TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus ja yrityksen hallituksen vastuu

Traficomin julkaisuja
2/2020

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-465-4
ISSN 2669-8757

Johdanto

Yritykset ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä. Samalla niihin kohdistuvat kyberuhkat lisääntyvät jatkuvasti. Hyvin rakennettu kyberturvallisuus suojaa yrityksen toimintakykyä ja varmistaa, että liiketoiminnassa voidaan hyödyntää digitaaliteknologian tarjoamia hyötyjä täysimääräisesti. Yrityksessä hallituksen keskeinen tehtävä on edistää yhtiön etua. Siksi sen jäsenillä on oltava riittävät tiedot myös kyberturvallisuudesta ja siihen liittyvistä liiketoimintariskeistä.

Oppaan tarkoitus

Tämä opas antaa yritysten hallituksille työkaluja ja tukea oman organisaation kyberturvallisuuden edistämiseen. Siinä ei niinkään keskitytä teknologiaan, vaan autetaan hallituksen jäseniä kysymään oikeat ja kriittiset kysymykset johdolta ja henkilöstöltä.

Opas on suunnattu erityisesti suurten ja keskisuurten organisaatioiden hallitusten jäsenille, mutta se toimii myös kyberturvallisuudesta vastaavien henkilöiden arjen työkaluna. Käytännössä opasta voivat hyödyntää kaikenkokoiset organisaatiot toimialaan katsomatta.

Oppaan rakenne

Opas sisältää yleisen johdannon kyberturvallisuuteen ja sen eri luvuissa käsitellään teemaa hallituksen ja organisaation näkökulmasta. Osioissa:

- selitetään mistä kyberturvallisuudessa on kysymys ja miksi siihen pitää suhtautua vakavasti
- annetaan toimintamalleja hallitukselle ja organisaatiolle
- esitetään kysymyksiä, joita hallitus voi käsitellä organisaation sisällä.

Osa 1 sisältää johdannon kyberturvallisuuteen sekä esimerkkejä yleisimmistä uhkista. Osa 2 antaa ohjeistusta nykytilan kartoittamiseen. Osat 3, 4 ja 5 käsittelevät riskienhallintaa, organisaation uhkaympäristön ymmärtämistä sekä kyberturvallisuuden vastuita ja järjestämistä. Osat 6, 7 ja 8 tarjoavat toimintamalleja, joilla hallitus voi edistää kyberturvallisuuden ylläpitoa ja kehittämistä. Osat 9 ja 10 käsittelevät yhteistyötä ja suunnittelua kriisitilanteiden varalle.

Oppaan lopussa on liitteinä kuvaukset kyberturvallisuuteen liittyvästä keskeisestä lainsäädännöstä ja viranomaisvastuista.

Oppaan ovat toteuttaneet Liikenne- ja viestintäviraston Kyberturvallisuuskeskus sekä Huoltovarmuusorganisaation Digipooli. Opasta ovat luonnosvaiheessa kommentoineet Anne Berner, Satu Koskinen, Harri Pynnä, Tuija Soanjärvi ja Juhani Strömberg. Opas perustuu NCSC-UK:n julkaisuun Cyber Security Toolkit for Boards.

Lisätietoa ja ohjeistusta kyberturvallisuudesta löydät Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen internetsivuilta: https://www.kyberturvallisuuskeskus.fi/

I OSA

Mitä kyberturvallisuus on?

Kyberturvallisuus on suhteellisen uusi ja sisällöltään vielä vakiintumaton termi. Käytännössä sillä viitataan organisaatioiden ja yhteiskunnan digitalisoitumisen aiheuttamiin uudenlaisiin turvallisuushaasteisiin. Tässä oppaassa kyberturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla organisaatio suojaa liiketoiminnassa tarvittavat järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet kyberuhkilta.

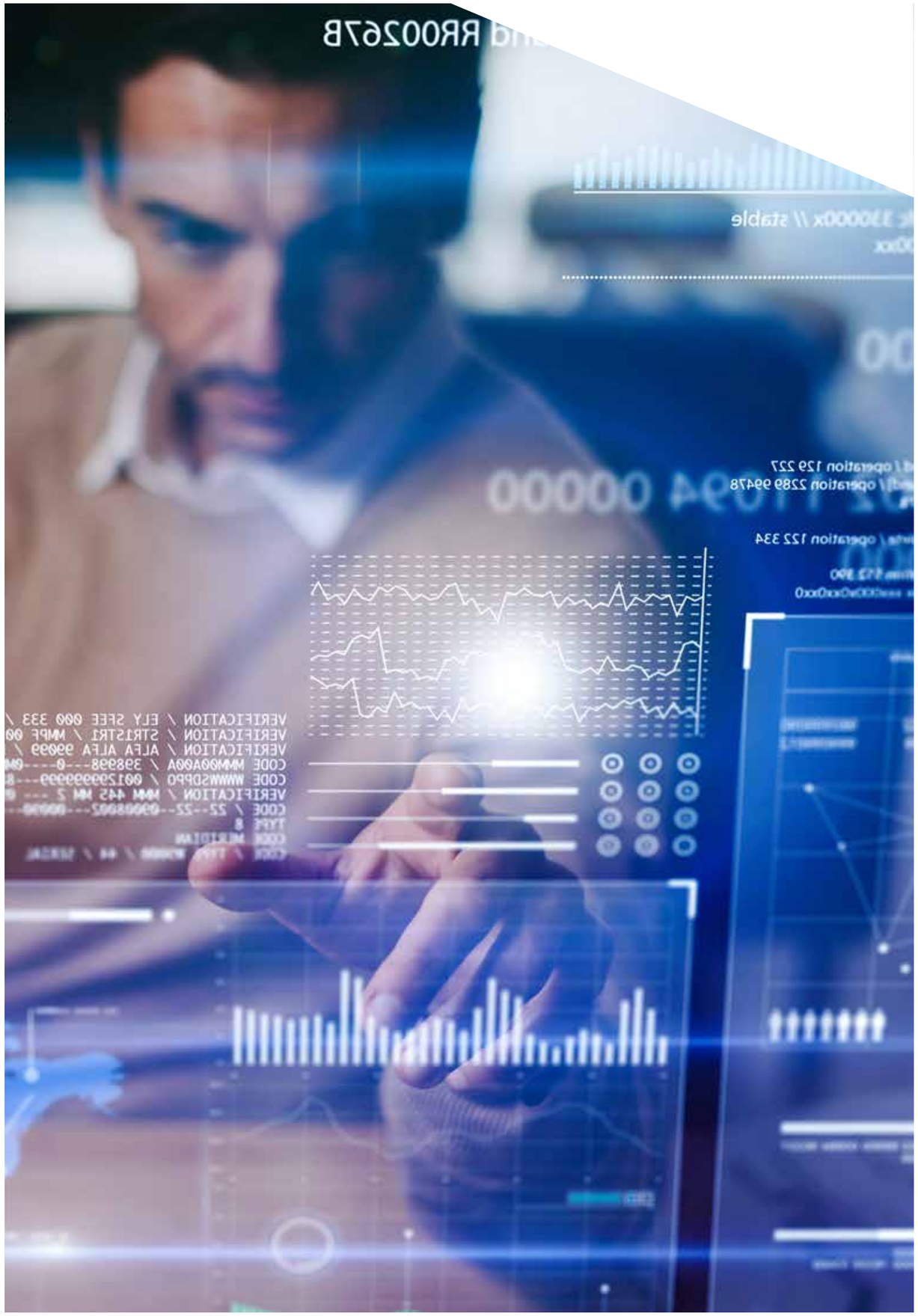
Kyberuhkat ovat haitallisia tapahtumia tai kehityskulkuja, jotka voivat vaikuttaa organisaation toimintaan, talouteen, sen hallussa olevaan tietoon ja pahimmillaan jopa liiketoiminnan jatkuvuuteen.

