Suojeluohje

Voimassa 1.4.2017 alkaen.

Kybervakuutuksen suojeluohje S711

290104f 04.17

1 Tarkoitus

Tämä suojeluohje on tarkoitettu liitettäväksi vakuutussopimukseen täydentämään varsinaisia vakuutusehtoja. Ohje sisältää suojeluteknisiä määräyksiä ja neuvoja, joita noudattamalla voidaan ehkäistä vahinkojen syntymistä ja pienentää vahinkomääriä.

2 Velvoittavuus

Tämä suojeluohje on osa vakuutussopimusta. Vakuutuksenottajan ja vakuutetun on noudatettava tätä suojeluohjetta ja sen määräyksiä. Mikäli suojeluohjetta ei noudateta, voidaan korvausta vakuutussopimuslain mukaan vähentää tai se voidaan evätä.

Vakuutuksenottaja on velvollinen huolehtimaan siitä, että tämän ohjeen sisältö on yrityksessä työskentelevien henkilöiden tiedossa.

Nämä kyberturvallisuuteen liittyvät ohjeet on tarkoitettu pääasiassa auttamaan sellaisia pieniä ja keskisuuria organisaatioita, joilla ei välttämättä ole mahdollisuuksia palkata omaa tai ulkopuolista kyberturvallisuushenkilöstöä, käymään läpi ja parantamaan omaa kyberriskien hallintaansa.

3 Kyberturvallisuusohjeita

3.1 Tietoturvapolitiikan kehittäminen ja ylläpito

Organisaation tulee määrittää ja dokumentoida tietoturvapolitiikka tai täydentää olemassa olevaa tietoturvapolitiikkaansa niin, että se kattaa ainakin seuraavat alueet:

Tietojen ja tietojärjestelmien luokittelu

Miten tiedot luokitellaan, millaista tietoturvaa tulee noudattaa eri tasoisia tietoja käsitellessä, millaisilla tietojärjestelmillä eri tietoja käsitellään.

Roolit ja vastuut tietoturvaan liittyen

Tietoturvapolitiikassa tulee selkeästi määritellä tietoturvaan liittyvät roolit ja vastuut: kuka vastaa tietoturvasta, kuka toimii tietosuojavastaavana, kenellä on oikeudet käsitellä minkäkin tasoista tietoa, kuka huolehtii järjestelmien ja tietovarastojen tietoturvasta ja käsittelyoikeuksien hallinnoinnista.

Henkilötietojen käsittely ja turvaaminen

Mikäli organisaatio kerää henkilö- tai asiakastietoja, tulee tietoturvapolitiikassa määritellä toimintamallit, joilla henkilötietoja käsitellään henkilörekisterilain ja EU:n tietosuoja-asetusten mukaisesti.

Sosiaalisen median ja tietoverkkojen käytön ohjeet

Tietoturvapolitiikassa on ohjeet ja rajoitukset henkilöstön sosiaalisen median ja tietoverkkojen käytölle.

Ylläpito ja päivittäminen

Tietoturvapolitiikassa tulee määritellä, miten sitä ylläpidetään ja päivitetään sekä taho, joka hyväksyy muutokset. Siinä on myös määritettävä, miten politiikka saatetaan tehokkaasti kaikkien organisaation työntekijöiden ja muiden relevanttien sidosryhmien tietoon.

Tietoturvapolitiikassa tai sitä täydentävässä tietoturvaohjeistuksessa voidaan myös käsitellä yksityiskohtaisemmin jäljempänä kohdissa 3.2-3.11 esitettyjä asioita.

3.2 Tietoturvallisuus ja yksityisyydensuoja

Organisaation tulee selvittää tietojen ja tietoturvan osalta ainakin seuraavaa:

- Millaista tietoa organisaatio käyttää ja säilyttää toiminnassaan. Onko esim. asiakastietoa, tilitietoja, tietoja finanssitransaktioista, yhteystietoja, ostokäyttäytymiseen liittyviä tietoja, pankkiyhteystietoja, korttimaksutietoja, palkkatietoja, verotietoja, henkilötietoja, terveystietoja, potilastietoja, liikesalaisuuksia ym. luottamuksellista tietoa asiakkaista, työntekijöistä tai muista sidosryhmistä.
- Miten tätä tietoa käsitellään ja kuinka se on suojattu.
- Kenellä on pääsy tietoihin ja millä edellytyksillä. Kenellä on tarve päästä käsiksi luottamuksellisiin tietoihin työtehtävien hoitamiseksi ja ketkä eivät tarvitse pääsyä luottamuksellisiin tietoihin. Millaiset tietojen käyttö- ja pääsyoikeudet eri tahoilla on.
- Mitkä tietojärjestelmät tai tiedot ovat liiketoiminnan jatkuvuuden kannalta kriittisiä.

