimerkiksi siten, että toimitusongelmien ja koronapandemiasta aiheutuvien rajoitusten vuoksi tietokoneita ei pystytty vaihtamaan alkuperäisen suunnitelman mukaisesti vaan ne jatkovuokrattiin leasing-yhtiöltä. Tämä aiheutti hetkellisesti palvelujen käytettävyyteen haasteita. Koronapandemia on sittemmin päättynyt ja toimitusvaikeudet ovat toistaiseksi ohi.

Koronapandemian jälkeen alkoi Ukrainan sota, joka nosti lähes kaikkia hintoja. Muun muassa hintojen nousun ja sodasta aiheutuvien lisääntyvien kyberuhkien torjunnan vuoksi Suomen evankelis-luterilaisessa kirkossa ja sen seurakunnissa kuluu vuosittain kyberturvallisuuden ylläpitoon yhä enemmän resursseja. Varautuminen ja vaihtoehtoisten toimitusketjujen selvittäminen on osa kyberturvallisuutta.

7.2.4. Kyberuhilta suojautuminen teknisillä ratkaisuilla

Kyberturvallisuutta parannetaan monilla eri teknisillä ratkaisuilla ja suojaustoimenpiteillä. Ne kohdistuvat muun muassa laitteisiin, tietoliikenneverkkoihin, työntekijöiden käyttöoikeuksiin tai järjestelmien käyttöön. Tarkemmin teknisiä ratkaisuja on kuvattu kirkon yleisissä tietoturvamääräyksissä. Tässä oppaan luvussa esitellään tärkeimmät asiat, jotka seurakuntien ja seurakunnan työntekijöiden ja luottamushenkilöiden pitää huomioida työssään tai luottamushenkilönä toimiessaan kyberturvallisuuden näkökulmasta.

I Suojaa järjestelmät

Kaikki laitteet ja järjestelmät pitää säännöllisesti päivittää ja pitää ne valmistajan tuen piirissä. Tämä osaltaan estää järjestelmistä löydettyjen haavoittuvuuksien hyödyntämisen tietomurroissa. Järjestelmät pitää myös suojata antivirus-ohjelmilla ja palomuureilla. Antivirus havaitsee ja poistaa järjestelmistä virukset ja haittaohjelmat ja palomuuri estää ulkopuolisen tahon pääsyn järjestelmiin tietoliikenneverkon kautta. Työhön liittymättömien pelien ja sovellusten asentaminen työnantajan laitteisiin on kielletty. Myös nettisurffailu epäasiallisilla sivuilla voi vaarantaa koko kirkon tietoturvallisuuden, sillä niiden kautta laitteisiin voi asentua viruksia tai muita haittaohjelmia sekä vaikuttaa tietoliikenneverkon toimivuuteen.

Laittomien ohjelmistojen eli piraattikopioiden käyttäminen tai levittäminen on ehdottomasti kielletty. Ohjelmistoja tulee käyttää ainoastaan siihen tarkoitukseen, mihin se on käyttöehtojen mukaisesti sallittu. Työnantajan tarjoamia laitteita tai ohjelmistoja ei esimerkiksi saa käyttää omaan kaupallisen käyttöön. Toisaalta henkilökohtaiseen käyttöön hankituissa ohjelmistoissa saattaa olla rajoitteita, jotka estävät niiden käytön seurakuntatyössä.

Esimerkiksi kaikkia puhelimiin tarjolla olevia sovelluksia ei välttämättä voi käyttää työssä, vaan ne ovat kotikäyttöön suunnattuja. Usein sovelluksista onkin tarjolla erikseen maksullinen lisenssi eli käyttöoikeus, kun niitä hyödynnetään kaupalliseen käyttöön. Tarjolla voi olla myös ei-kaupalliseen käyttöön tarjolla olevia edullisempia lisenssejä, joita kirkko ja sen seurakunnat usein voivat hyödyntää.

Nykyisin seurakuntien käyttämät järjestelmät ovat pääasiassa hinnoiteltuja seurakunnan työntekijä- ja/tai laitemäärän mukaisesti, jolloin seurakunnan on seurattava lisenssien käyttöä ja ilmoitettava ohjelmistotoimittajalle säännöllisesti mahdollisista muutoksista. Myös seurakunnan jäsenmäärä voi olla hinnoittelun peruste. Vastuullinen ja tekijänoikeudet huomioiva järjestelmien käyttö on osa kyberturvallisuutta.

Suojaustoimenpiteet koskevat niin seurakunnan tietokoneita ja puhelimia kuin rakennusautomaatio- tai kameravalvontajärjestelmiä. Mikäli järjestelmät ovat yhteydessä Internetiin, niihin voidaan murtautua ja hyödyntää niitä osana palvelunestohyökkäyksiä, varastaa niistä tietoa tai muuten vaikuttaa niiden toimintaan. Mikäli laitteet eivät ole kytketty Internetiin, pitää kuitenkin varmistua, että laitetiloihin ei pääse ulkopuolisia henkilöitä käyttämään niitä tai varastamaan laitteita.

Tietojärjestelmien testaus- ja kehitysympäristöjen tulisi olla erillään tuotantoympäristöstä, jotta esimerkiksi päivitykset voidaan testata ennen tuotantojärjestelmiin asentamista ja havaita mahdolliset virheet. Testaus- ja kehitysympäristössä ei myöskään pitäisi säilyttää kriittistä tietoa.

Järjestelmien suojauksen näkökulmasta, on turvallisempaa käyttää niitä työnantajan tarjoamilla laitteille kuin henkilökohtaisilla laitteilla. Tämän vuoksi kirkon kriittisiin järjestelmiin onkin pääsy ainoastaan IT-tuen hallinnoimilla laitteilla, jolloin niiden kyberturvallisuudesta on huolehdittu tietoturvamääräysten edellyttämällä tavalla. Seurakunnan onkin varmistettava, että henkilöstölle on tarjolla tarvittavat tietotekniset laitteet työtehtävien hoitamista varten ja laitteiden turvallinen käyttö on opastettu. Kun työntekijän palvelussuhde tai luottamushenkilön luottamustoimi päättyy, hänen pitää palauttaa työnantajalta saamansa laitteet ja poistaa mahdolliset työnantajan tarjoamat kotikäyttöön tarjotut ohjelmistot henkilökohtaisilta laitteilta. Palvelussuhteen päättyessä on poistettava myös työntekijän tai luottamushenkilön käyttöoikeudet kirkon järjestelmiin.

II Suojaa laitteet

Laitteiden, kuten tietokoneiden ja matkapuhelimien, osalta pitää varmistaa, että näytöt lukitaan poistuttaessa työpisteeltä. Etätyön lisäännyttyä on huolehdittava laitteiden suojaaminen myös kotona ja matkustettaessa. Laitteita ei saa jättää nähtäville ilman valvontaa esimerkiksi seurakunnan asiakaspalvelu- tai neuvottelutiloihin tai autoon. Asiakastiloissa asiakkaiden käyttöön tarkoitetut laitteet ovat suositeltavaa lukita kiinni kalusteisiin varkauksien estämiseksi ja rajata asiakaskoneilla pääsy ainoastaan julkiseen Internetiin.

Laitteet ovat myös herkempiä rikkoontumisilta, kun etätyö edellyttää laitteiden mukana kuljettamista. Postitse tai seurakunnan sisäpostissa kuljetettavien laitteiden osalta on huolehdittava myös niiden tietoturvallisuudesta ja estettävä niiden rikkoontuminen. Rikkoontuneen laitteen mukana saatetaan menettää tärkeitä tietoja. Varastetusta tai rikkoontuneesta laitteesta pitää aina ilmoittaa esihenkilölle ja IT-alueen tekniseen tukeen. Laitteiden kiintolevyn salaamisella estetään ulkopuolisen pääsy laitteen tietoihin, mikäli laite varastetaan. Samaa koskee myös ulkoisia USB-muisteja, mikäli niissä kuljetaan luottamuksellista tietoa.

Laitteiden suojaus pitää huolehtia myös laitteen elinkaaren päättyessä. Tietokoneet, monitoimilaitteet, kameratallentimet, tietoliikennelaitteet, turvatuloksen tunnisteet ja puhelimet SIM- ja muistikortteineen pitää asianmukaisesti tyhjentää ennen kierrättämistä tai uudelleenkäyttöä. Useat seurakunnat hyödyntävät tietokoneissa elinkaarimallia, jossa laitteet hankitaan leasing-sopimuksella ja laitteen elinkaaren päättyessä ne tyhjennetään palveluntarjoajan toimesta tietoturvallisesti. Lisämaksusta palveluntarjoaja voi ottaa myös muut seurakunnan laitteet kierrätettäväksi tietoturvatyhjennys huomioiden.

Mikäli seurakunta myy tai lahjoittaa käytöstä poistettuja tietokoneita, puhelimia, kameroita tai muita laitteita, niiden tyhjennykseen pitää erityisesti kiinnittää huomioita. Käytetyt laitteet saattavat luottamuksellisten tietojen lisäksi sisältää tietoa kirkon tietoliikenneverkosta tai käyttäjätunnuksista, joita rikolliset voivat hyödyntää toiminnassaan. Lisäksi ne saattavat sisältää ohjelmistolisenssejä, joita vain kirkossa on lupa käyttää.

III Suojaa käyttäjätunnukset ja salasanat

Käyttäjätunnukset ovat aina henkilökohtaisia eikä niitä saa antaa muiden käyttöön. Kaikkien salasanojen pitää noudattaa kirkon tietoturvamääräyksiä. Salasanat pitää olla tarvittavan pitkiä ja täyttää kirkon kompleksisuusvaatimukset. Hyvä salasana on helppo muistaa, mutta vaikea arvata. Mikäli on epäily, että salasana on päätynyt muiden tietoon, se pitää välittömästi vaihtaa tai ilmoittaa tekniseen tukeen tunnuksen väliaikaisesta sulkemisesta. IT-tuki, työkaveri, pankki tai muu virallinen toimija ei koskaan pyydä työntekijän salasanaa puhelimitse, sähköpostilla tai muulla tavalla. Mikäli näin tapahtuu, se on huijaus ja siitä pitää aina ilmoittaa eteenpäin.

Testien mukaan esimerkiksi kuuden (6) merkin pituisen salasanan, jossa on pelkästään merkkejä ja pieniä kirjaimia, voi nykytietokoneet ratkaista muutamassa minuutissa brute force -tekniikalla eli väsytyshyökkäyksellä. Siinä tietokone laitetaan kirjautumaan johonkin järjestelmään, kuten työntekijän sähköpostiin, automaattisesti erilaisilla salasanoilla. Kun salasanaan lisätään isoja kirjaimia, salasana on edelleen mahdollista selvittää muutamassa tunnissa. Lisäämällä sekä merkkimäärää, että lisäämällä mukaan erikoismerkkejä, salasanasta tulee vasta turvallinen. Tämäkin silloin, kun salasan ei ole helposti arvattava, kuten esimerkiksi *Salasana1!*. Tietokoneiden kehittyessä, brute force -tekniikalla pystytään murtautumaan yhä nopeammin erilaisiin järjestelmiin, vaikka salasana olisikin vaikeasti arvattava. (Neskey, 2024.)

Käyttäjätunnuksia tai salasanoja ei saa säilyttää muistiin kirjoitettuna paikoissa, joissa ne ovat ulkopuolisen löydettävissä. Samaa salasanaa ei pidä käyttää kaikissa järjestelmissä. Hyvän salasanan tekemisestä on tarkemmin ohjeistettu Liitteessä 4.

Tietoliikennelaitteiden, langattomien verkkojen ja tietojärjestelmien oletussalasanat pitää aina vaihtaa. Sama koskee myös kotiverkkoja. Esimerkiksi tietoliikennelaitteiden oletuskäyttäjätunnukset ja -salasanat voi helposti selvittää laitteen käyttöohjeesta, jotka ovat yleensä saatavilla valmistajan sivuilta internetistä. Oletussalasanojen käyttäminen on merkittävä riski kyberturvallisuudelle ja altistaa tietomurroille.

IV Suojaa työntekijöiden käyttöoikeudet

Työntekijöiden käyttöoikeudet järjestelmiin myönnetään työtehtävien mukaisesti ja Zero Trust -periaatteen mukaisesti mahdollisimman pienillä oikeuksilla. Tämä minimoi työntekijän tekemien inhimillisten virheiden laajuuden. Myös mahdollisissa tietomurroissa rikollisilla on käytössä mahdollisimman vähäiset käyttöoikeudet ja näin voidaan estää laajempien tietomurtojen synty.