Esimerkkejä kyberuhkista

Tietojenkalastelu

Tietojenkalastelun (eng. phishing) tavoitteena on saada rikollisten haltuun käyttäjätunnus- ja salasanapareja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja, kuten maksukorttitietoja. Esimerkiksi verkkopalvelun käyttäjä voidaan huijata vierailemaan rikollisten tekemällä

Esimerkki Office 365 huijausviestistä.



internetsivustolla, joka muistuttaa ulkoasultaan palvelun aitoa sisäänkirjautumissivustoa. Kun käyttäjä syöttää tiedot huijaussivustolle, ne päätyvät rikollisten käyttöön. Näitä tietoja voidaan hyödyntää monin tavoin riippuen rikollisten motiiveista, haltuun saadun käyttäjätilin haltijan roolista tai tehtävistä organisaatiossa.

Useimmiten rikolliset pyrkivät huijaamaan itselleen mahdollisimman monta sähköpostitunnusta. Tämän jälkeen he kirjautuvat tileille ja etsivät laskutukseen liittyviä hakusanoja. Näiden tietojen pohjalta luodaan valelaskuja, jossa hyödynnetään oikean laskun tietoja ja kontekstia.

Tiliä voidaan hyödyntää myös uusiin tietojenkalasteluviesteihin, joita lähetetään uhrin kontakteille. Varastetuilla käyttäjätunnuksilla on puolestaan mahdollista vakoilla yrityssalaisuuksia. Onnistuneeseen tietojenkalasteluun voi liittyä myös maine- ja sääntelyriskejä.

Erityisen yleistä tietojenkalastelu on Microsoft Office 365 -ympäristössä. Se on Suomessa suosittu palvelu, eivätkä kaikki organisaatiot osaa käyttää riittävästi sen suojauskeinoja.

Suomessa Microsoft Office 365 -tietojenkalastelun uhriksi on joutunut jo useita satoja organisaatioita. Niistä aiheutuneet vahingot lasketaan useissa miljoonissa euroissa.

Hallituksen jäsenenä pääset käsiksi monenlaiseen rikollisia kiinnostavaan tietoon. Tämän vuoksi voit joutua kyberrikollisten kohteeksi. Hyökkääjät voivat esimerkiksi udella käyttämiesi IT-palvelujen käyttäjätunnuksia ja salasanoja tai tekeytyä sinuksi sähköpostissa. Sen jälkeen he voivat luoda ja lähettää esimerkiksi huijaussähköposteja, joiden avulla organisaation taloushallintoa harhautetaan maksamaan väärennettyjä laskuja.

Esimerkki 1

Tekniseen kauppaan erikoistunut Algol Oy joutui taitavan Office 365 -tietomurron kohteeksi. Tuntemattomaksi jääneen varkaan jäljet päättyivät lokitietojen mukaan Ruotsiin ja hän onnistui murtautumaan yrityksen sähköpostijärjestelmään. Sieltä varas lähetti väärennettyjä, uskottavan näköisiä tilausvahvistuksia ja maksuohjeita talousosastolle. Seurauksena oli 140 000 euron lasku, joka oli osoitettu huijarin pankkitilille. Menetys olisi voinut olla vielä suurempi, mutta hongkongilaispankin valppaus esti toisen suorituksen perillemenon.

Esimerkki 2

Suomalaisen finanssialan yrityksen Office 365 -pilvipalveluun murtauduttiin tietojenkalastelun avulla. Yrityksen kahdelle työntekijälle lähetettiin sähköpostia, jossa oli linkki tietojenkalastelusivulle. Rikollinen seurasi järjestelmässä yrityksen sähköpostiliikennettä useamman kuukauden ajan ja loi sähköpostin edelleenlähetykseen sääntömuutoksia yrityksen tietämättä. Yrityksellä ei näin ollen ollut tarkkaa käsitystä siitä, kuinka kauan sen sähköpostiliikennettä oli seurattu eikä myöskään tietoa siitä, mitä dataa yrityksestä on saattanut vuotaa.

Myös yrityksen maksuliikenteeseen oli yritetty lisätä laskuja, jotka olisivat maksettaessa siirtäneet rahat huijareiden tilille. Laskussa oli käytetty hyväksi normaalista sähköpostiliikenteestä saatuja tietoja ja saatu lasku näin näyttämään mahdollisimman aidolta.

Haittaohjelmat

Haittaohjelmat ovat tietokoneohjelmia, jotka aiheuttavat ei-toivottuja tapahtumia tietojärjestelmässä tai sen osissa. Yleensä haittaohjelmat leviävät sähköpostien liitetiedostojen, haittaohjelmilla saastutettujen verkkosivustojen sekä haavoittuvien palvelinten kautta. Haittaohjelma voi olla lähes harmiton, mutta entistä useammin niistä on myös vakavaa haittaa.

Maailmalla onkin yleistynyt ilmiö, jota kutsutaan nimellä Big Game Hunting. Termillä viitataan siihen, että rikollinen valitsee kohteikseen erityisen houkuttelevia ja rahakkaita organisaatioita.

Hyökkäyksessä rikollinen tunkeutuu organisaation järjestelmiin ja levittäytyy sen verkkoon. Lopuksi hyökkääjä käynnistää salatun kiristyshaittaohjelman, joka hidastaa ja haittaa organisaation toimintaa tai lamauttaa sen lähes kokonaan. Tämän jälkeen kiristetään lunnaita salauksen purkamiseksi. Nimensä mukaisesti hyökkääjät pyrkivät löytämään kohteita, joilla on hyvä maksukyky. Myös suuri käyttäjä- tai asiakasmäärä tekevät kohteesta houkuttelevan.

Esimerkki 3

Kyberturvallisuuskeskuksella on tiedossaan Suomessa lukuisia tapauksia, joissa kiristyshaittaohjelmatartunta on aiheuttanut organisaatiolle merkittäviä kustannuksia. Ne ovat syntyneet liiketoiminnan keskeytyksestä sekä IT-järjestelmien palauttamisesta toimintakuntoon. Ainakin yksi suomalainen yritys on joutunut lopettamaan koko liiketoimintansa, koska kiristyshaittaohjelman tuhoaman ICT-ympäristön uudelleenrakentaminen olisi tullut liian kalliiksi.