Ylläolevan perusteella tiedot tulee luokitella luottamuksellisuutensa mukaan esimerkiksi seuraaviin luokkiin, joka perustuu vm.fi/VAHTI -ohjeistoon:

- Erittäin salainen
- Salainen
- Luottamuksellinen
- Käyttö rajoitettu
- Julkinen

Kun tiedot on luokiteltu, tulee määrittää kullekin luokalle käyttöoikeudet ja tietoturvan periaatteet lähtökohtaisesti niin, että mitä salaisemmasta tai kriittisemmästä tiedosta on kyse, sitä harvemmilla on siihen käyttöoikeus ja sitä paremmin tieto on suojattu (esim. salasanoilla, salauksella ja tarvittaessa fyysisillä tunnistautumisvälineillä tai biometrisillä tunnisteilla).

Vakuutuksenottajan on huolehdittava päivittäin, että tiedostoista on olemassa ajantasaiset varmuuskopiot. Varmuuskopioita tulee säilyttää eri tiloissa kuin alkuperäistä tietoa ja varmuuskopiot on myös tarvittaessa salattava.

Tietojen varmuuskopiointi tulee myös järjestää siten, että kaikki toiminnan kannalta tärkeä tieto on mahdollista palauttaa varmuuskopioilta tarvittaessa. Tietojen palautus varmuuskopioista tulee testata säännöllisesti, jotta varmistutaan, että varmuuskopiot ovat toimivia ja että palautusprosessi toimii. On määritettävä, kuka on vastuussa varmuuskopioinnista, mitä tietoa varmuuskopioidaan, millä välineillä, kuinka usein, miten varmuuskopioita säilytetään ja kenellä on pääsy varmuuskopioihin.

Tietomurron tai tietojen tuhoutumisen varalle on laadittava toimintaohjeet ja ne on saatettava kaikkien tietojen parissa työskentelevien tietoon.

3.3 Henkilökunnan tietoturvakäytännöt

Henkilöstölle tulee määritellä työrooliensa edellyttämät oikeudet käyttää tietoja ja tietojärjestelmiä. Mikäli henkilöllä ei ole tarvetta käsitellä luottamuksellista tietoa työtehtävissään, tulee hänen pääsynsä näihin tietoihin estää. Mikäli työtehtävä edellyttää luottamuksellisen tiedon käsittelyä, tulee tapauskohtaisesti määrittää kunkin henkilön käyttövaltuudet ja rajata ne sellaisiin tietoihin ja järjestelmiin, joita työtehtävän hoitaminen edellyttää.

Asiakastietoja tai muita luottamuksellisia tietoja ei tule tarkastella ilman työhön liittyvää tarvetta. Tietoja ei tule luovuttaa kolmansille osapuolille, ellei ole täysin varma henkilöllisyydestä ja oikeuksista tarkastella ko. tietoa.

On aina käytettävä tietoturvallisia tiedonsiirtomenetelmiä ja salattava tieto tarvittaessa, jos se lähetetään julkiseen sähköpostiin.

Luottamuksellista tietoa (sähköisessä muodossa tai paperikopiona) tulee säilyttää vain niin kauan kuin sitä tarvitaan tai pitää säännösten mukaan säilyttää. Vanhentuneen tai muutoin hävitettäväksi menevän tietoaineiston tietoturvallisesta hävittämisestä tulee huolehtia.

Kaikkien työntekijöiden tulee noudattaa puhtaan pöydän politiikkaa, jotta luottamuksellista tietoa sisältäviä dokumentteja ei ole tiloihin mahdollisesti pääsevien ulkopuolisten nähtävillä.

Kaikkien työntekijöiden tulee käydä tietoturvakoulutus, jossa käydään läpi organisaation tietoturvapolitiikka, tietotekniikan turvallinen käyttö sekä keskeiset tietoturvariskit ja niiden hallinnan välineet. Kertauskoulutusta tulee järjestää säännöllisesti tai aina, kun on tarpeen tiedottaa uusista tietoturvaan liittyvistä uhista tai menettelytavoista.