Mikäli työntekijän työtehtävät muuttuvat, pitää huolehtia myös tarpeettomien käyttöoikeuksien poistamisesta. Erityisen tärkeää on huolehtia tunnusten ja käyttöoikeuksien poistamisesta, kun työntekijän työt päättyvät. Onkin suositeltavaa hyödyntää mahdollisimman laajasti kertakirjautumista (Single Sing-On eli SSO). Kertakirjautumisessa eri järjestelmiin kirjautuminen tapahtuu samalla henkilökohtaisella käyttäjätunnuksella, jolla kirjaudutaan myös koneelle. Tällöin käyttöoikeudet eri järjestelmiin poistuvat automaattisesti käyttäjätunnuksen poistamisen yhteydessä.

Työntekijällä voi olla henkilökohtaisen käyttäjätunnuksen lisäksi erilaisia käyttäjätunnuksia ja -oikeuksia esimerkiksi seurakunnan sosiaalisen median palveluihin, pikaviestipalveluihin tai seurakunnan lukitus- ja kameravalvontajärjestelmiin. Myös näiden tunnusten ja oikeuksien rajoittaminen tai poistaminen on tärkeää työtehtävien muuttuessa tai päättyessä.

On tärkeää huomioida, että työsähköpostia käytetään ainoastaan työasioiden hoitoon. Vapaa-ajan asiointiin ja yhteydenpitoon pitää luoda erillinen sähköpostiosoite. Tämä sen vuoksi, että palvelussuhteen päättyessä työsähköposti ei ole enää käytettävissä. Mikäli esimerkiksi rekisteröidyt johonkin verkkokaupan asiakkaaksi työsähköpostilla, et palvelussuhteen päättyessä pääse enää esimerkiksi vaihtamaan verkkokaupan salasanaa tai et saa tietoa tehtyjen tilaustesi etenemisestä.

Sama koskee työpuhelinnumeroa ja työpuhelinta. Työpuhelinta käytetään ainoastaan työasioiden hoitoon. Palvelussuhteen päättyessä käytössä ollut puhelinnumero saatetaan siirtää toiselle työntekijälle seurakunnassa. Mikäli työntekijä on käyttänyt työnumeroa vapaa-ajan asioinnissa, siihen saattaa siirron jälkeen edelleen tulla esimerkiksi tekstiviestimuistutuksia verkkokauppatilauksista tai lääkärikäynneistä, viestejä pikaviestisovelluksista tai muita työasioihin kuulumattomia yhteydenottoja. Osa seurakunnista tarjoaa työntekijöilleen ja/tai luottamushenkilöilleen puhelinetua, jolloin työpuhelin on myös vapaa-ajan käytössä ja työnantaja maksaa myös työntekijän yksityispuhelut. Näiden osalta työnantajalla on omat tietoturvakäytännöt esimerkiksi palvelussuhteen tai luottamustoimen päättymisen yhteydessä.

V Suojaa kirjautuminen monivaiheisella tunnistautumisella

Kertakirjautumisen lisäksi kirjautumisessa pitää hyödyntää monivaiheista tunnistautumista (Multi-Factor Authentication eli MFA). Siinä kirjautuminen palveluun todennetaan käyttäjätunnuksen ja salasanan lisäksi henkilökohtaista työpuhelinta hyödyntäen. Mikäli käyttäjätunnus ja salasana ovat esimerkiksi tietojenkalastelun vuoksi päätyneet rikolliselle, kirjautuminen vaatii vielä puhelimella tunnistautumisen. Monivaiheinen tunnistautuminen voidaan tehdä esimerkiksi erillisellä Microsoft Authenticator -puhelinsovelluksella tai tekstiviestillä. Monivaiheinen tunnistautuminen parantaa oikein käytettynä merkittävästi kyberturvallisuutta.

Kirkon tietoturvaohjeistuksen mukaisesti jokaisen työntekijän pitää ottaa käyttöön monivaiheinen tunnistautuminen käyttäessään Microsoftin palveluita. Tämän lisäksi MFA:ta on syytä käyttää myös verkkokauppoihin ja muihin verkkopalveluihin kirjauduttaessa erityisesti silloin kun asiointi liittyy työtehtävien hoitoon.

Monivaiheinen tunnistautuminen pitää ottaa käyttää myös niissä palveluissa, joihin ei kirjauduta kirkon käyttäjätunnuksella, vaan käytetään seurakunnan palveluita oman henkilökohtaisen tilin kautta. Näitä palveluita voivat olla esimerkiksi seurakuntien sosiaalisen median palvelut, kuten Facebook tai YouTube. Yleisesti ottaen voidaan todeta, että MFA käyttö niin töissä kuin vapaa-ajalla on aina suositeltavaa.

VI Suojaa tiedot

Laitteiden, järjestelmien, käyttäjäoikeuksien lisäksi on suojattava myös varsinainen seurakunnan sähköinen tieto eli asiakirjat, kuvat, sähköpostit, järjestelmien lokitiedot yms. Pilvipalvelujen myötä työntekijöillä on nykyään käytännössä rajattomasti tallennustilaa henkilökohtaisessa sähköpostissa ja pilvitallennustilassa. On kuitenkin huomioitava, että näitä palveluja ei varmuuskopioida palveluntarjoajan toimesta, eivätkä ne ole virallisia seurakunnan (sähköisiä) arkistoja. Henkilökohtainen pilvitallennustila onkin tarkoitettu ainoastaan henkilökohtaisen tiedon tallentamiseen.

Mikäli seurakunnalle tärkeää tietoa on tallennettu ainoastaan työntekijän sähköpostiin tai henkilökohtaiseen pilvitallennustilaan, tieto häviää esimerkiksi työntekijän irtisanouduttua tai jäädessä eläkkeelle. Tällöin käyttäjätunnus poistetaan ja samalla poistuu myös henkilökohtainen sähköposti yhteystietoineen, pilvitallennustila, pilvitallennustilasta jaetut tiedostot Microsoft Teams -keskusteluryhmistä ja paljon muuta tietoa. Tärkeän tiedon, kuten sopimusten, menetyksellä voi olla seurakunnalle merkittäviä taloudellisia vaikutuksia.

Toisaalta tietoa pitäisi myös poistaa säännöllisesti. Esimerkiksi vanhoja sähköposteja, kalenterimerkintöjä ja yhteystietoja olisi syytä poistaa. Siivoamalla säännöllisesti sähköpostia tiedon löytyminen nopeutuu, mutta myös kyberturvallisuus parantuu tiedon vähentämisen myötä. Mikäli rikollinen pääsee esimerkiksi tietojenkalastelun kautta työntekijän sähköpostiin tai henkilökohtaiseen pilvitallennustilaan, riski tietojen väärinkäytölle on sitä pienempi mitä vähemmän tietoa on tarjolla. Sama koskee myös sähköpostijärjestelmän kalenterimerkintöjä tai yhteystietoja.

Tiedon suojaamista sähköpostiliikenteessä on mahdollista lisätä sähköpostin salauksella. Tämä on suositeltavaa erityisesti lähettämällä luottamuksellista aineistoa evl.fi-osoitteiden ulkopuolelle. Osa seurakunnista on hankkinut vielä lisäsuojausta joihinkin sähköpostiosoitteisiin erillisellä turvapostiominaisuudella, jolloin sähköpostin avaaminen edellyttää tekstiviestitse lähetettävää PIN-koodia. Turvapostin kautta voidaan sekä salata posti, että varmistua sen vastaanottajasta.

Mikäli on tarve kuljettaa luottamuksellista tietoa mukana, on silloin käytettävä salausominaisuuksilla varustettuja USB-muisteja. Vaikka tiedot olisivatkin suojattu, liittyy muistitikkuihin tai muihin ulkoisiin tallennusvälineisiin aina myös rikkoontumisen tai häviämisen riski. Tämän vuoksi niiden käyttöä olisi nykyisin syytä välttää ja käyttää sen sijaan henkilökohtaista pilvitallennustilaa. Muiden kuin työnantajan omistuksessa olevia muistilaitteita käytettäessä, on niiden tietoturvallisuudesta varmistuttava vähintään tarkistamalla ne virusten varalta.

Seurakunnissa pitäisikin olla tarkat ohjeet tiedon tallentamiseen ja säilyttämiseen. Seurakuntien arkistonmuodostussuunnitelmassa eli AMS:ssa on määritelty esimerkiksi asiakirjojen säilyttämisajat ja tallennuspaikat. Mikäli seurakunnalla ei ole käytössä sähköistä asian- ja dokumenttienhallintajärjestelmää, ainoa vaihtoehto on tulostaa esimerkiksi pysyvästi säilytettävät asiakirjat paperille ja arkistoida ne asianmukaisesti seurakunnan paperiarkistoon.

Viime vuosina näiden sähköisten asian- ja dokumenttienhallintajärjestelmien käyttö on lisääntynyt seurakunnissa. Sähköisessä asianhallintajärjestelmässä sähköinen arkistonmuodostussuunnitelma eAMS eli tiedonohjaussuunnitelma määrittää automaattisesti asiakirjojen säilytysajat ja mahdollisesti myös käyttöoikeudet asialle ja sen eri asiakirjoille. Sähköinen asianhallintajärjestelmä parantaa monella tapaa seurakunnan kyberturvallisuutta, sillä tiedon käytettävyys, eheys ja luottamuksellisuus on ennalta määritelty ja dokumentoitu.

Sähköisen asianhallintajärjestelmän ja henkilökohtaisen sähköpostin ja pilvitallennustilan lisäksi tietoa on myös seurakunnan muissa järjestelmissä. Esimerkiksi seurakuntien verkkoasemilla, intrassa, Microsoft Teamsissä sekä erityisesti asiakasrekistereissä on paljon suojattavaa tietoa. Näidenkin osalta tulisi tietoja myös pystyä poistamaan arkistonmuodostussuunnitelma ja lainsäädäntö huomioiden. Esimerkiksi asiakastiedot eri järjestelmistä sellaisten asiakkaiden osalta, jotka eivät ole pitkään aikaan olleet seurakunnan asiakkaina, tulisi poistaa tai ainakin anonymisoida eli muuttaa sellaiseen muotoon, josta asiakasta ei voi tunnistaa. Anonymisointi tietojen poiston sijaan voi olla tarpeen esimerkiksi tilastoinnin vuoksi.

VII Suojaa toimitilat

Seurakuntien tilajärjestelyjen pitää tukea kyberturvallisuutta. Tilat järjestellään siten, että ulkopuolisilla ei ole pääsyä seurakunnan toimistotiloihin, eikä sitä kautta seurakunnan laitteisiin ja tietoihin. Mikäli ulkopuolisia on tarve päästää toimisto- tai laitetiloihin, on huolehdittava heidän vastaanottamisesta sekä saattamisesta ulos tiloista. Myös kameravalvonnalla ja nykyaikaisella lukitusjärjestelmällä voidaan lisätä myös toimitilojen kyberturvallisuutta. Mikäli seurakunnilla on käytössään arkisto- tai laitetiloja, koskee niitä toimistotiloja tiukemmat ohjeet kulunvalvonnan ja lukituksen osalta.

Näköyhteys työntekijöiden näyttöpäätteille on estettävä esimerkiksi tilaratkaisuin ja näytön tietosuojakalvoilla. Ikkunat on syytä suojata verhoilla tai teippauksilla erityisesti niissä tiloissa, joissa käsitellään tai keskustellaan luottamuksellisesta tiedosta. Turvatulostus, jossa vaaditaan tunnistautuminen myös monitoimilaitteille, estää niiden ulkopuolisen käytön ja tulosteiden hallitsemattoman kerääntymisen laitteille.

Mikäli palveluntarjoajille, kuten kiinteistöhuollolle, annetaan vapaa pääsy seurakuntien tiloihin, on varmistettava salassapitositoumuksilla ja palvelusopimuksilla, että toimittaja ymmärtää myös tietoturvallisuuden vaatimukset palvelutuotannossa. Samat vaatimukset koskevat myös alihankkijoita.

Etätyössä on tärkeää huomioida, etteivät ulkopuoliset pääse seuraamaan tietokoneen käyttöä, kuulemaan luottamuksellisia keskusteluja tai urkkimaan luottamuksellisia tietoja tai salasanoja. Tarkemmin etätyön kyberturvakäytänteistä on hyvä sopia työntekijän ja työnantajan välillä etätyösopimuksessa.

7.3.Kyberuhkien havainnointi

Mikäli kirkkoon tai sen seurakuntaan kohdistuu tahallinen tai tahaton tietoturvapoikkeama tai sen yritys, pitää se osata myös havainnoida. Mitä enemmän tietoturvapoikkeamasta tai sen yrityksestä on oikeaa ja yksityiskohtaista tietoa, sitä helpompi siihen on reagoida riittävällä tavalla sekä estää vastaavat tapahtumat. Väärän tiedon saaminen sen sijaan hidastaa asian selvittämistä. Jokaisen työntekijän on tiedettävä, missä tilanteessa ja kenelle tietoturvapoikkeamista on ilmoitettava ja miten se tapahtuu. Tietoturvapoikkeamien ilmoittamisesta on tarkemmin kerrottu luvussa 8.