Palvelunestohyökkäykset

Palvelunestohyökkäykset ovat internetissä jo arkipäivää ja niitä tehdään Suomessakin tuhansittain joka vuosi. Palveluestohyökkäyksessä verkkoa kuormitetaan ylimääräisellä tietoliikenteellä. Tavoitteena on lamaannuttaa jokin palvelu tai tietojärjestelmä. Usein hyökkäyksen kohteena on organisaation julkinen internetsivusto tai esimerkiksi asiakkaiden hyödyntämä palvelu. Hyökkäykset kestävät yleensä niin kauan, kun niillä on vaikutusta kohteen toimintaan. Useimmiten se loppuu, kun palvelunestohyökkäys saadaan torjuttua ja palvelun toiminta palautettua entiselleen. Monesti hyökkääjä kuitenkin vain vaihtaa kohdetta, ja keskittyy seuraavaksi johonkin muuhun saman kohdeorganisaation palveluun.

Suurin osa kohdatuista kyberuhkista ei kohdistu yhteen ja tietoisesti valittuun organisaatioon. Kyberrikollisuus on luonteeltaan varsin opportunistista. Tavoitteena on lähinnä löytää organisaatioiden järjestelmistä ja prosesseista heikkouksia, joita voi hyödyntää rikolliseen tarkoitukseen. Toiminta on usein kansainvälistä ja pitkälle automatisoitua. Muiden rikollisten tavoin

Suurin osa kohdatuista kyberuhkista ei kohdistu vain yhteen ja tietoisesti valittuun organisaatioon.

kyberrikollisia kiinnostaa mahdollisuus nopeaan rahan saantiin.

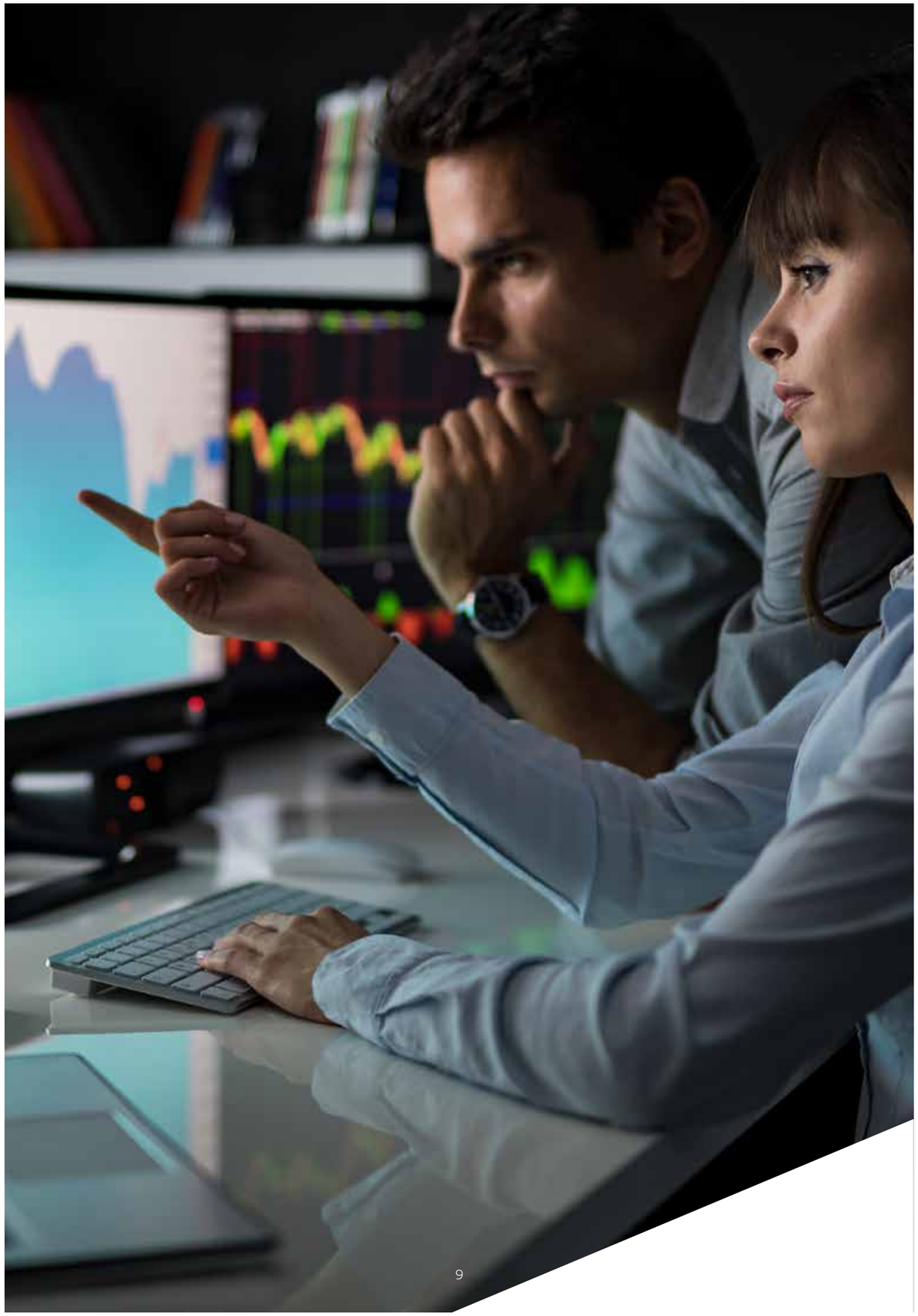
Kaiken lisäksi merkittävä osa kyberhyökkäyksistä toteutetaan hyvin yksinkertaisilla välineillä. Tällaisia ovat muun muassa erilaiset huijaussähköpostit, joiden avulla pyritään keräämään esimerkiksi organisaation käyttäjien käyttäjätunnuksia ja salasanoja. Siksi kyberturvallisuutta voi parantaa yksinkertaisillakin keinoilla, kuten kouluttamalla henkilöstöä tunnistamaan huijausyritykset.

Organisaation pitää kehittää kyberturvallisuutta johdonmukaisesti ja riskilähtöisesti. Tarvittavat toimenpiteet voivat olla luonteeltaan sekä teknisiä että ei-teknisiä. Hallituksen tehtävänä on huolehtia siitä, että organisaatiolla on riittävästi kyberturvallisuusosaamista. Johdolla on puolestaan oltava tarvittava tieto oikeiden ja tehokkaiden päätösten pohjaksi.