On luotava toimintatavat, joilla organisaatiossa työskentelyn lopettavilta poistetaan käyttöoikeudet järjestelmiin ja tietoihin välittömästi työsuhteen päättyessä.

3.4 Petokset ja huijaukset

Sähköinen tiedonvälitys ja internet tarjoavat rikollisille paljon uusia mahdollisuuksia suorittaa petoksia tai huijata joko organisaatiota tai sen asiakkaita. Osa tämän tyyppisistä rikoksista ei ole vakuutustekniisessä mielessä kybervakuutuksen piirissä vaan ne katetaan perinteisillä rikosvakuutuksilla. Keskeisiä suojautumiskeinoja ovat mm.

- epäilyttäviä sähköpostin liitetiedostoja tai linkkejä ei tule avata
- tietokoneille ei saa asentaa mitään ohjelmistoja, joiden toiminnasta ja käyttötarkoituksesta tai alkuperästä ei ole tarkempaa tietoa. Vain pääkäyttäjillä tulisi olla oikeudet asentaa ohjelmia koneille.
- käyttöjärjestelmä, virustorjunta, palomuurit ja muut ohjelmistot tulee aina olla päivitetty viimeisimmillä turvallisuuspäivityksillä. Automaattipäivityksiä on käytettävä kaikissa ohjelmistoissa, joissa tämä on mahdollista.
- työntekijät on koulutettu tunnistamaan huijausyritykset ja tietojenkalastelu (phishing, social engineering)
- puhelimessa henkilökohtaista informaatiota tiedustelevien henkilöllisyys on aina tarkistettava soittamalla hänelle takaisin tiedossa olevaan oikeaan puhelinnumeroon
- asiakkaille on ilmoitettu, että heiltä ei koskaan kysytä salassapidettävää, henkilökohtaista informaatiota (salasanat, pankkiyhteystiedot, maksukorttitiedot, ym.) puhelimessa tai sähköpostilla
- tarpeetonta muistitikkujen ja muiden siirrettävien tiedontallennusvälineiden käyttöä vältetään ja ne tarkastetaan aina virustorjuntaohjelmistolla haittaohjelmien varalta
- Verkkosivustojen pop-up-ikkunoiden linkkejä ei pidä avata vakoiluohjelmien välttämiseksi

3.5 Tietoverkon turvallisuus

Organisaation verkko tulee erottaa julkisesta verkosta palomuureilla ja välityspalvelimilla (proxy) kaikissa rajapinnoissa julkista verkkoa vastaan. Virustorjuntaohjelmistoja sekä tunkeutumisyritykset havaitsevia ohjelmistoja tulee käyttää jokaisessa rajapinnassa tarvittaessa, jotta saavutetaan riittävät turvallisuuskontrollit.

Mikäli käytössä on pilvipalveluita, on varmistettava, että palveluntarjoaja tarjoaa vähintään yhtä hyvän suojaustason palvelussa olevalle tiedolle kuin omakin verkko. On varmistettava, että palvelusopimuksessa on määritetty palveluntoimittajan vastuut, tarjottavan palvelun taso, palautusajat ja mahdolliset varmuuskopiointipalvelut sekä mahdollisuus auditoida palvelua.

On luotava salasanakäytännöt, jotka edellyttävät työntekijöitä käyttämään riittävän vahvoja (tarvittavia ohjeita löytyy esimerkiksi viestintäviraston sivuilta) salasanoja, jotka vaihdetaan säännöllisesti ja ovat vain käyttäjien omassa tiedossa.

Langattoman verkon (WLAN) pääsyn tulee olla rajattu vain organisaation määrittämille laitteille ja käyttäjille. Langattoman verkon salauksen tulisi olla WPA2-tasoa.

Mikäli käytössä on langaton verkko vierailijoiden käyttöön, tulee sen olla erillinen organisaation omasta verkosta, jotta vierailijaverkon kautta ei ole pääsyä organisaation verkon tietoihin ja sovelluksiin.

Kaikki salaiseksi ja luottamukselliseksi luokiteltu tieto on mahdollisuuksien mukaan salattava. Jos yrityksellä on verkkosivut, on näiden suojauksesta varmistuttava.

Kaikki verkon järjestelmät ja ohjelmistot tulee päivittää aina uusimmilla ohjelmistoversioilla ja –päivityksillä, kun ne tulevat saataville. Automaattisia päivityksiä kannattaa käyttää erityisesti virustorjuntaan, haittaohjelmien torjuntaan ja palomuureihin liittyvissä ohjelmistoissa.