Havainnointi kerää tietoa esimerkiksi siitä, mitä on tapahtunut, milloin on tapahtunut, miten on tapahtunut ja kenelle on tapahtunut. Havaintoja tapahtumista kerätään useista eri lähteistä ja havainnointi seurakunnissa ja IT-alueilla on jatkuvaa. Työntekijöiden ja esihenkilöiden havainnot ja ilmoitukset tietoturvapoikkeamista ja/tai järjestelmien hälytykset ovat osa tätä kokonaisuutta. Esimerkiksi antivirusohjelman havaitessa ja poistaessa haittaohjelman seurakunnan laitteessa, lähtee siitä automaattisesti ilmoitus IT-alueen tai Kirkkohallituksen tekniseen tukeen. Tekninen tuki reagoi haittaohjelman aiheuttamaan tietoturvapoikkeamaan sitten parhaaksi katsomallaan tavalla.

Seurakunnissa on tiedettävä, mikä on normaalia tai epänormaalia toimintaa kyberturvallisuuden osalta. Tämän vuoksi tiedottaminen etukäteen esimerkiksi järjestelmien tai tietoliikenneverkon suunnitelluista huoltokatkoista on tärkeää. Sama koskee järjestelmiin tehtäviä päivityksiä tai suunniteltuja muutoksia työntekijöiden käyttöoikeuksiin. Kun työntekijät ovat etukäteen tietoisia tehtävistä muutoksista, tämä vähentää aiheettomia ilmoituksia mahdollisista tietoturvapoikkeamista.

Myös viranomaisten ilmoitusten seuraaminen maailmalla havaituista ohjelmistohaavoittuvuuksista on osa havainnointia. Esimerkiksi Kyberturvallisuuskeskus julkaisee verkkosivuillaan lähes päivittäin erilaisia haavoittuvuustiedotteita liittyen esimerkiksi tietoliikenneverkon laitteisiin ja ohjelmistoissa havaittuihin tietoturva-aukkoihin. Tiedotteissa on kerrottu, miten rikolliset ovat maailmalla haavoittuvuuksia hyödyntäneet ja kuinka ne voidaan korjata. Ensisijaisesti tiedotteet ovat tarkoitettu tekniselle tuelle, mutta niihin voi tutustua kuka tahansa asiasta kiinnostunut. Haavoittuvuustiedotteisiin voi tutustua osoitteessa https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet.

Nykyään kyberturvallisuusuhista ja kyberrikollisten tekemistä tietomurroista uutisoidaan laajasti eri medioissa. Lisäksi viranomaiset järjestävät erilaisia kampanjoita kyberturvallisuuden tietoisuuden lisäämiseksi. Näiden seuraaminen on myös osa havainnointia.

7.4. Reagointi kyberturvallisuuden häiriötilanteisiin

Kaikkiin saapuneisiin havainnointeihin, ilmoituksiin tai hälytyksiin on jollain tavalla reagoitava. Osa niistä on aiheettomia, eikä vaadi kyberturvallisuuden näkökulmasta toimenpiteitä. Esimerkiksi työntekijän ilmoitus tietokoneen toimimattomuudesta on ensisijaisesti teknisen tuen ratkaistavissa oleva ongelma kuin varsinainen tietoturvapoikkeama.

Mikäli tietoturvapoikkeama todetaan aiheelliseksi tai on vahva epäily kyberturvallisuuden vaarantumisesta, on pyrittävä estämään kaikin tavoin lisävahinkojen synty. Tähän on useita keinoja riippuen tapahtuneesta. Esimerkiksi jos on tiedossa, että työntekijän käyttäjätunnus ja salasana on tietojenkalastelun myötä joutunut vääriin käsiin, tekninen tuki sulkee väliaikaisesti työntekijän käyttäjätilin. Tuki voi estää myös sähköpostiliikenteen tietyltä lähettäjältä, jos on tiedossa, että osoitteesta lähetetään tietojenkalasteluviestejä. Myös yksittäisten tietojenkalasteluviestien tai haittaohjelmia sisältävien viestien poistamien on mahdollista teknisen tuen toimesta. Jos uhka kohdistuu johonkin laitteeseen, voidaan yksi tai useampi laite eristää tietoliikenneverkosta. Mikäli kyseessä on jokin tietojärjestelmä, voidaan se sammuttaa. Tämän jälkeen toteutetaan tarkempi analysointi ja toteutetaan toimenpiteet poikkeaman korjaamiseksi.

Havainnointiin ja reagointiin kehitetään jatkuvasti erilaisia teknisiä välineitä ja automatiikkaa myös kirkossa. Tämä ei kuitenkaan poista seurakuntien työntekijöiden velvollisuutta ilmoittaa havaituista asioista. Jotta toimenpiteet olisivat oikeanlaisia, pitää olla tarkkaa tietoa ongelman laajuudesta ja aiheuttajasta. On parempi kuitenkin ylireagoida ja tehdä tarvittavat varotoimenpiteet nopeasti kuin odottaa tekemättä mitään. Kyberturvallisuuden näkökulmasta koko Suomen evankelis-luterilainen kirkko on yhtä organisaatiota ja se mahdollistaa poikkeaman laajentumisen muihin laitteisiin, järjestelmiin tai tietoliikenneverkkoihin. Myös leviäminen muihin organisaatioihin on mahdollista.

Tietoturvapoikkeama voi olla hetkellinen tai kestää viikkoja. Se voi kohdistua yksittäiseen laitteeseen tai työntekijään. Vakavassa tapauksessa kokonaiseen järjestelmään ja tuhansiin rekisteröityihin seurakuntalaisiin tai seurakunnan asiakkaisiin. Tämän vuoksi esimerkiksi yksittäiseen seurakuntaan kohdistuvat tietomurrot voisivat nousta valtakunnan uutisiin ja aiheuttaa laajasti kyselyjä seurakuntalaisilta eri seurakuntiin.

Tämän vuoksi myös (kriisi)viestintä ja johtaminen on tärkeä osa reagointia. Kun mahdollisista varotoimenpiteiden tekemisestä on etukäteen tiedotettu henkilöstöä ja ne ovat seurakunnan johdossa hyväksyttyjä, niiden toteuttaminen on tositilanteessa helpompaan ja nopeampaa. Ajantasaisen dokumentaation avulla ehkäiseviä ja korjaavia toimenpiteitä voi toteuttaa myös ne henkilöt, jotka eivät päivittäin ole tekemissä tietoturvallisuuden kanssa.

Poikkeamatilanteisiin reagointia ja viestintää onkin suositeltavaa harjoitella säännöllisin väliajoin joko järjestämällä harjoituksia tai osallistumalla ulkopuolisen tahon järjestämään harjoitukseen. Esimerkiksi Digi- ja väestötietoviraston vuosittain järjestämä valtakunnallinen kyberturvallisuutta koskeva Taisto-harjoitus tarjoaa turvallisen tilaisuuden harjoitella, testata ja kehittää toimintamalleja kuvitteellisten häiriötilanteiden kautta.

Toinen kyberturvallisuuteen liittyvä valtakunnallinen harjoitus on Digipoolin järjestämä Tieto-harjoitus, joka koostuu useammasta harjoittelujaksosta ja se on jaettu usealle vuodelle. Seurakunnassa pitäisikin olla varauduttu erilaisiin kyberuhkiin valmiussuunnittelussa. Esimerkiksi palvelunestohyökkäys kirkon tai seurakunnan tietoliikenneverkkoon saattaa pysäyttää koko seurakunnan toiminnan useaksi päiväksi. Myös seurakunnan viestinnässä olisi hyvä varautua erilaisiin tilanteisiin etukäteen valmistelluilla kriisiviestinnän tiedotepohjilla. (Digi- ja väestötietovirasto 2023, Digipooli, 2024.)

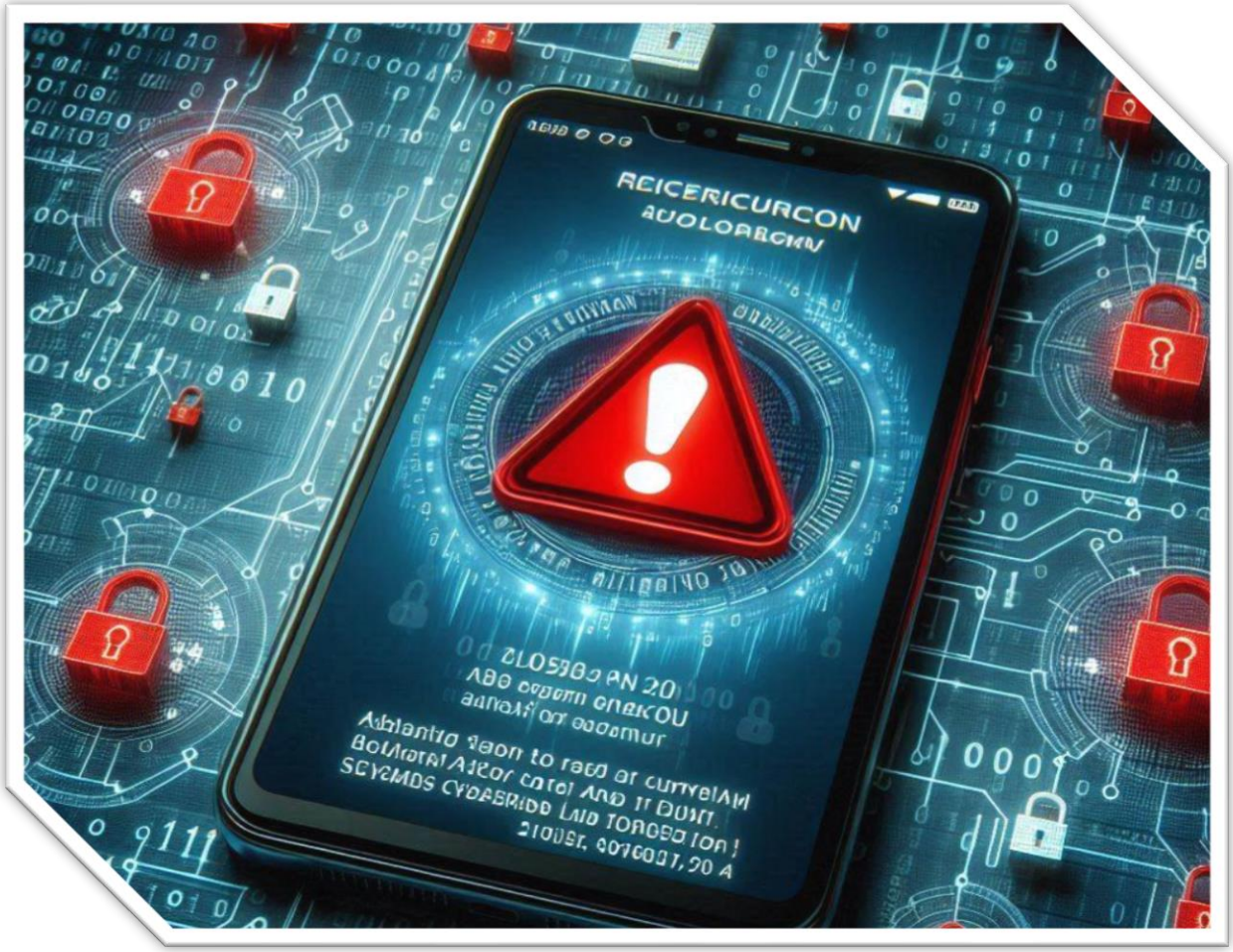
7.5. Palautuminen kyberturvallisuuden häiriötilanteesta

Mikäli seurakuntaan kohdistuu erilaisista suojaustoimista huolimatta esimerkiksi tietomurto tai palvelunestohyökkäys, on siitä osattava myös palautua. Säännöllisellä harjoittelulla ja valmiussuunnitellulla sekä tarvittavilla resursseilla, toipuminen kyberhyökkäyksestä on nopeampaa. Jatkotoimenpiteet vastaavan tapahtuman estämiseksi on toteutettava pikaisesti ja viestintä eri sidosryhmille tapahtuneesta on tärkeää. Näin muut organisaatiot voivat varautua toiminnassaan vastaaviin uhkiin ja estää vastaavat tapahtumat omassa digitaalisessa ympäristössä. Avoin ja säännöllinen viestintä myös mainehaitan minimoimiseksi on tärkeää.