Esimerkki 4

Internetverkon kannalta useimmat palvelunestohyökkäykset ovat normaalia liikennettä ja vain hyökkäyksen kohde voi kunnolla arvioida, onko kyse hyökkäyksestä. Palvelunestohyökkäyksiä ei pystytä kokonaan estämään, joten organisaatioiden kannattaa varautua sietämään niitä ja sopia internetpalveluntarjoajiensa kanssa torjuntakeinoista. Palvelunestohyökkäyksen kohteeksi voi joutua myös sivullisena uhrina, jos hyökkäys kohdistuu esimerkiksi organisaation käyttämään palvelinhotelliin.

Palvelunestohyökkäysten kohteeksi joutuu Suomessa useita organisaatioita joka päivä ja ne on huomioitava myös riskiarviossa. Jos yrityksen palveluiden on oltava jatkuvasti saatavilla verkossa, on myös suunniteltava suojautuminen palvelunestohyökkäyksiä vastaan. Lisäksi niihin on varauduttava hyvissä ajoin.



II OSA

Organisaation tilanteen selvittäminen

Organisaatiossa on selvitettävä, mitkä tietoteknisen ympäristön (järjestelmät, tiedot, palvelut ja verkot) osat ovat kaikkein kriittisimpiä organisaatiolle asetettujen tavoitteiden saavuttamisessa. Lisäksi organisaatiossa pitää olla ymmärrys, mistä sen tietotekninen ympäristö käytännössä koostuu.

Organisaatiossa tulisi määrittää, mitkä tietoteknisen ympäristön osat ovat kriittisiä liiketoimintatavoitteiden saavuttamiseksi.

Mitä hallitus voi tehdä?

Selvittäkää tärkeimmät asiat

Liiketoimintariskien tavoin organisaatio ei voi koskaan poistaa kaikkia kyberturvallisuusriskejä. Hallituksen on kuitenkin varmistettava, että organisaatiossa suojataan erityisesti niitä asioita, jotka tukevat liiketoimintatavoitteiden saavuttamista.

Hallituksen on pohdittava riskejä laaja-alaisesti. Hallitus ja johto saattavat esimerkiksi tietää, että tietty kumppani on organisaatiolle ratkaisevan tärkeä ja että kyseisen kumppanin tietojen vaarantuminen olisi katastrofaalista organisaation taloudelle tai maineelle. Näistä riskeistä on aina viestittävä myös organisaation kyberturvallisuudesta vastaaville tahoille.

Viestinnän on oltava hallituksen, johdon ja asiantuntijoiden välillä aktiivista ja jatkuvaa, koska hallituksella ja johdolla on liiketoimintaan liittyviä tietoja, joita teknisillä asiantuntijoilla ei välttämättä ole. Tällaista on esimerkiksi tieto siitä, mitä kumppanuussuhteita organisaatio priorisoi. Teknisillä asiantuntijoilla on puolestaan tietoja keskeisten tavoitteiden saavuttamisen edellytyksistä. Tällaista on esimerkiksi tieto siitä, mistä järjestelmistä tai tiedosta kumppanit ovat riippuvaisia.

Tärkeimmät liiketoimintatekijät ovat organisaatiolle arvokkaimpia asioita. Ne voivat olla arvokkaita yksinkertaisesti siksi, että organisaatio ei kykene toimimaan ilman niitä. Liiketoimintatekijöiden vaarantuminen voi vahingoittaa myös organisaation mainetta tai aiheuttaa taloudellisia tappioita. Tällaisia voivat olla esimerkiksi:

- organisaation hallussa olevat henkilötiedot
- organisaation immateriaalioikeudet
- julkinen verkkosivusto
- teollisuuden ohjausjärjestelmät
- sisäverkon käyttäjien- ja pääsynhallinta järjestelmä.

Mitä organisaatiossa voidaan tehdä?

Lähtötilanteen määrittely

Lähtötilanteen määrittely on tärkeää, koska sen myötä saadaan kuva organisaation tarvitsemista ja mahdollisista suojautumistoimenpiteistä. Niiden määrittämisessä on ratkaisevan tärkeää tietää:

- mitkä järjestelmät ovat yhteydessä toisiinsa
- kenellä on pääsy tiettyihin tietoihin
- kuka omistaa minkäkin verkon tai palvelun.

Näiden tietojen kerääminen mahdollistaa muun muassa haavoittuvien järjestelmien päivittämisen ja suojautumisen hyökkäyksiltä. Tietoja saatetaan tarvita myös hyökkäykseen reagoitaessa. Näin voidaan arvioida, millaista vahinkoa hyökkääjä voi tehdä tai millainen vaikutus mahdollisilla korjaavilla toimenpiteillä on.

Koko ympäristön täydellinen ymmärtäminen voi olla haasteellista erityisesti organisaatioissa, joiden verkot ja järjestelmät ovat kasvaneet ajan myötä orgaanisesti. Jo perusasioiden ymmärtäminen, kuten mitä järjestelmiä organisaation eri verkoissa on, auttaa kuitenkin käynnistämään tarvittavia toimenpiteitä.

Kriittisten tietoteknisten resurssien määrittely

Organisaatiossa tulisi määrittää, mitkä tietoteknisen ympäristön osat ovat tärkeimpiä liiketoimintatavoitteiden saavuttamiseksi. Organisaatiolle voi olla esimerkiksi tärkeää huolehtia pitkäaikaisista asiakkuuksista. Kyberturvallisuustoimenpiteillä voidaan tukea tämän tavoitteen toteutumista esimerkiksi suojaamalla asiakastiedot, varmistamalla tilaus-toimitusjärjestelmän häiriötön toimivuus sekä varmistamalla organisaation internetsivujen toimivuus kaikissa tilanteissa.

Yhteistyö palveluntarjoajien ja kumppanien kanssa

Suurimmalla osalla organisaatioista on palveluntarjoajia tai kumppaneita, joilta ne saavat, jakavat tai toimittavat tietoja, järjestelmiä tai palveluja. Organisaation on huomioitava nämä ulkopuoliset palveluntarjoajat ja kumppanit riskienhallinnassaan. Keskeinen keino on sopia kyberturvallisuuteen liittyvistä vastuista ja oikeuksista kumppaneiden kanssa.

Kysymyksiä pohdittavaksi

Ymmärrämmekö organisaationa, miten tekniset järjestelmät, prosessit tai resurssit edistävät tavoitteidemme saavuttamista?

- Mitkä ovat organisaatiomme kriittiset tietotekniset resurssit, joita ilman organisaatiomme ei selviäisi?
- Mitä vaatimuksia meidän on täytettävä (esimerkiksi oikeudelliset vaatimukset tai sopimusvelvoitteet)?
- Mitä emme halua tapahtuvan ja miten se voisi tapahtua?
- Onko organisaatiollamme prosessi tärkeiden järjestelmien, tietojen ja palvelujen tunnistamiseen sekä näiden toimivuuden ja turvallisuuden seuraamiseen.

Onko organisaatiossa viestitty selkeästi organisaation tärkeimmistä tavoitteista ja varmistettu, että nämä prioriteetit ohjaavat myös kyberturvallisuustoimenpiteitä?