Pääsyä sellaisille sivustoille, joihin työntekijöillä ei ole tarvetta työssään päästä, on syytä rajoittaa. Selainten asetukset tulee asettaa sellaisiksi, että sisäisen verkon kautta ei pääse kielletyille sivustoille.

Mikäli käytössä on etäyhteyksiä, niiden tietoturvasta on huolehdittava. Etäkäytössä tulee käyttää turvallisia yhteyksiä ja vahvaa tunnistautumista, jossa käytetään lisävarmentimena erillisiä vaihtuvia tunnuslukuja tai kiinteitä tunnistevälineitä.

Tietoturvapolitiikassa on tuotava kaikkien tietoon, että tuntemattomia muistitikkuja tai muita siirrettäviä tiedontallennusvälineitä ei saa kytkeä verkossa oleviin tietokoneisiin tai mobiililaitteisiin ennen niiden tarkastamista haittaohjelmien varalta.

3.6 Kotisivujen ja verkkopalvelimien turvallisuus

Verkkopalvelimet, joilla tarjotaan tietoa ja palveluita asiakkaiden käyttöön, ovat yksi yleisimmistä kyberhyökkäyksen kohteista. Verkkopalvelimet, niiden ohjelmistoalustat ja niihin liittyvä verkkoinfrastruktuuri tulee suojata huolellisesti tietomurtoja, palvelunestohyökkäyksiä ja asiatonta käyttöä vastaan.

Asiakkaille avointa www-palvelua suunniteltaessa tulee ottaa huomioon sen vaatimat turvallisuusresurssit. On huolehdittava, että laitteisto- ja ohjelmistoratkaisut mahdollistavat riittävän turvallisuustason ja että turvallisuustason ylläpitoon ja päivittämiseen on käytettävissä riittävä osaaminen.

Www-palvelun toteutuksessa on otettava huomioon, että laitteistojen ja ohjelmistojen turvatason tehdasasetukset on usein asetettu käytön helppoutta ja nopeutta tukemaan eikä välttämättä riittävälle turvallisuustasolle. On syytä käydä huolellisesti läpi järjestelmän turvallisuusasetukset ja muuttaa ne vastaamaan organisaation tarpeita. Erityisen tärkeää on vaihtaa kaikki oletussalasanat organisaation tietoturvapolitiikan mukaisiin vahvoihin salasanoihin ja huolehtia, että uusimmat tietoturvapäivitykset ovat käytössä. Tarpeettomat palvelut, sovellukset ja sisältö on syytä poistaa verkkopalvelusta. Verkkopalvelujen ja –sisältöjen tietoturvallisuus tulee myös testein varmistaa.

On myös syytä varmistaa, että verkkopalvelussa julkistetaan vain asiaankuuluvaa, tarpeellista ja soveliasta tietoa. Mikäli palvelussa on julkistettava salassapidettävää tietoa tai henkilötietoja, on niiden julkistamisessa noudatettava erityisen suurta turvallisuustasoa. Tarvittaessa sensitiivinen tieto on salattava ja käyttäjien tunnistautumisen tulee olla riittävästi varmennettu.

Verkkopalvelussa julkaistavan tiedon eheys on varmistettava. On huolehdittava, että tiedon luvaton käyttö tai muuttaminen on riittävän tehokkaasti estetty.

Verkkopalvelimen turvallisuuden ylläpito vaatii jatkuvia säännöllisiä toimenpiteitä, joiden tekemiseen on varattava riittävät resurssit, kuten:

- lokitietojen ylläpito ja analysointi
- viimeisimpien päivitysten ja korjausten asennus ja testaus
- kriittisten tietojen säännöllinen varmuuskopiointi
- toipumismenettelyjen luonti häiriöiden varalle
- verkkopalvelun turvallisuuden säännöllinen testaaminen.

3.7 Sähköpostin turvallisuus

Sähköposti on monelle organisaatiolle kriittinen osa päivittäisen toiminnan pyörittämistä. Sähköpostin turvallisuudesta huolehdittaessa on otettava huomioon mm. seuraavia näkökohtia:

Kaiken sähköpostin tarkastamiseen on käytettävä roskapostisuodattimia ja virustorjuntaa. On lisäksi huolehdittava, että suodattimet ja virustorjunta päivittyvät automaattisesti uusimpiin versioihinsa. Roskapostisuodattimen asetukset on tarkistettava säännöllisesti, jotta ne eivät vahingossa estä tarpeellisten sähköpostien perillepääsyä.