Tietomurto, palvelunestohyökkäys tai esimerkiksi työntekijän virhe on voinut estää kirkon yhteisten järjestelmien tai seurakunnan oman järjestelmän käytön useiksi päiviksi. Tällöin on voitu jo siirtyä varautumissuunnitelman mukaisiin manuaalisiin työtapoihin esimerkiksi kirjaamalla asiat paperille tai toiseen järjestelmään. Kun järjestelmät saadaan jälleen käyttöön ja palaudutaan normaaliin toimintatilaan, on tiedon eheyden vuoksi välttämätöntä tallentaa tiedot jälkikäteen oikein järjestelmiin.

Mitä kriittisempi järjestelmä on kyseessä, sitä tarkemmin tiedot pitää järjestelmään tallentaa. Esimerkiksi talous- ja henkilöstöhallinnon järjestelmien tai Kirjuri-jäsentietojärjestelmän tietojen eheys ovat riippuvaisia kaikista sinne tehdyistä päivittäisistä muutoksista, joita työntekijät tai muut järjestelmät sinne automaattisesti tekevät. Mikäli tietoja joudutaan jälkikäteen korjaamaan tai syöttämään, tämä voi viedä aikaa useita päiviä tai jopa viikkoja järjestelmän käyttökatkon pituuden mukaan. Tietojen syöttö jälkikäteen voi tarvita myös merkittäviä lisäresursseja seurakunnassa.

Normaalioloihin palautumisen jälkeen, on tärkeää dokumentoida tapahtunut tarkasti. Mikäli kyseessä on ollut tietomurto, se on rikos, ja sen selvittely voi vaatia useita vuosia. Dokumentointi auttaa myös kehittämään seurakunnan ja koko kirkon valmiutta sekä suojautumaan jatkossa vastaavilta tapahtumilta.



8. KYBERTURVAPOIKKEAMASTA ILMOITTAMINEN

Kyberturvapoikkeamalla tai tietoturvapoikkeamalla tarkoitetaan esimerkiksi niitä kyberuhkia, joita luvussa 5 on kuvattu. Eli tietojenkalastelua, tietomurtoja, palvelunestohyökkäyksiä tai näiden yrityksiä. Mikäli havaitset tietoturvapoikkeaman seurakunnassasi, ota yhteys seurakuntasi tietoturvan yhdyshenkilöön ja/tai IT-alueesi tietoturvavastaavaan. Kirkon IT-alueiden tietoturvavastaavat ovat lueteltuna liitteessä 6.

Kirkon tietoturvavastaavat tekevät valtakunnallista yhteistyötä ja ilmoittavat tarvittaessa poikkeamista Kyberturvallisuuskeskukselle. Jotta virallinen ilmoitus voidaan tehdä, kerää mahdollisimman tarkat tiedot havaitsemastasi poikkeamasta. Mitä on tapahtunut, kenelle ja milloin on tapahtunut, mahdollisimman tarkka kuvaus tapahtumasta, liitteeksi alkuperäinen viesti tai kuvakaappaus sekä arvio millaista vahinkoa seurakunnalle tapahtumasta voi koitua. Mikäli korjaaviin toimenpiteisiin on jo ryhdytty, on ne hyvä tuoda myös esiin ilmoituksessa.

Tärkeintä on tehdä ilmoitus havaituista poikkeamista seurakuntasi tietoturvan yhdyshenkilölle ja/tai IT-alueen tietoturvavastaavalla pienellä kynnyksellä sekä mahdollisimman pian. Tällä tavoin poikkeamiin voidaan puuttua nopeasti ja estää laajempien ongelmien syntyminen esimerkiksi tiedottamalla koko kirkon henkilöstöä tai toteuttamalla korjaavat tekniset toimenpiteet.

Mikäli IT-alueen tietoturvavastaava näkee tarpeelliseksi tehdä virallinen ilmoitus Kyberturvallisuuskeskukselle, hän hoitaa ilmoittamisen seurakunnan puolesta. Kirkon yhteisten palveluiden osalta ilmoituksen Kyberturvallisuuskeskukselle tekee Kirkkohallituksen tietoturvapäällikkö tai hänen sijaisensa.

Ilmoitusten avulla Kyberturvallisuuskeskus kerää jatkuvasti ajankohtaista tilannekuvaa kyberturvallisuudesta Suomessa ja on tarvittaessa seurakunnan apuna tietoturvapoikkeaman selvittämisessä. Ilmoitukset voidaan tehdä sähköisellä lomakkeella Kyberturvallisuuskeskuksen nettisivujen kautta. Mikäli kyseessä epäillään tapahtuneen rikoksen, tietoturvapoikkeama voi aiheuttaa myös rikosilmoituksen tekemisen Poliisille.

Mikäli on epäily, että tietoturvapoikkeamassa on mahdollisesti henkilötietoja tuhoutunut, hävinnyt, muuttunut tai niihin on päässyt käsiksi taho, jolla ei ole niihin oikeutta, ota yhteys myös seurakuntasi tietosuojan yhdyshenkilöön ja tietosuojavastaavaan. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä eli seurakunta on tullut tietoiseksi henkilötietojen tietoturvaloukkauksesta. Henkilötietojen tietoturvaloukkaukset voidaan ilmoittaa sähköisellä lomakkeella tietosuojavaltuutetun toimiston nettisivujen kautta.

Henkilötietojen tietoturvaloukkauksesta on mahdollisesti ilmoitettava myös rekisteröidylle eli henkilölle, jonka tietoja loukkaus koskee. Ilmoitus on tehtävä, jos se aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisteröidylle ilmoitus pitää hoitaa henkilökohtaisesti tai julkisella tiedonannolla jos henkilökohtainen yhteydenotto ei ole mahdollista.

Henkilötietojen tietoturvaloukkausten ilmoitusvelvollisuus on aina rekisterinpitäjällä eli seurakunnalla. Ilmoituksen tekeminen on hyvä tehdä yhteistyössä seurakunnan tietosuojan yhdyshenkilön ja tietosuojavastaavan kanssa sekä tarvittaessa myös seurakunnan tietoturvan yhdyshenkilön ja IT-alueen tietoturvavastaavan kanssa.

Riippumatta siitä, millaisia toimenpiteitä tai viranomaisilmoituksia havaittu tietoturvapoikkeama vaatii, seurakunnan pitää dokumentoida tietoonsa saadut tietoturvapoikkeamat. Ilmoituksia voidaan sitten hyödyntää esimerkiksi henkilöstön koulutuksia suunniteltaessa, seurakunnan toimintakertomuksessa, kyberturvallisuuden kehittämisessä tai yleisen kyberturvallisuuden tilannekuvan ylläpitämisessä.

9. LINKKIVINKIT KYBERTURVALLISUUDESTA

Tähän on kerätty laajasti erilaista materiaalia tietosuojaan, tietoturvallisuuteen ja kyberturvallisuuteen Suomen evankelis-luterilainen kirkko huomioiden. Internetistä löytyy muun muassa maksuttomia verkkosivuja, TV-ohjelmia, podcasteja, mobiilipelejä ja kokonaisia verkkokursseja liittyen kyberturvallisuuteen. Osa palveluista saattaa edellyttää käyttäjätilin luomista palveluun.

⚖️ Lainsäädäntö

- Asiakastietolaki eli laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) 4–7, 9–15 ja 17 §, 19 §:n 1 momenttia, 22, 24, 37–42, 44, 45, 50–52, 62 ja 63 §
- EU:n yleinen tietosuoja-asetus GDPR (2016/679) ja Tietosuojalaki (1050/2018)
- Digipalvelulaki eli laki digitaalisten palvelujen tarjoamisesta (306/2019)
- Julkisuuslaki eli laki viranomaisten toiminnan julkisuudesta (621/1999)
- Kirkkolaki (652/2023) ja kirkkojärjestys (657/2023)
- Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016)
- Rikoslaki (39/1889)
- Tiedonhallintalaki eli laki julkisen hallinnon tiedonhallinnasta (906/2019) 4 §:n 2 momentti, 12—17 ja 21—24 §:ää sekä 6 luku
- Työelämän tietosuojalaki eli laki yksityisyyden suojasta työelämässä (759/2004)
- Valmiuslaki (1522/2011)

✉️ Kirkkohallituksen yleiskirjeet

- 19/2024 Kirkkolain 3 ja 8 luvun muutokset (mm. henkilötietojen käsittely diakoniatyössä)
- 17/2024 Suosituksia saavutettavuuden kehittämiseen seurakunnissa
- 12/2024 Seurakuntien palvelut palvelutietovarantoon
- 30/2023 Kirkkolakiuudistuksen vaikutus kirkon arkistotoimeen 1.7.2023 alkaen
- 29/2023 Hallintosääntö
- 26/2023 Seurakuntien ja seurakuntayhtymien päätöksistä tiedottaminen sekä oikaisuvaatimusohjeet ja valitusosoitukset
- 19/2023 Henkilötietojen käsittelyn sääntely tarkentuu uuden kirkkolain myötä
- 16/2023 Tiedonhallintalain soveltaminen kirkossa
- 4/2023 Ilmoittajansuojelulaki
- 30/2022 Kirkon säädöskokoelma nro 159–2022 kirkkohallituksen päätös kirkon tietoturvapolitiikasta ja yleisistä tietoturvamääräyksistä
- 10/2020 Suomi.fi-viestit -palvelun käyttöönotto
- 14/2019 Seurakunnan valmiussuunnitelman laatimisohje 2019

Yleiskirjeet ovat luettavissa osoitteesta
https://evl.fi/plus/paatoksenteko/kirkkohallitus/kirkkohallituksen-yleiskirjeet/

💻 Verkkosivut

- Digi- ja väestötietoviraston Digiturvapalvelut - https://dvv.fi/digiturva
- Digipooli - https://www.digipooli.fi
- Huijarille luu kurkkuun! -kampanjasivusto - https://www.huijaamaton.fi
- Huoltovarmuuskeskus - https://www.huoltovarmuuskeskus.fi
- Huoltovarmuuskeskuksen Varmuuden vuoksi -verkkolehti - https://www.varmuudenvuoksi.fi/
- Kyberturvallisuuskeskus - https://www.kyberturvallisuuskeskus.fi
- Nyt valppaana - kampanjasivusto - https://nytvalppaana.fi/
- Poliisi – kyberrikokset - https://poliisi.fi/kyberrikokset
- Sakastin Tietoturva ja tietosuoja -sivusto - https://sakasti.fi/hallinto-ja-talous/tietosuoja*
- Tietosuojavaltuutetun toimisto - https://tietosuoja.fi
- Tuovi – sisäisen turvallisuuden portaali - https://sisainenturvallisuus.fi

* Sakastin Tietoturva ja tietosuoja -sivusto on osa kirkon työntekijöille suunnattua suljettua intranetiä.

👨‍🎓 Verkkokurssit

- Avoimet kyberturvallisuuskurssit yliopistoissa (Ficom) - https://ficom.fi/digiala/avoimia-kyberturvallisuuskoulutuksia/
- Digitreenit – Tietoturva (YLE) - https://yle.fi/aihe/digitreenit/tietoturva
- Digiturma vai digiturva – täsmäiskut oppimiseen (DVV) - https://www.youtube.com/playlist?list=PL1_-EIQ-Ddub-gVbetAX0qKVPhcdf-ar3
- eOppiva - https://www.eoppiva.fi/koulutus-kokonaisuudet/turvallisuus/
- Hakkerin tietoiskut (Yle) - https://yle.fi/aihe/a/20-10001759
- Kansalaisen kyberturvallisuus (Jyväskylän yliopisto) - https://onlinecourses.jyu.fi/course/view.php?id=60
- Taitoja työelämään (Microsoft) - https://www.microsoft.com/fi-fi/skills-for-jobs/

🎮 Mobiilipelit

- Kyberturvallisuuspeli Cyber Citizen - https://cyber-citizen.eu/
- Digiturvallinen elämä (DVV) - https://dvv.fi/digiturvallinen-elama
- Kyberturvallisuuspeli Spoofy (CGI ja kumppanit) - https://www.spoofy.fi

🎉 Tapahtumat, messut ja seminaarit

- Digiturvallisuusmessut - https://www.paviljonki.fi/messut/digiturvallisuusmessut/
- Digiturvaviikko - https://dvv.fi/digiturvaviikko
- Kybertuskapäivä - https://digiportaat.fi/koulutukset/kybertuska-2024-2
- Tietoturva-seminaari - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tapahtumat/tietoturva-2024-seminaari

📺 TV-ohjelmat (Yle areena)

- Kybersoturit - https://areena.yle.fi/1-66193016

”Kaksiosainen dokumentti neljästä norjalaismiehestä, jotka yrittävät vaikuttaa Venäjään kybertoiminnan kautta.”

- Team Whack - kaikki on hakkeroitavissa - https://areena.yle.fi/1-4664681

”Kolme ammattihakkeria paljastaa, kuinka sinunkin elämäsi voidaan sekoittaa. Toisella kaudella kohteeksi joutuvat yksityiset älylaitteet, pelistriimi ja vakuutusyhtiö. Ensimmäisellä kaudella kohteina olivat älylaitteiden lisäksi mm. henkilöauto ja kokonainen taloyhtiö. Tavoitteena on auttaa suojautumaan hyökkäyksiltä.”