- Kyberturvallisuuden tulee tukea organisaation strategiaa. Kyberturvallisuutta ohjaavien dokumenttien, kuten kyberturvallisuusstrategian tai -politiikan, on suojattava organisaation strategisia tavoitteita.

III OSA

Riskienhallinta ja kyberturvallisuus

Organisaatiot tekevät usein riskiarviointeja ainoastaan vaatimustenmukaisuuden noudattamiseksi. Näitä voivat olla esimerkiksi:

- ulkoisista tekijöistä, kuten sääntely-vaatimuksista johtuvat velvoitteet
- asiakkaiden vaatimukset
- lakisääteiset vaatimukset.

Näillä perusteilla on kuitenkin vaarana, että riskinhallinnasta tulee vain ”rasti ruutuun” toimintaa. Tällaisessa tilanteessa organisaatiot voivat luulla hallitsevansa riskejä, vaikka ne ovat ainoastaan toimineet määritellyn prosessin mukaisesti.

Vaatimusten noudattaminen ja turvallisuus eivät ole sama asia. Ne voivat olla päällekkäisiä, mutta yleisiä turvallisuusvaatimuksia voidaan noudattaa käytännössä heikoilla turvallisuuskäytännöillä. Hyvä riskienhallinta ulottuu pelkkää vaatimusten noudattamista pidemmälle.

Hyvä riskienhallinta ulottuu vaatimusten noudattamista pidemmälle.

Mitä hallitus voi tehdä?

Sisällyttäkää kyberturvallisuus organisaation riskinhallintaprosesseihin

Kyberriskien on oltava osa organisaation arjen riskienhallintaa. Kyberriskien käsitteleminen erillään tai niiden luokitteleminen yksinkertaisesti ’tietoteknisiksi riskeiksi’ vaikeuttaa niiden vaikutusten tunnistamista. Samalla voi jäädä myös epäselväksi, mitä vaikutuksia organisaation muilla riskeillä voi olla sen kyberturvallisuuteen.

Kyberturvallisuustoimenpiteiden tulee tukea ja mahdollistaa liiketoimintaa hallitsemalla digitaaliteknologian käytöstä johtuvia riskejä. Ne eivät kuitenkaan saa estää tai hidastaa olennaisia liiketoimintaa edistäviä toimenpiteitä tai aiheuttaa kohtuuttomia kustannuksia.

Älkää mitatko onnistumista riskitason pienentymisellä

Myös toimenpiteiden onnistumisen mittaaminen voi olla vaikeaa. Hyvän kyberturvallisuuden tyypillinen lopputulos on toiminnan häiriöttömyys. Tätä voi olla kuitenkin hankala mitata, koska häiriöt voivat johtua myös organisaation kyberturvallisuustoimenpiteistä riippumattomista asioista.

Riskiarvioinneissa esitetään tavallisesti jonkinlainen arvio riskin todennäköisyydestä ja vaikutuksista (esimerkiksi suuri - keskisuuri - pieni). Tällaisen arviomenetelmän käyttäminen toimenpiteiden onnistumisen mittarina voi olla houkuttelevaa. On kuitenkin syytä huomioida, että tällaiset arviot saattavat mitata vajavaisesti organisaation toteuttamia toimenpiteitä. Tämä johtuu siitä, että kyberriskeihin vaikuttavat ulkoiset tekijät, kuten ohjelmistohaavoittuvuudet, muuttuvat nopeasti ja ovat usein organisaation vaikutusmahdollisuuksien ulottumattomissa.

Esimerkkejä toimenpiteiden mittareista kuvaillaan jäljempänä osassa VIII Toimenpiteiden seuranta.

Mitä organisaatiossa voidaan tehdä?

Kyberriskien hallintaan sovelletaan samoja riskienhallinnan periaatteita kuin muihinkin riskeihin. Kyberturvallisuuden ratkaisut ja teknologiat kehittyvät kuitenkin niin nopeasti, että vaarana on jäädä jälkeen ja käyttää kyberriskien arviointiin vanhentuneita menetelmiä. Siksi kyberriskejä olisi hyvä arvioida useammin kuin muita riskejä.

Kyberturvallisuus on vielä uusi termi ja sen käyttö vakiintumatonta. Niinpä organisaatiolla ei välttämättä ole samanlaista ymmärrystä kyberriskeistä kuin esimerkiksi taloudellisista tai työntekijöiden turvallisuuteen liittyvistä riskeistä. Käytettävissä ei välttämättä ole myöskään tietopohjaa, jonka perusteella riskien arviointi voitaisiin tehdä. Tämä on syytä huomioida, kun pohditaan kyberriskien arvioinnin luotettavuutta – etenkin jos sen tuloksia verrataan suoraan ”perinteisiin” riskiarviointeihin.

Kysymyksiä pohdittavaksi

Onko organisaatiolla käytössään prosessi, jolla varmistetaan, että päätöksentekijät saavat mahdollisimman kattavat tiedot?

- Prosessissa on keskityttävä ensisijaisesti siihen, että päätöksentekijät voivat tehdä päätöksiä parhaiden mahdollisten saatavilla olevien tietojen pohjalta. Päätöksentekijöitä voivat olla hallitus, johto tai muut organisaation työntekijät. Sekä hallituksen että toimenpiteen toteuttajan on saatava mahdollisimman paljon ymmärrettävää tietoa päätöksenteon tueksi.
- Riskiarviointien tulokset on jäsenneltävä niiden merkityksellisyyden perusteella. Useimmiten laadulliset tulokset ovat parempi vaihtoehto kuin tulokset, joihin lisätään mielivaltaisia numeroita tai kertoimia pistearvon saamiseksi.

Onko organisaatiolla prosessi, jossa kyberriskien arviointi on sidottu osaksi liiketoimintariskien arviointia?