Kaikki sähköpostien kanssa tekemisissä oleva henkilökunta tulee kouluttaa sähköpostin turvalliseen käyttöön. Henkilökunnan pitää osata tunnistaa sähköpostin käyttöön liittyvät riskit ja ymmärtää milloin ja miten sähköpostia voi käyttää työtehtävissä sekä milloin on syytä hankkia asiantuntijan apua.

Luottamuksellista tietoa lähetetään sähköpostitse vain niille tahoille, joilla on oikeus tätä tietoa käyttää. On määritettävä, millaista tietoa ei saa lähettää sähköpostilla ja millainen tieto on sähköpostitse lähetettäessä salattava.

3.8 Mobiililaitteet

Mobiililaitteiden tietoturvan osalta on keskeistä huolehtia mm. seuraavista asioista:

Tietoturvasovellusten käyttö kaikissa mobiililaitteissa

Kaikissa puhelimissa ja tableteissa olisi hyvä käyttää niille suunniteltuja tietoturvaohjelmistoja, jos sellaisia on saatavissa.

Ohjelmistojen päivittäminen

Yhtä lailla kuin kiinteissä laitteissa, mobiililaitteiden osalta on huolehdittava, että ohjelmistot ja tietoturvasovellukset on päivitetty viimeisillä päivityksillä.

Salasanojen käyttö puhelimissa ja muissa mobiililaitteissa

Mobiililaitteissa tulee mahdollisuuksien mukaan käyttää vahvoja salasanoja vastaavasti kuin kiinteissä päätelaitteissa. Mobiililaitteet tulee säätää lukittumaan automaattisesti, mikäli niitä ei käytetä.

Mobiililaitteissa olevan tiedon salaaminen

Mobiililaitteissa olevat tiedot tulee salata, jotta laitteen kadotessa tai joutuessa vääriin käsiin tietoon ei päästäisi käsiksi.

Ympäristön huomioiminen

Mobiililaitteiden käyttäjien tulee estää luottamuksellisten tietojen tai salasanojen näkyminen ulkopuolisille laitteita käytettäessä.

Sähköpostin ja sosiaalisen median käyttö mobiililaitteilla

Sähköpostin ja sosiaalisen median käytössä on noudatettava vastaavia turvallisuusmääräyksiä kuin kiinteillä laitteilla.

Toimintamalli, jos mobiililaite varastetaan tai katoaa

On luotava toimintamalli sen varalle, että mobiililaite varastetaan tai katoaa. Käyttäjien tulee tietää, miten tulee toimia, jotta laitteen saa poistettua käytöstä ja siinä olevat tiedot suojattua.

Käytöstä poistettujen mobiililaitteiden tyhjennys

Kun laitteita poistetaan käytöstä, tulee varmistaa, että niissä olevat tiedot poistetaan peruuttamattomasti. Myös käytöstä poistetut SIM-kortit tulee hävittää tietoturvallisesti.

3.9 Toimitila- ja operatiivinen turvallisuus

Toimitila- ja operatiivisen turvallisuuden alueilla on otettava huomioon mm. seuraavia tietoturvaan liittyviä näkökohtia:

Toimitilojen fyysisen turvallisuuden järjestäminen siten, että laitevarkauksien ja tietovuotojen riskit minimoidaan

Helposti mukaan otettavia tietojenkäsittelyvälineitä (kannettavat tietokoneet, tabletit, älypuhelimet) ei tule säilyttää paikoissa, joihin on mahdollista päästä julkisista tiloista. Tarvittaessa voidaan käyttää esimerkiksi kaapelilukituksia, mikäli laitteita on säilytettävä tiloissa, joihin on helppo päästä. Laitteisiin voi myös asentaa jäljitysohjelmistoja.

Käyttäjätunnusten ja salasanojen säilyttäminen päätteiden läheisyydessä tulee kieltää.

Luottamuksellista tietoa käsittelevien järjestelmien näytöt tulee sijoittaa siten, että ne eivät näy tiloihin, joihin ulkopuoliset pääsevät.