📹 Podcastit ja webinaarit

- Digiturvakompassi - https://www.eoppiva.fi/podcast/digiturvakompassi

”Digitaalisesta turvallisuudesta puhutaan paljon, mutta mitä sillä oikeastaan tarkoitetaan? Miten digitaalista turvallisuutta kehitetään? Näiden ja monien muiden kysymysten äärelle johdattaa #digiturvakompassi. Podcastissa näistä teemoista keskustelevat tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä ja VAHTI-pääsihteeri Kimmo Rousku Digi- ja väestötietovirastosta, jotka molemmat työkseen edistävät julkisen hallinnon digiturvallisuutta.”

- Digiturvatunti https://dvv.fi/digiturvatilaisuudet

”Webinaarisarja summaa kuukausittain 60 minuuttiin digimaailman uhkat, joita meihin kaikkiin kohdistuu töissä ja vapaa-ajalla, sekä tarjoaa vinkkejä niiltä suojautumiseen. Käymme läpi uusimmat huijausyritykset, julkaisemme ajankohtaisen lyhyen koulutusvideon ja vastaamme meille esitettyihin kysymyksiin.”

- Herrasmieshakkerit - https://hakkerit.libsyn.com

”Tervetuloa Herrasmieshakkereiden kartanoon takkatulen ääreen. Tässä ohjelmasarjassa käsittelemme tietoturvaan ja vääjäämättömään kybertuhoon liittyviä asioita ja ilmiöitä. Oppaananne verkon alamaailmassa toimivat Suomen tietoturvakentän wiralliset wanhukset Mikko Hyppönen ja Tomi Tuominen.”

- Kyberin ytimessä - https://podcasters.spotify.com/pod/show/kyberin-ytimessa

”Digitaalinen turvallisuus koskettaa meitä kaikkia. Matkalla kyberin ytimeen pureudutaan alan ajankohtaisiin aiheisiin, uutisiin ja ilmiöihin kansankielisesti. Asiantuntijat kertovat mitä digitaalisessa maailmassa tapahtuu juuri nyt. Sukella kanssamme kyberin ytimeen!

Podcast on Keski-Suomen kyberturvallisuusosaamisen tunnettavuuden kasvattaminen -hankkeen tuottama. Rahoittajina toimii Keski-Suomen liitto, AKKE-rahoitusohjelma, sekä hankkeen toteuttajat Jyväskylän ammattikorkeakoulu ja Jyväskylän yliopisto.”

- Kyberrosvot - https://www.dna.fi/yrityksille/kyberrosvot-podcast

”Kyberrosvot on Tivin & DNA:n yhteistyössä toteuttama true crime -podcast, joka esittelee kiinnostavia kyberrikostapauksia Suomesta ja ulkomailta. NotPetya - onko tässä maailman kyberhistorian tuhoisin haittaohjelma? Mitä tapahtui Psykoterapiakeskus Vastaamossa, kun portti numero 3306 jäi auki? Kuka halusi kaataa Iltalehden? Ja keitä nämä kyberrosvot oikein ovat?

Juontajana Peter Nyman, vakiovieraana DNA:n tietoturvaliiketoiminnan asiantuntija Juho Saarinen ja vaihtuvina vieraina Suomen eturivin kyberasiantuntijat.”

- Turvakäräjät - https://turvakarajat.fi

”Ajankohtaista kyberiä, melkein Suomen kielellä. Käräjillä mukana Antti Kurittu, Laura Kankaala ja Juho Jauhiainen.”

LÄHTEET

Finanssiala ry 2024. Huijaukset kovassa kasvussa – pankit onnistuivat pysäyttämään yli 18 miljoonaa euroa huijattua rahaa. WWW-dokumentti. https://www.finanssiala.fi/uutiset/huijaukset-kovassa-kasvussa-pankit-onnistuivat-pysayttamaan-yli-18-miljoonaa-euroa-huijattua-rahaa/. Päivitetty 17.9.2024. Luettu 20.9.2024.

Digi- ja väestötietovirasto 2022. Digitaalisen turvallisuuden arkkitehtuuri. WWW-dokumentti. https://wiki.dvv.fi/display/DTARK/Digitaalisen+turvallisuuden+arkkitehtuuri. Päivitetty 12.12.2022. Luettu 10.1.2024.

Digi- ja väestötietovirasto 2023. Taisto-harjoitus. WWW-dokumentti. https://dvv.fi/taisto. Päivitetty 18.12.2023. Luettu 10.1.2024.

Digipalvelulaki eli laki digitaalisten palvelujen tarjoamisesta 306/2019. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Digipooli 2024. TIETO24-Harjoitus - Tietoyhteiskunnan valmiusharjoitus. WWW-dokumentti. https://www.digipooli.fi/fi/tieto24. Päivitetty 5.12.2023. Luettu 15.4.2024.

EU:n kyberturvallisuusvirasto 2022. Suurimmat kyberuhat EU:ssa. WWW-dokumentti. https://www.consilium.europa.eu/fi/infographics/cyber-threats-eu/. Päivitetty 2.2.2023. Luettu 1.11.2023.

Hallintolaki 434/2003. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Helsingin kaupunki 2024. Kasvatuksen ja koulutuksen tietomurto. WWW-sivusto. https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto. Päivitetty 12.7.2024. Luettu 11.8.2024.

Iltasanomat 2024. Kuvia ihmisten passeista päätynyt kyber-rikollisille – aineistoa huuto-kaupattu pimeässä verkossa. WWW-dokumentti. https://www.is.fi/digitoday/tietoturva/art-2000010118858.html. Päivitetty 14.1.2024. Luettu 15.1.2024.

Jyväskylän ortodoksinen seurakunta 2023. Huijausviestejä liikkeellä kirkkoherran nimissä. WWW-dokumentti. https://jklort.fi/2023/12/21/huijausviesteja-liikkeella-kirkkoherran-nimissa/. Päivitetty 21.12.2023. Luettu 21.12.2023.

Jyväskylän seurakunta 2024. Taulumäen kirkkoon on murtauduttu. WWW-sivusto. https://www.jyvaskylanseurakunta.fi/uutiset/-/news/148302791. Luettu 18.7.2024. Päivitetty 17.7.2024

Kangasalan seurakunta 2019. Tiedote: Kangasalan seurakunta on joutunut maksurikospetoksen uhriksi. WWW-sivusto. https://www.kangasalanseurakunta.fi/uutiset/-/news/55389820. Luettu 15.1.2024. Päivitetty 15.9.2019.

Kirkkojen maailmanjärjestö 2023. WCC hit by ransomware attack. WWW-dokumentti. https://www.oikoumene.org/news/wcc-hit-by-ransomware-attack. Päivitetty 23.12.2023. Luettu 15.1.2024.

Kirkkohallitus 2019. Virastonhoidon ohjeet. Kirkon työntekijöiden intranet. WWW-dokumentti. Ei päivitystietoa. Luettu 4.4.2023.

Kirkkolaki 652/2023. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Kirkon viestintä 2020. Kauneimmat Joululaulut -FB-tapahtumiin kohdistunut huijausyrityksiä – Ohje seurakunnille (12.12.). WWW-dokumentti. https://sakasti.fi/ajankohtaista/kauneimmat-joululaulut-tapahtumiin-facebookissa-on-kohdistunut-huijausyrityksia-ohje-seurakunnille/. Päivitetty 10.12.2020. Luettu 14.4.2024.

Kyberturvallisuuskeskus 2023a. Pidempi parempi - Näin teet hyvän salasanan. WWW-dokumentti. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan. Päivitetty 13.7.2023. Luettu 3.1.2024.

Kyberturvallisuuskeskus 2023b. Varoitus 1/2023. Tietomurtoaalto leviää organisaatiosta toiseen – katkaise tietojenkalastelu. WWW-sivusto. https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoaalto-leviaa-organisaatiosta-toiseen-katkaise-tietojenkalastelu. Päivitetty 8.11.2023. Luettu 21.10.2023.

Laki yksityisyyden suojasta työelämässä 759/2004. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Microsoft 2020. Mitä kyberturvallisuus on? WWW-sivusto. https://support.microsoft.com/fi-fi/topic/mit%C3%A4-kyberturvallisuus-on-8b6efd59-41ff-4743-87c8-0850a352a390. Ei päivitystietoa. Luettu 5.11.2023.

Neskey, Corey 2024. Are Your Passwords in the Green?. WWW-dokumentti. https://www.hivesystems.com/blog/are-your-passwords-in-the-green. Ei päivitystietoa. Luettu 1.5.2024.

Ruotsin kirkko 2023. Cyberangrepp mot Svenska kyrkan. WWW-dokumentti. https://via.tt.se/pressmeddelande/3393640/allvarlig-driftsstorning-hos-svenska-kyrkan?publisherId=1344892&lang=sv. Päivitetty 8.1.2024. Luettu 10.1.2024.

Sanastokeskus 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. EI päivitystietoa. Luettu 20.11.2023.

Suomen ev.lut. kirkko 2019. Seurakunnan valmiussuunnitelma. WWW-dokumentti. https://sakasti.fi/kriisit-ja-varautuminen/nain-varaudut/seurakunnan-valmiussuunnitelma/. Ei päivitystietoa. Luettu 3.1.2024.

Suomen ev.lut. kirkko 2020. Suomen evankelis-luterilaisen kirkon strategia vuoteen 2026. PDF-dokumentti. https://evl.fi/plus/wp-content/uploads/sites/3/2023/09/Ev.lut_.kirkko-strategia.pdf. Ei päivitystietoa. Luettu 1.11.2023. OK

Suomen ev.lut. kirkko 2022a. Kirkon tietoturvapolitiikka. PDF-dokumentti. https://evl.fi/documents/1327140/97032515/30_2022+liite+2+159-2022+Kirkon+tietoturvapolitiikka+2022.pdf. Päivitetty 30.11.2022. Luettu 20.11.2023.

Suomen ev.lut. kirkko 2022b. Kirkon yleiset tietoturvamääräykset. PDF-dokumentti. Salainen. Päivitetty 30.11.2022. Luettu 20.11.2023.

Suomen ev.lut. kirkko 2024a. Kirkon digitalisaatiostrategia 2026–2031 - Projektisuunnitelma. PDF-dokumentti. Päivitetty 15.4.2024. Luettu 15.4.2024.

Suomen ev.lut. kirkko 2024b. Piispantarkastuksen hallinnon ja tarkastuksen ohjeet. PDF-dokumentti. Luettu 17.1.2024.

Tiedonhallintalaki eli Laki julkisen hallinnon tiedonhallinnasta. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Tietosuojalaki 1015/2018. http://www.finlex.fi. Ei päivitystietoa. Luettu 5.11.2023.

Tietosuojavaltuutetun toimisto 2024. Julkaisimme päivitetyt ohjeet tietosuojavastaavan nimittäneelle organisaatiolle. https://tietosuoja.fi/-/julkaisimme-paivitetyt-ohjeet-tietosuojavastaavan-nimittaneelle-organisaatiolle. WWW-dokumentti. Päivitetty 18.6.2024. Luettu 1.7.2024.

Valtioneuvosto 2022. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukeva työryhmä. WWW-dokumentti. https://valtioneuvosto.fi/hanke?tunnus=LVM044%3A00/2022. Ei päivitystietoa. Luettu 1.2.2024.

Valtioneuvosto 2023. Valtioneuvoston julkaisuja 2023:58. Pääministeri Petteri Orpon hallituksen ohjelma 20.6.2023. PDF-dokumentti. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165042/Paaministeri-Petteri-Orpon-hallituksen-ohjelma-20062023.pdf. Ei päivitystietoa. Luettu 21.11.2023.