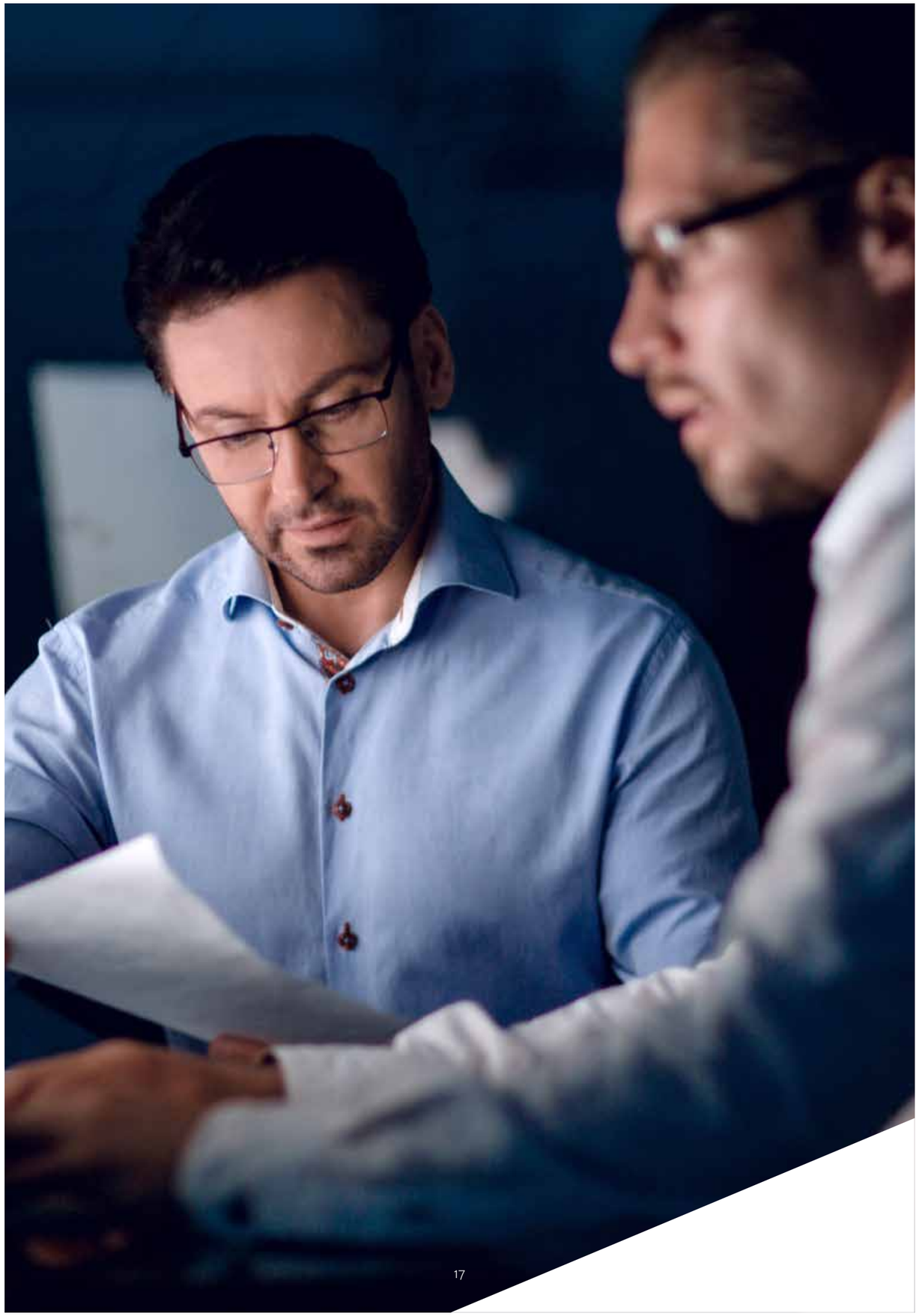
- Arvioidaanko kyberriskejä osana liiketoiminta- ja muita päätöksiä?

Onko organisaatiolla tehokas ja asianmukainen lähestymistapa kyberriskien hallintaan?
Hallituksen ja muiden organisaation toimijoiden on kyettävä esittämään prosessi selvästi ja yksinkertaisesti muutamassa minuutissa esimerkiksi seuraavien tietojen avulla:

- Miten riskit eskaloidaan?
- Mikä on kynnys hallituksen osallistumiselle riskiä koskevaan päätökseen?
- Kuinka usein riskejä arvioidaan?
- Mikä riski kuuluu kenenkin vastuulle?
- Kuka on vastuussa riskienarviointiprosessista ja sen tarkoituksenmukaisuudesta?

Ovatko hallitus ja johto määritelleet selvästi, miten riskejä organisaatiossa hallitaan?

- Ovatko riskien raportointia koskevat prosessit selkeät?
- Onko eri riskejä arvioitu keskenään? Onko eri riskien merkitys viestitty organisaatiossa? Organisaatio saattaa esimerkiksi hyväksyä riskinä sen, että sähköposti ei toimi yhden päivän ajan, mutta ei sitä, että organisaatiosta vuotaa julkisuuteen henkilötietoja.
- Onko kasautuvat riskit huomioitu? Mitä organisaatiossa toimitaan, jos kaksi tai useampia riskejä toteutuu yhtä aikaa?



IV OSA

Mikä organisaatiotamme uhkaa?

Kun organisaatioon tai sen yhteistyökumppaneihin kohdistuvat uhkat ymmärretään, voidaan määrittää myös organisaation kyberturvallisuustoimenpiteet ja -investoinnit. Organisaatiossa onkin tehtävä tietoinen päätös siitä, miltä uhkilta se pyrkii suojautumaan. Muutoin vaarana on, että yritetään suojautua kaikelta. Se taas johtaa helposti tehottomiin toimenpiteisiin.

Mitä hallitus voi tehdä?

Ymmärtäkää uhka

Kyberuhkien ymmärtäminen auttaa hallitusta tekemään tietoisia toimintaa ohjaavia päätöksiä. Keskeistä on tietoisuus hyökkääjien vaikuttimista: Miksi he olisivat kiinnostuneita juuri teidän organisaatiostanne? Hyökkääjän motiivina voi toki olla vain se, että organisaatiollanne on internetiin kytkettyjä ja helposti haavoitettavia tietokoneita, joita voidaan hyödyntää rikolliseen toimintaan.

Varmistakaa, että organisaatio tekee turvallisuuteen liittyvää yhteistyötä

Kumppanit ja vertaisorganisaatiot ovat usein hyviä lähteitä saada tietoa uhkista ja hyvistä suojauskäytännöistä. Yhteistyösuhteiden ja tiedonvaihdon kehittäminen voikin parantaa merkittävästi kykyä suojautua kyberuhkilta. Tätä ei myöskään tule nähdä kilpailuriskinä: jaettu tieto koituu lopulta kaikkien hyödyksi.

Arvioikaa uhkat

Merkittävien uhkien ja mahdollisten hyökkääjien kartoittaminen helpottaa päätöksentekoa siitä, miltä uhkilta organisaation tulisi suojautua aktiivisesti.

Organisaation johdon, hallituksen ja asiantuntijoiden välinen jatkuva keskustelu auttaa organisaatiota priorisoimaan uhkia ja tarvittavia suojaustoimenpiteitä. Asiantuntijat ymmärtävät uhkien teknisen luonteen. Hallitus puolestaan tiedostaa, miksi organisaatio voi olla houkutteleva kohde hyökkääjille. Lisäksi on tärkeää keskustella jo etukäteen kaikista sellaisista päätöksistä, joilla voi olla merkittävää vaikutusta organisaation uhkaprofiiliin. Näin teknisillä asiantuntijoilla on riittävästi aikaa toteuttaa tarvittavat suojautumistoimenpiteet.

Kyberturvallisuuskeskus kehottaa kaikkia organisaatioita aktiiviseen tiedonvaihtoon. Kyberturvallisuuskeskus ylläpitää toimialakohtaisia tiedonjakoon keskittyviä ISAC-tiedonvaihtoryhmiä (Information Sharing and Analysis Centre). Varmistakaa, että organisaatio osallistuu aktiivisesti kyberturvallisuuteen liittyvään tiedonvaihtoon esimerkiksi osana toimialan ISAC-ryhmää tai muuta tiedonvaihtotoimintaa. Lisätietoa ISAC-toiminnasta: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Mitä organisaatiossa voidaan tehdä?