Tulostettavan luottamuksellisen materiaalin turvaaminen

Luottamuksellisen materiaalin tulostamista tulee välttää mahdollisuuksien mukaan. Paperitulosteita tulee säilyttää lukittavissa arkistokaapeissa tai kassakaapeissa. Tulostimet, joilla tulostetaan luottamuksellista aineistoa tulisi varustaa ohjelmistoilla, jotka sallivat tulostuksen vain tulosteet noutavalle, tunnistautuvalle käyttäjälle, jotta tulosteita ei jää lojumaan tulostimeen tai sen läheisyyteen.

Kirjepostin turvallisuus

Myös kirjepostin osalta postin lähettämiseen ja vastaanottamiseen on luotava tietoturvalliset toimintatavat. Luottamuksellinen kirjeposti ei saa joutua olosuhteisiin, joissa sen tietoturva voi vaarantua.

Roskien tietoturvallinen hävittäminen

Roskien tietoturvallisesta hävittämisestä on huolehdittava. On luotava toimintatavat luottamuksellista tietoa sisältävän materiaalin tietoturvalliseen silppuamiseen tai keräämiseen lukollisiin säiliöihin hävitettäväksi.

Hävitettävät tai kierrätettävät tietokoneet, tabletit, älypuhelimet tai tiedontallennusvälineet on tietoturvallisesti tyhjennettävä luottamuksellisesta tiedosta, pelkkä tiedostojen tuhoaminen ei riitä.

3.10 Maksutietojen turvallisuus

Mikäli organisaatio tarjoaa korttimaksamisen tai verkkomaksamisen mahdollisuutta asiakkailleen, on huolehdittava tässä yhteydessä tallennettavien tietojen turvallisuudesta. Tyypillisesti kortti- ja verkkomaksamisen palvelun tuottaa ulkopuolinen maksupalvelun tuottaja, joka myös käsittelee kortti- ja maksutiedot ja huolehtii niiden tietoturvasta. Mikäli organisaatio tallettaa itselleen maksujen yhteydessä tietoa asiakkaasta, korteista tai tileistä esimerkiksi asiakasrekisterin yhteyteen tulee näiden tietojen tietoturvallisesta käsittelystä kaikissa prosessin vaiheissa huolehtia erityisen tarkasti. Mikäli muihin kuin maksutarkoituksiin kerättävät korttinumerot ja asiakkaan henkilökohtainen informaatio on mahdollista korvata joillakin muilla tunnisteilla, näin kannattaa ehdottomasti tehdä.

Vain maksujärjestelmäkäyttöön hyväksyttyjä laitteistoja ja ohjelmistoja tulee käyttää. Ulkopuolisten pääsy käsittelemään maksupäätteitä tulee estää, jotta niihin ei pysty asentamaan skimmauslaitteita, joilla korttitiedot voi kopioida.

Organisaation omassa maksuliikenteessä tulee käyttää vain hyväksyttyjä maksunvälitysohjelmistoja tai sovelluksia. Pääsy maksusovelluksiin tulee rajata vain niille henkilöille, joilla on työtehtävissään tarve tehdä maksuja. Mikäli maksujärjestelmiä on tarpeen käyttää etäyhteydellä, tulee yhteyksien olla suojattuja.

Maksujärjestelmien ja –ohjelmistojen tietoturvakysymyksissä maksupalvelun tarjoaja voi useimmissa tapauksissa tarkemmin neuvoa ja ohjeistaa niiden tietoturvalliseen käyttöön.

3.11 Tietoturvaloukkauksiin tai kyberhyökkäyksiin varautuminen

Tietoturvaloukkauksien tai kyberhyökkäyksen varalta tulee olla määritellyt ja dokumentoidut toimintamallit ja –ohjeet, jotta tietoturvaloukkauksen tapahtuessa siihen pystytään reagoimaan viipymättä oikealla tavalla.

Toimintamallin tulee kattaa eri tyyppiset kyberuhat, kuten esimerkiksi: laitteistovarkaudet, laitteistojen hajoaminen tai katoaminen, järjestelmiin tunkeutuminen, haittaohjelmat, virukset, palvelunestohyökkäykset, tietovarkaudet tai vahingossa tapahtuneet tietovuodot sekä kyberkiristys.

Tietoa tietoturvaloukkauksiin ja poikkeamatilanteiseen varautumisen vaatimuksista löytyy julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivustolta mm. dokumentista 8/2017 Tietoturvapoikkeamatilanteiden hallinta tai siitä tuoreemmasta versiosta.