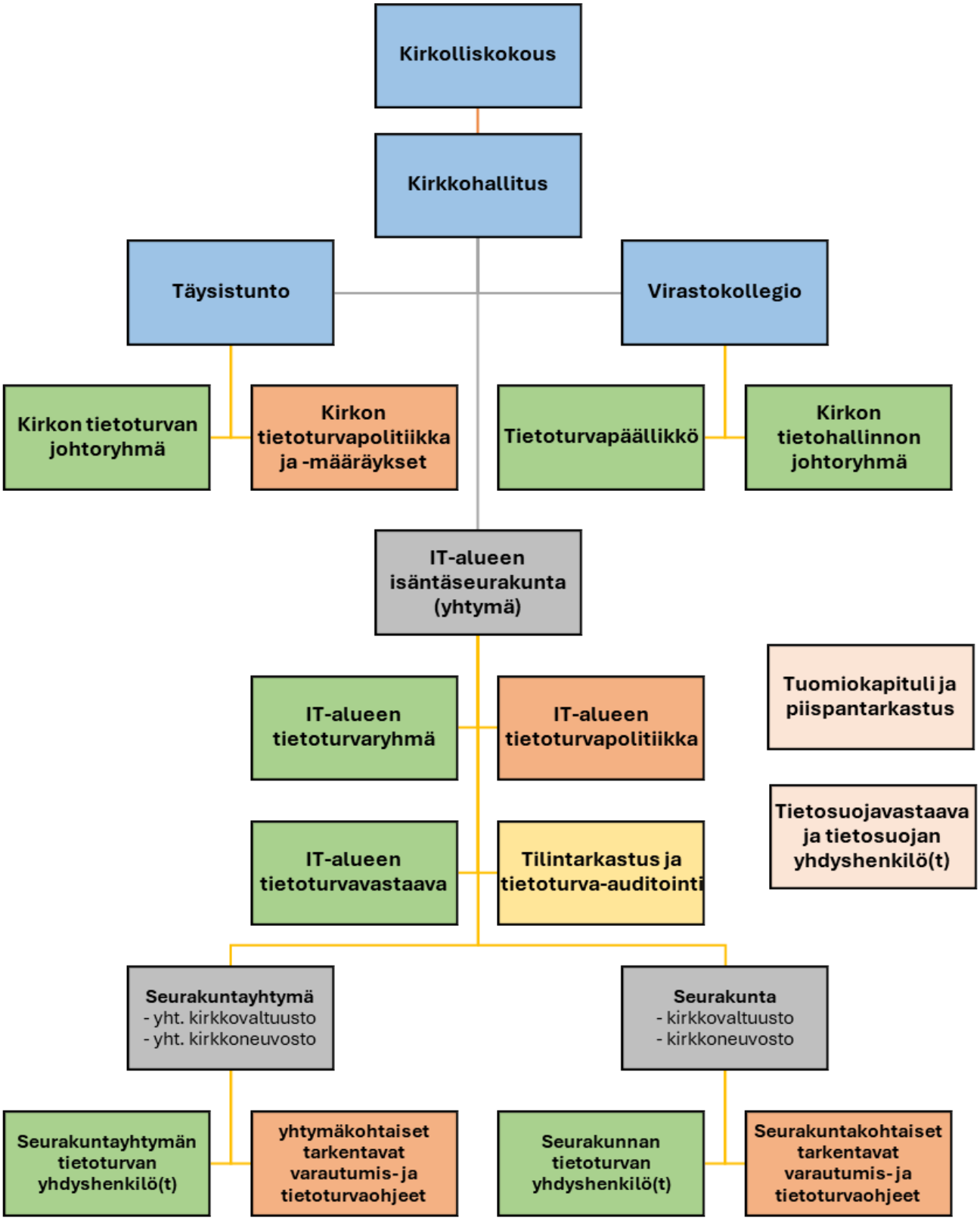
Wikipedia 2024. Vastaamon tietomurto. WWW-dokumentti. https://fi.wikipedia.org/wiki/Vastaamon_tietomurto. Päivitetty 16.11.2023. Luettu 15.1.2024.

Sisäministeriö. Kyberrikollisuus - Sisäministeriö (intermin.fi). Luettu 6.1.2024.

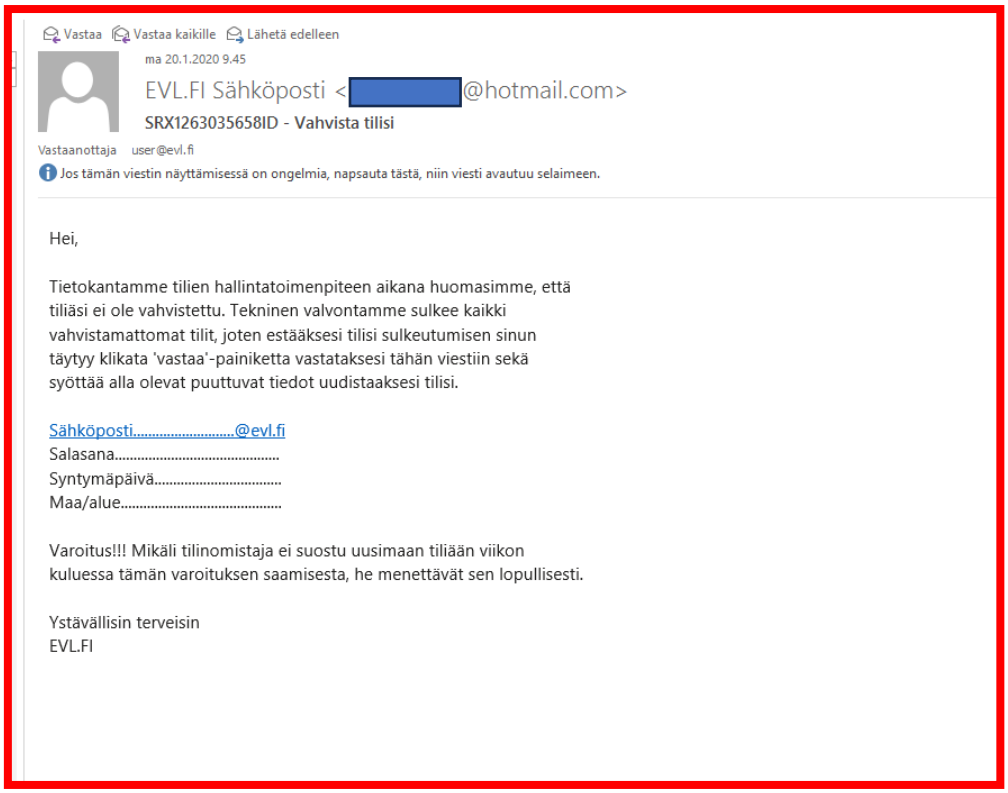
10. LIITTEET

LIITE 1 – Suomen evankelis-luterilaisen kirkon tietoturvaorganisaatio
LIITE 2 – Esimerkkejä huijausviesteistä
LIITE 3 – Huoneentaulu - näin tunnistat tietojenkalastelun
LIITE 4 – Huoneentaulu - näin teet hyvän salasanan
LIITE 5 – Seurakunnan kyberuhkien arviointi (malli)
LIITE 6 – Suomen evankelis-luterilaisen kirkon IT-alueiden tietoturvavastaavat
LIITE 7 – Kyberturvallisuus seurakunnassa -työkirja

LIITE 1 – Suomen evankelis-luterilaisen kirkon tietoturvaorganisaatio



LIITE 2 – Esimerkkejä huijausviesteistä



Vastaa Vastaa kaikille Lähetä edelleen

ma 20.1.2020 9.45

EVL.FI Sähköposti <[redacted]@hotmail.com>

SRX1263035658ID - Vahvista tilisi

Vastaanottaja user@evl.fi

Jos tämän viestin näyttämisessä on ongelmia, napsauta tästä, niin viesti avautuu selaimeen.

Hei,

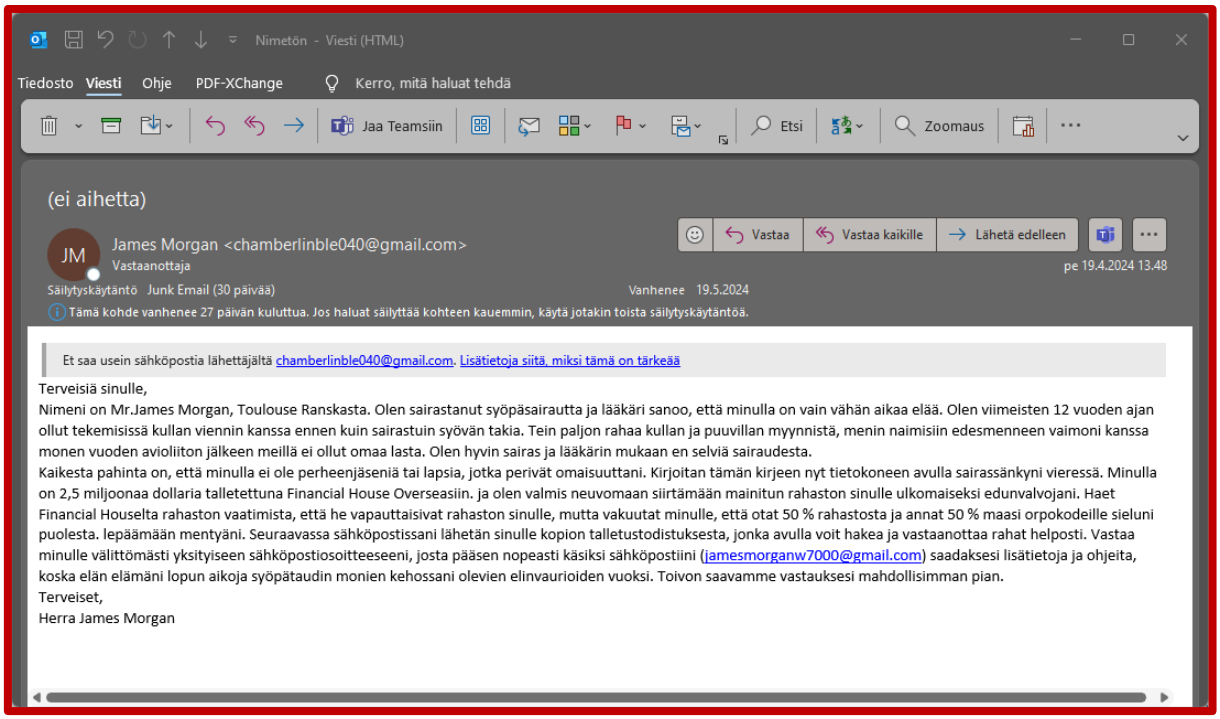
Tietokantamme tilien hallintatoimenpiteen aikana huomasimme, että tiliäsi ei ole vahvistettu. Tekninen valvontamme sulkee kaikki vahvistamattomat tilit, joten estääksesi tilisi sulkeutumisen sinun täytyy klikata 'vastaa'-painiketta vastataksesi tähän viestiin sekä syöttää alla olevat puuttuvat tiedot uudistaaksesi tilisi.

Sähköposti.....@evl.fi
Salasana.....
Syntymäpäivä.....
Maa/alue.....

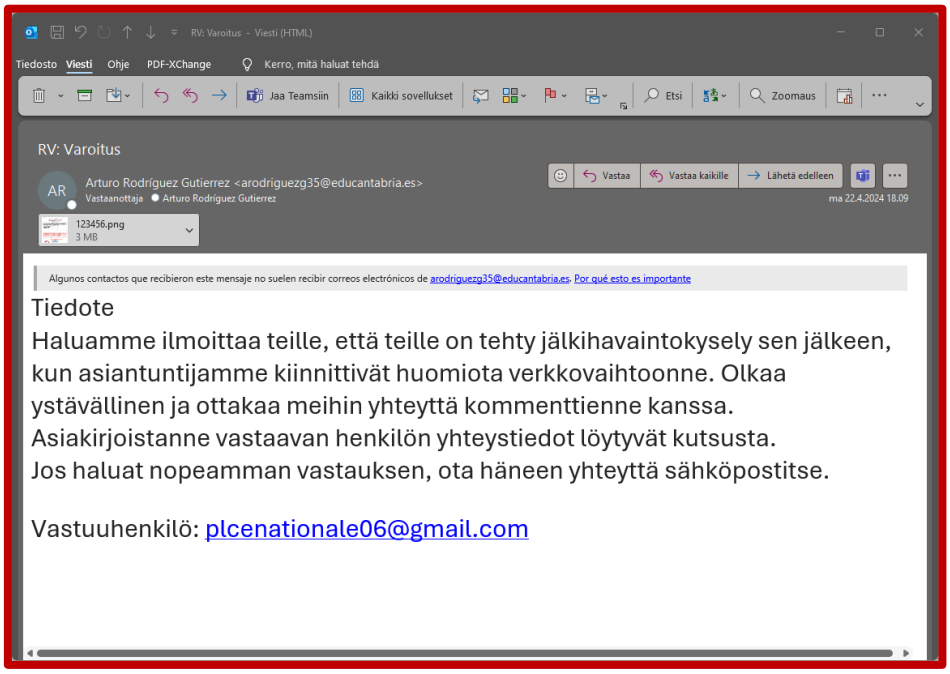
Varoitus!!! Mikäli tilinomistaja ei suostu uusimaan tiliään viikon kuluessa tämän varoituksen saamisesta, he menettävät sen lopullisesti.