Kohdistamattomia hyökkäyksiä ei saa aliarvioida

Kohdistamattomassa hyökkäyksessä hyökkääjä haluaa saavuttaa samalla kertaa tuhansia potentiaalisia uhreja yhden valikoidun kohteen sijaan. Hyökkääjät käyttävät usein automaattisia ja yleisesti saatavilla olevia välineitä, jotka esimerkiksi skannaavat julkisia verkkosivustoja tai muita palveluja haavoittuvien järjestelmien tai palvelujen löytämiseksi. Kun sellainen löytyy, sama työkalu hyödyntää automaattisesti sen haavoittuvuutta esimerkiksi tietomurron toteuttamiseksi. Tällaisen massahyökkäyksen vaikutukset voivat olla yhtä vakavia kuin kohdistetun hyökkäyksen. Kyberturvallisuuden hyvä perustaso kuitenkin suojaa järjestelmät valtaosasta kohdistamattomia hyökkäyksiä.

Hankkikaa hyviä tilannekuvatietoja ja hyödyntäkää niitä

Toimintaa ohjaavia päätöksiä varten tarvitaan tilannekuvatietoa kyberturvallisuudesta. Markkinoilta löytyy paljon toimijoita, jotka tarjoavat tätä tietoa. Niiden sisältö voi vaihdella yleisiä suuntauksia koskevista vuosikertomuksista tietynlaisia haittaohjelmia käsitteleviin teknisiin raportteihin. Suomessa kyberturvallisuuden tilannekuvaa tuottaa muun muassa Kyberturvallisuuskeskus: https://kyberturvallisuuskeskus.fi/fi

Kysymyksiä pohdittavaksi

Mitkä uhkat ovat merkityksellisiä organisaatiolle ja miksi?

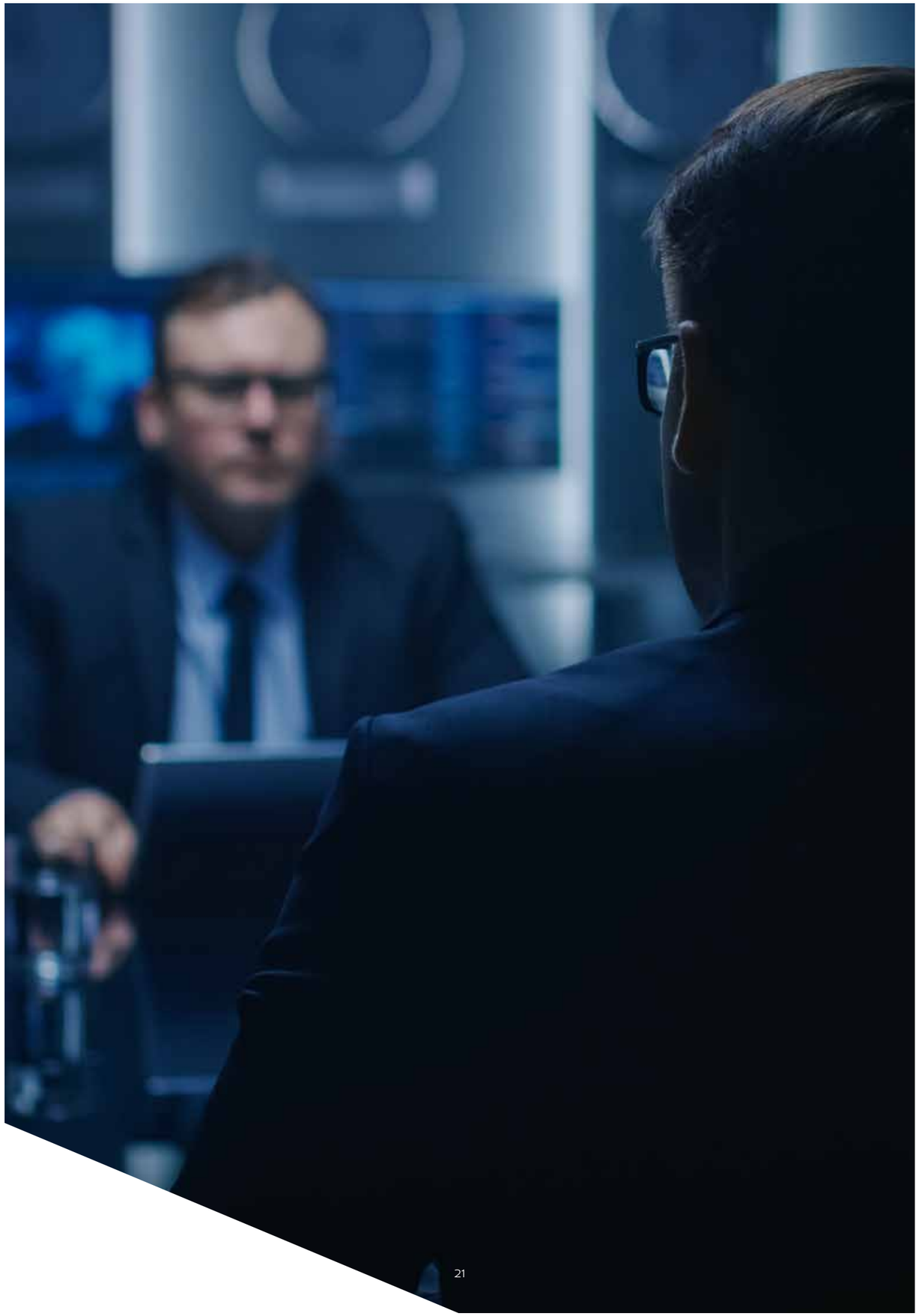
Arvioinnissa:

- määritellään uhkien mahdolliset vaikutukset ja sen todennäköisyys, että uhkat kohdistuvat organisaatioon
- määritellään, millaisia riskejä organisaatio on valmis sietämään
- käytetään hyväksi aineistoa organisaation aiemmin kohtaamista hyökkäyksistä.

Kuinka organisaatiomme pysyy ajan tasalla kyberuhkista?

Organisaatio voi:

- etsiä todisteita hyökkäyksistä mahdollisista järjestelmälokitiedoistaan
- hyödyntää erilaisia tilannekuvatuotteita (esimerkiksi Kyberturvallisuuskeskuksen tilannekuvatuotteet)
- osallistua tiedonvaihtoon (esimerkiksi ISAC-tiedonvaihtoryhmässä)
- ottaa käyttöön keinoja, joilla voi jakaa sisäisesti tietoa keskeisistä kyberuhkista.



V OSA

Kyberturvallisuus osaksi organisaation tavoitteita

Kyberturvallisuus on tärkeä elementti organisaation tavoitteiden toteuttamisessa ja se nähdään yhä useammin myös kilpailukykytekijänä. Tämä edellyttää myönteistä kyberturvallisuuskulttuuria, investointeja kyberturvallisuuteen ja sen asianmukaista hallintaa organisaatiossa.