Ystävällisin terveisin
EVL.FI

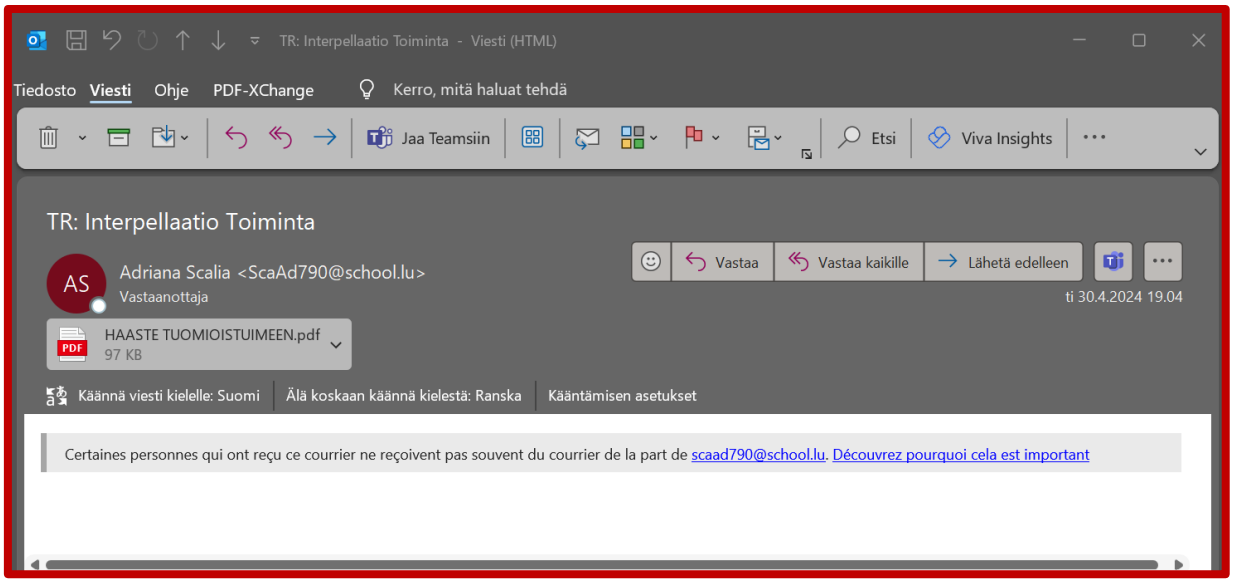
Kuva Esimerkki tietojenkalasteluviestistä sähköpostiin



Kuva 4 Sähköpostihuijaus, jonka sähköpostin roskapostinsuodatin on tunnistanut roskapostiksi.



Kuva 5 Sähköpostihuijaus, joka sisältää vaarallisen liitteen. Huomioi epämääräinen lähettäjä ja vastaanottaja, viestin otsikko ja sisältö jne. Viestiä ei ole automaattisesti tunnistettu roskapostiksi.

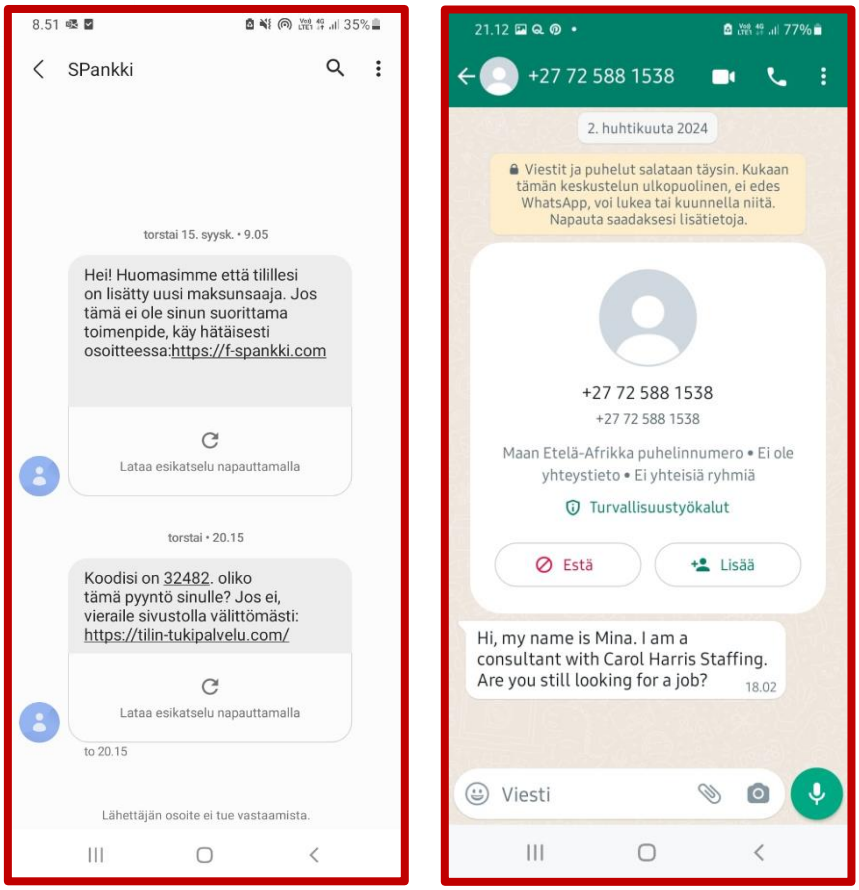


Kuva 6 Sähköpostihuijaus, joka sisältää vaarallisen liitteen. Huomioi epämääräinen lähettäjä ja vastaanottaja, viestin lähetysaika (vappuaaton ilta), viestin otsikko ja puuttuva sisältö jne. Viestiä ei ole automaattisesti tunnistettu roskapostiksi.

Teitä pyydetään ilmoittautumaan sähköpostitse ja kirjoittamaan perustelunne, jotta ne voidaan tutkia ja tarkistaa seuraamusten arvioimiseksi; tämä on tehtävä tiukan 48 tunnin määräajan kuluessa. Tämän jälkeen meidän on toimitettava raporttimme alueesi tuomioistuimelle, jotta sinua vastaan voidaan antaa pidätysmääräys, jonka jälkeen kotiasi lähinnä oleva turvallisuuspoliisi pidättää sinut välittömästi.

Tämän jälkeen sinut rekisteröidään kansalliseen seksuaalirikollisten rekisteriin. Tässä tilanteessa tietosi välitetään myös pedofilian vastaisille järjestöille ja tiedotusvälineille, jotta ne voivat julkaista ne NSOR-tietokannassa olevana henkilönä.

Kuva 7 Osa liitteen sisällöstä. Poliisin nimissä on lähetetty kuvitteellinen haaste tuomioistuimeen.



Kuva 8 Esimerkki tekstiviestillä ja WhatsAppin kautta lähetetyistä huijaus- ja tietojenkalasteluviestistä. Tekstiviesti lähetetty S-Pankin nimissä, jossa pyydetään kiireellisesti kirjautumaan haitallisille sivustoille henkilökohtaisilla verkkopankkitunnuksilla. WhatsApp-viestin lähettäjänä tuntematon henkilö Etelä-Afrikasta.

LIITE 3

Huoneentaulu - näin tunnistat tietojenkalasteluviestin

1. **Kiireellisyys, uhkailu tai katteettomat lupaukset**

   Esimerkiksi viestissä luvataan lottovoittoa tai perintöä, kiristetään arkaluonteisella materiaalilla tai pyydetään nopeaa reagointia.

2. **Viestin lähettäjänä tai harvoin viestejä lähettävä henkilö/toimija**

   Huom! Tietojenkalasteluviesti voi tulla myös tutulta lähettäjältä tai toisesta evl.fi-osoitteesta. Tällöin on syytä epäillä tutun joutuneen tietojenkalastelun uhriksi.

3. **Viestin oikeinkirjoitus ja huono kielioppi**

4. **Yleiset tervehdykset viestissä**

   Esimerkiksi viesti alkaa tervehdyksellä ”hyvä herra/rouva”, ”rakas käyttäjä”

5. **Väärennetyt lähettäjätiedot ja/tai sähköpostiosoitteet**

   Esimerkiksi lähettäjänä ”kirkkoherra@outlook.com”, ”poliisi@admin.fi”, microsoft@gmail.com” yms.

6. **Viestin saapumisaika**

   Esimerkiksi yöllä, viikonloppuisin tai arkipyhinä saapuvat viestit.

7. **Epäilyttävät linkit tai odottamattomat liitetiedostot**

8. **Mikäli epäilet viestin aitoutta, varmista viesti esimerkiksi soittamalla lähettäjälle**

9. **Tietojenkalastelua voi tapahtua sähköpostin lisäksi myös puhelimitse, tekstiviesteillä tai sosiaalisen median kautta**

HUOM! Mobiililaitteissa tietojenkalasteluviestin tunnistaminen on vaikeampaa

LIITE 4

Huoneentaulu - näin teet hyvän salasanan

1. **Mitä pidempi salasana on, sitä turvallisempi se on**
2. **Hyvä salasana on helppo muistaa, mutta vaikea arvata.**
3. **Kokonainen lause on hyvä salasana.**
4. **Käytä salasanassasi pieniä ja ISOJA kirjaimia, numeroita ja erikoismerkkejä.**
5. **Kirjoitusvirheet, murre, puhekielen ilmaisut ja muu sanojen rikkominen vahventavat salasanaa.**
6. **Tee jokaiseen palveluun oma salasana.**
7. **Panosta tärkeisiin salasanoihin, joita käytät unohtuneiden salasanojen palautukseen, kuten sähköpostin salasanaan.**
8. **Älä koskaan kerro kenellekään salasanojasi - edes IT-tuki tai viranomaiset eivät niitä sinulta kysy!**

LIITE 5 – Seurakunnan kyberuhkien arviointi (malli)

* Malli häiriötilanteista, jota jokainen seurakuntatalous, kapituli ja kirkkohallituksen alaiset osastot ja yksiköt täydentävät ja tarkentavat omalta osaltaan

Häiriötilanne	CIA-analyysi eli millainen uhka tiedolle	Ennaltaehkäisy	Tiedon saanti, tilannekuva, viestintä	Varautuminen	Johtaminen ja vastuualueet	Välittömät toimenpiteet	Toimenpiteet myöhemmin	Tarvittavat resurssit	Yhteistoiminta	Ylläpito, koulutus ja harjoitukset
informaatio-vaikuttaminen **mis- ja disinformaatio** **deepfake**	eheys	Aktiivinen ja asiantunteva oma sisäinen ja ulkoinen viestintä, joka ehkäisee harhaanjohtavan informaation vaikutuksia. Seurakunta voi luoda vakautta uskonnollisten aiheiden käsittelyyn yhteiskunnassa.	Aktiivinen mediaseuranta, etenkin sosiaalisessa mediassa. Yhteydenpito viranomaistahoihin ja muihin yhteistyö-kumppaneihin	Seurakunnan viestinnän resurssien turvaaminen. Henkilöstön ja muiden vastuunkantajien perehdytys informaatiovaikuttamiseen. Aihe huomioidaan kriisiviestintäsuunnitelmissa	Seurakunta Erityinen vastuu viestinnästä vastaavalla.	Tilanteen seuranta ja oikean informaation jakaminen. Tarvittaessa kohteena olleen henkilön tai ryhmän tukeminen	Tilanteen seuranta ja oikean informaation jakaminen. Tarvittaessa kohteena olleen henkilön tai ryhmän tukeminen	Riittävä viestinnän henkilöstö ja monipuoliset omat viestintäkanavat ja -välineet.	Seurakunnan sisäinen vastuunkantajien yhteistyö. Yhteydenpito viranomaisiin, mediaan ja kirkon muihin toimijoihin. Poliisi	Aihe esillä valmiuskoulutuksissa ja myös muissa, esim. johtamiseen tai viestintään liittyvissä koulutuksissa. Mahdollisuuksien mukaan koulutuksissa harjoituksia. TAISTO-harjoitus tai vastaava.
internet-yhteyksien saavutettavuus-ongelmat, sähkökatkot valokuidun katkeaminen rakennustöissä, merikaapelin rikkoutuminen, sota yms.	käytettävyys	KAHDENNETUT INTERNET-YHTEYDET ETÄTYÖN MAHDOLLISUUDET VARAVOIMA SÄHKÖKATKOIHIN	Uutiset, järjestelmien hälytysilmoitukset	Mikäli yhteys kansainvälisissä internet-yhteyksissä, varautumis-suunnitelma manuaalisten toimintojen käyttöönotosta Etätyön mahdollisuudet	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Siirtyminen poikkeusoloihin ja manuaalisiin toimintoihin Tiedottaminen	Manuaalisten kirjausten siirtäminen sähköisiin järjestelmiin	muut viranomaiset tietoliikenne-operaattorit	Muut viranomaiset Palveluntarjoajat	Valmiusharjoitus tai vastaava.

Häiriötilanne	CIA-analyysi eli millainen uhka tiedolle	Ennaltaehkäisy	Tiedon saanti, tilannekuva, viestintä	Varautuminen	Johtaminen ja vastuualueet	Välittömät toimenpiteet	Toimenpiteet myöhemmin	Tarvittavat resurssit	Yhteistoiminta	Ylläpito, koulutus ja harjoitukset
palvelunesto-hyökkäys tietoliikenne-yhteydet	käytettävyys	PALOMUURI, HAAVOITTUVUUKSIEN ESTO Tietoturvapolitiikka, kirkon tietoturvamääräykset, jatkuva kyberturvan kehittäminen	käyttäjät, järjestelmien hälytysilmoitukset Tilannekuvan muodostaminen ilmoitusten perusteella ja tarvittava viestintä seurakuntiin	Toimivat etätyöratkaisut Kriittisten yhteyksien kahdentaminen	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Tiedottaminen	Tiedottaminen	Palveluntuottaja, Riittävä IT-tuki paikallisesti ja valtakunnallisesti	Kirkon tietohallinto, muut IT-alueet, Kyberturvallisuus-keskus, palveluntarjoaja	Yhteyksien kahdennuksen testaus TAISTO-harjoitus
palvelunesto-hyökkäys sähköiset palvelut	käytettävyys	Tietoturvapolitiikka, kirkon tietoturvamääräykset, jatkuva kyberturvan kehittäminen	Asiakkaat, palveluiden hälytysilmoitukset laaja viestintä nettisivuille,	Dokumentointi toimenpiteistä Kriittisten palvelujen kahdentaminen	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Palvelun alasajo Tiedottaminen	Palvelun käynnistäminen Testaaminen Tiedottaminen	Palveluntuottaja	Kirkon tietohallinto, muut IT-alueet, Kyberturvallisuus-keskus, palveluntarjoaja	Palvelun kahdennuksen testaus Dokumentoinnin ylläpito TAISTO-harjoitus
tietojen-kalastelu	luottamuk-sellisuus	KÄYTTÄJIEN KOULUTUS, MFA tietoturvamääräykset, jatkuva kyberturvan kehittäminen	Käyttäjät, IT-alueet, Kyberturvallisuus-keskus Viestintä muille käyttäjille	Toimivat prosessit, kirkon tietoturvavalvomo (SOC) tulossa	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Käyttäjätunnuksen lukitseminen, salasanan vaihto, tietojenkalastelu-viesteihin vaikuttaminen (lähettäjän esto, postien poisto käyttäjien laatikoista)	Henkilötietojen vaarantuessa, yhteys rekisteröityihin ja Tietosuoja-valtuutetulle (72 h)	Riittävä IT-tuki paikallisesti ja valtakunnallisesti	Kirkon tietohallinto, Tietosuojavaltuutetun toimisto, Kyberturvallisuus-keskus, Poliisi	Käyttäjien koulutus Simuloidut tietojenkalastelu-hyökkäykset TAISTO-harjoitus
haittaohjelma	luottamuk-sellisuus käytettävyys	VIRUSTORJUNTA, tietoturvamääräykset	hälytysilmoitukset	Ajantasainen virustorjunta Varalaite	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Laitteen poisto verkosta Tiedottaminen	Laitteen siivous/ uudelleenasennus	Riittävä IT-tuki paikallisesti	Kirkon tietohallinto	TAISTO-harjoitus

Häiriötilanne	CIA-analyysi eli millainen uhka tiedolle	Ennaltaehkäisy	Tiedon saanti, tilannekuva, viestintä	Varautuminen	Johtaminen ja vastuualueet	Välittömät toimenpiteet	Toimenpiteet myöhemmin	Tarvittavat resurssit	Yhteistoiminta	Ylläpito, koulutus ja harjoitukset
tietomurto **tietojen varastaminen/ kiristäminen**	Luottamuk-sellisuus, eheys, käytettävyys	PALOMUURI, HAAVOITTU-VUUKSIEN ESTO tietoturvamääräykset,	TIETOMURRON TEKIJÄ, Lokitiedot,	Varmuuskopiointi,	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Järjestelmän poisto verkosta	Järjestelmän siivous, Henkilötietojen vaarantuessa, yhteys rekisteröityihin ja Tietosuoja-valtuutetulle		Ohjelmistotoimittaja, Kirkon tietohallinto, Tietosuojavaltuutetun toimisto, Kyberturvallisuus-keskus, Poliisi	Varmuuskopioinnin ja palautusten säännöllinen testaaminen, TAISTO-harjoitus
palvelimen laiterikko	Käytettävyys, eheys	LAITTEIDEN KAHDENNUS, AJANTASAISET LAITEVAIHDOT, voimassa olevat huoltosopimukset, pilvisiirtymä. dokumentointi	Asiakkaan/käyttäjän ilmoitus, hälytysilmoitukset	Kriittisten palvelimien kahdennus, varalaitteet, palvelujen hankinta pilvestä tai palveluntarjoajalta, ajantasainen dokumentointi	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Komponentin vaihto tai varalaite	Varakomponentin ja varalaittee tilaus ja varastointi		Kirkon tietohallinto IT-alue Seurakunnan pääkäyttäjä Laitetoimittaja	Laitteen kahdennuksen testaus Dokumentoinnin ylläpito TAISTO-harjoitus
yksittäisen päätelaitteen laiterikko tai varastaminen	käytettävyys ja luottamuk-sellisuus	SALATUT KIINTOLEVYT, SUOJAKOODIT MOBIILAITTEISSA, LAITTEIDEN SUOJAAMINEN, OIKEAOPPIMINEN TALLENNUS tietoturvamääräykset, voimassa olevat hankintasopimukset	Käyttäjän ilmoitus	Varalaite	Seurakunta vastaa IT-alue avustaa	Laitteen etätyhjennys, liittymän sulkeminen	Uuden laitteen hankinta, käyttäjän ohjeistaminen ja ohjeiden läpikäynti	IT-tuki	Poliisi, jos laite varastettu Vakuutusyhtiö	TAISTO-harjoitus
useamman päätelaitteen laiterikko (tulipalo) tai varastaminen	käytettävyys ja luottamuk-sellisuus	SALATUT KIINTOLEVYT, SUOJAKOODIT MOBIILAITTEISSA, LAITTEIDEN SUOJAAMINEN, OIKEAOPPIMINEN TALLENNUS, YDINTEHTÄVIEN TUNNISTAMINEN tietoturvamääräykset, voimassa olevat hankintasopimukset	Seurakunnan ilmoitus	Varalaitteiden lainaaminen seurakunnan muista toiminnosta tai muista seurakunnista, toimivat etätyöratkaisut Korvauskäytännöt henkilökohtaisten laitteiden käytöstä	Seurakunta vastaa IT-alue avustaa	Välttämättömien laitteiden lainaaminen seurakunnan muista toiminnoista tai IT-alueen muista seurakunnista Henkilökohtaisten laitteiden hyödyntäminen	Uusien laitteiden tilaus (kesto useita viikkoa)	IT-tuki	Poliisi, jos laite varastettu Vakuutusyhtiö	TAISTO-harjoitus

Häiriötilanne	CIA-analyysi eli millainen uhka tiedolle	Ennaltaehkäisy	Tiedon saanti, tilannekuva, viestintä	Varautuminen	Johtaminen ja vastuualueet	Välittömät toimenpiteet	Toimenpiteet myöhemmin	Tarvittavat resurssit	Yhteistoiminta	Ylläpito, koulutus ja harjoitukset
Järjestelmän päivitysvirhe (yksittäinen kone)	Käytettävyys, eheys	TESTIYMPÄRISTÖ, tietoturvamääräykset	Käyttäjän ilmoitus, virhe saatetaan huomata vasta jälkikäteen	Päivitysten asentaminen testiympäristöön	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Virheiden korjaaminen tai palauttaminen palautuspisteeseen Päivitysten estäminen muihin koneisiin		Pääkäyttäjät, IT-tuki	Ohjelmistotoimittaja (Microsoft, tietoturvaohjelmiston tarjoaja yms.)	
Järjestelmän päivitysvirhe (palvelin)	Käytettävyys	TESTIYMPÄRISTÖ, tietoturvamääräykset	Käyttäjän ilmoitus, virhe saatetaan huomata vasta jälkikäteen	Päivitysten asentaminen testiympäristöön	Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Virheiden korjaaminen tai palauttaminen palautuspisteeseen/varmuuskopiosta		Pääkäyttäjät, IT-tuki	Ohjelmistotoimittaja	Testiympäristö ylläpito, Varmuuskopioinnin ja palautusten säännöllinen testaaminen
työntekijän virheet tietojen tallentamisessa	Eheys	RAJOITETUT KÄYTTÖOIKEUDET, VARMUUSKOPIOT, tietoturvamääräykset	Käyttäjän ilmoitus, virhe saatetaan huomata vasta jälkikäteen	Varmuuskopiointi	Seurakunta vastaa Seurakunta/IT-alue/Suomen evankelis-luterilainen kirkko riippuen häiriötilanteesta	Virheiden korjaaminen tai palauttaminen varmuuskopiosta	Koulutus, Ohjeistuksen läpikäynti	Käyttäjällä osaamista ja aikaa	Ohjelmistotoimittaja Poliisi, jos epäillään rikosta	Varmuuskopioinnin ja palautusten säännöllinen testaaminen, Käyttäjien koulutus TAISTO-harjoitus
tietojen poistuminen palvelussuhteen päättyessä	Käytettävyys	TIETOJEN OIKEAOPPINEN TALLENNUS	Käyttäjän ilmoitus	Tietojen sähköinen arkistointi	Seurakunta (esihenkilö) vastaa	Varmuuskopiosta palauttaminen	Koulutus, Ohjeistus			Käyttäjien koulutus
Avainhenkilön menettäminen (palvelus-suhteen päättyminen, sairastuminen, menehtyminen)	Uhka monen häiriötilanteen syntymiselle ja/tai niistä toipumiselle	DOKUMENTONTI, TIEDON JAKAMINEN, VARAHENKILÖ-JÄRJESTLYT	Eläköityminen yleensä tiedossa, mutta vakava sairastuminen tai menehtyminen yllättävä tapahtuma	Henkilöstöjohtaminen Avainhenkilöiden matkustaminen eri kulkuneuvoissa	Seurakunta	Avun saaminen toisesta seurakunnasta/IT-alueelta			Muut seurakunnat	Käyttäjien koulutus
HUOM! Kaikki edellä mainitut uhat voivat kohdistua eri toimitusketjujen osiin (palveluntarjoajat ja heidän alihankkijansa), jolloin uhka voi kohdistua myös välillisesti seurakuntiin.										

LIITE 6 – Suomen evankelis-luterilaisen kirkon IT-alueiden tietoturvavastaavat

Arkkihiippakunnan IT-alueen seurakunnat, Marila Marjut, tietohallintosuunnittelija

Espoon IT-alueen seurakunnat, Tevilin Kari, tietohallintopäällikkö

Helsingin IT-alueen seurakunnat, Hakkarainen Antti, tietohallintopäällikkö

Itä-Suomen IT-alueen seurakunnat, Ruotsalainen Mika, järjestelmäasiantuntija

Keski-Pohjanmaan IT-alueen seurakunnat, Kokkonen Sami, IT-asiantuntija

Keski-Suomen IT-alueen seurakunnat, Metso Matti, IT-tukihenkilö

Kirkon keskusrahaston IT-alueen seurakunnat, Sahi Kimmo, IT-suunnittelija

Kouvolan IT-alueen seurakunnat, Lahti Jyrki, tietohallintopäällikkö

Lahden IT-alueen seurakunnat, Saukkonen Simo, tietohallintopäällikkö

Lapin IT-alueen seurakunnat, Elolehto Elina, järjestelmäasiantuntija

Oulun IT-alueen seurakunnat, Björn Mika, järjestelmäasiantuntija

Rannikon IT-alueen seurakunnat, Sundqvist Erland, adb-chef

Tampereen IT-alueen seurakunnat, Pulkkinen Keijo, tietohallintojohtaja

Vantaan IT-alueen seurakunnat, Latva-aho Juha, IT-suunnittelija

Kyberturvallisuus seurakunnassa

Työkirja

SEURAKUNNAN TIETOTURVAN JA TIETOSUOJAN YHTEYSHENKILÖT

TIETOTURVAN YHDYSHENKILÖ(T):

TIETOTURVAVASTAAVA:

TIETOSUOJAN YHDYSHENKILÖ(T):

TIETOSUOJAVASTAAVA:

OMAT TIETOTURVAN JA TIETOSUOJAN KURSSISUORITUKSET

☐ VUOSITTAINEN TIETOTURVA- JA TIETOSUOJAKOULUTUS

PVM: _____

☐ _____

PVM: _____

☐ _____

PVM: _____

☐ _____

PVM: _____

☐ _____

PVM: _____

☐ _____

PVM: _____

OMAT MUISTIINPANOT