Mitä hallitus voi tehdä?

Kyberturvallisuus on osa organisaation tavoitteita ja riskejä

Kyberturvallisuus vaikuttaa organisaatioon kokonaisvaltaisesti. Siksi sen on oltava myös osa organisaation riskienhallintaa ja päätöksentekoa – näin sitä voidaan hallita asianmukaisesti. Esimerkiksi:

- Kyberturvallisuus vaikuttaa todennäköisesti operatiivisiin riskeihin, sillä organisaatio on riippuvainen useiden digitaalisten palvelujen turvallisuudesta (sähköpostipalvelut, ohjelmistot, jne.).
- Kyberriski on sidoksissa oikeudellisiin riskeihin, kuten liiketoimintakumppanien tietojen suojaamista koskeviin sopimusvaatimuksiin ja lakisääteisiin vaatimuksiin erityisistä tietojenkäsittelytavoista.
- Kyberriskit voivat olla taloudellisia riskejä. Tällaisia ovat esimerkiksi varojen menettäminen verkkohuijauksissa tai kyberhyökkäyksen aiheuttamat katkot palvelutarjonnassa.
- Kun kyberturvallisuus on hyvällä tasolla, voi organisaatio ottaa suunnitelmallisesti riskejä ja hyödyntää täysimääräisesti uusia teknologioita.

Kyberturvallisuuden tulisi olla sisäänrakennettuna organisaation toimintaan. Kyberturvallisuuden hyvä taso edellyttää toimivan teknologian lisäksi myös sitä, että koko henkilöstö on perehtynyt ja sitoutunut hyviin tietoturvakäytäntöihin. Organisaatio voi estää hyökkääjää saamasta arkaluonteisia tietoja ja varmistaa, että pääsy näihin tietoihin on ainoastaan henkilöillä, joilla on ajantasainen ja todennettu tiedonsaantitarve. Organisaation on tällöin huolehdittava, että:

- Tietojen tekninen säilytysratkaisu on asianmukainen.
- Tietoja käsittelevälle henkilöstölle tarjotaan siihen koulutusta.

Mitä organisaatiossa voidaan tehdä?

Kyberturvallisuus vaikuttaa koko organisaatioon – ei pelkästään tietohallintoon. Siksi sitä ei saa jättää yhden henkilön varaan. Onnistuneet kyberhyökkäykset voivat vaikuttaa esimerkiksi verkkomyyntiin ja sopimussuhteisiin tai johtaa oikeudellisiin tai sääntelyllisiin toimenpiteisiin. Hallituksessa olisikin oltava riittävästi asiantuntemusta, jotta se voi ohjata organisaation kyberturvallisuutta.

Osallistakaa asiantuntijoita

Pohtikaa, saako hallitus tarvitsemansa tiedot organisaation kyberturvallisuudesta. On tärkeää, että organisaatiossa kyberturvallisuudesta vastaavalla henkilöllä on sujuva yhteys organisaation johtoon ja että kyberturvallisuuteen liittyvä raportointi on järjestetty toimivalla tavalla.

Kysymyksiä pohdittavaksi

Ymmärrämmekö, miten kyberturvallisuus vaikuttaa hallituksen ja johdon vastuisiin? Pohtikaa seuraavia asioita:

- Onko hallituksella riittävästi asiantuntemusta, jotta se ymmärtää kyberturvallisuuden merkityksen organisaation liiketoiminnalle ja strategisille tavoitteille?
- Kuka vastaa kyberturvallisuuden valvonnasta?
- Olemmeko viestineet selkeästi, mitä tietoa kyberturvallisuudesta hallitus ja johto tarvitsevat?

Kenellä on vastuu kyberturvallisuudesta tällä hetkellä? Vastuun tulee kuulua nimetylle henkilölle. Pohtikaa seuraavia asioita:

- Miten hän on yhteydessä hallitukseen? Raportoiko hän suoraan hallitukselle tai osallistuuko hän johonkin muuhun raportointiprosessiin? Kannustaako tämä hallitusta osallistumaan aktiivisesti kyberturvallisuutta käsitteleviin keskusteluihin?
- Mitkä hänen tavoitteensa ovat ja kuka ne asettaa? Edistävätkö nämä tavoitteet kyberturvallisuutta koko organisaatiota hyödyttävällä tavalla?
- Onko hänellä yhteydet kaikkiin tarvittaviin henkilöihin tehokkaan kyberturvallisuuden varmistamiseksi? Yksinkertaisimmillaan tämä tarkoittaa, että kyberturvallisuuden parissa työskentelee riittävä määrä henkilöstöä. Sillä voidaan tarkoittaa myös muita organisaation osa-alueita, kuten henkilöstöhallintoa ja taloushallintoa.

Millä tavoin varmistamme hallituksessa sen, että organisaation kyberturvallisuustoimenpiteet ovat tehokkaita? Hallituksen kannattaa varmistaa, että:

- Organisaatiolla on käytössään asianmukaiset tekniset suojautumisratkaisut ja niiden tuloksista tiedotetaan ymmärrettävällä tavalla hallitukselle.
- Uhka-arviot ja tarvittavat suojautumisratkaisut tarkistetaan säännöllisesti ja suojaustoimet päivitetään sen mukaisesti.

Onko organisaatiollamme prosessi, jolla varmistetaan kyberriskien sisällyttäminen osaksi liiketoimintaan liittyviä riskejä?

- Onko organisaatiolla prosessi, jonka avulla eri toimintojen riskejä ja vaikutuksia voidaan arvioida keskenään? Onko organisaatiossa esimerkiksi tehty päätös omien päätelaitteiden, kuten matkapuhelinten käytöstä työasioihin? Tämä voi tuoda tehokkuutta ja joustavuutta työskentelyyn, mutta samalla se vähentää organisaation näkyvyyttä siihen kohdistuviin kyberuhkiin.

VI OSA

Turvallisuuskulttuuri

Organisaatiot keskittyvät usein kyberturvallisuuden teknisiin kysymyksiin ja sivuuttavat ihmisten tarpeet ja heidän arkiset työskentelytapansa. Tämä johtaa harvoin onnistumisiin. Jos virallinen käytäntö vaikeuttaa tai hidastaa työntekoa, ihmiset etsivät tilalle oikoteitä ja epävirallisia työtapoja. Onkin hyvä ymmärtää, ettei henkilöstö sitoudu kyberturvallisuuteen ilman hyvää turvallisuuskulttuuria.

Joissakin organisaatioissa henkilöstöä pidetään kyberturvallisuuden ”heikkona lenkkinä”. Tästä ajattelusta on päästävä eroon.

Mitä hallitus voi tehdä?

Johtakaa näyttämällä esimerkkiä

Hallituksella ja ylimmällä johdolla on merkittävä vaikutus muiden asenteisiin. Voi olla, ettei ylemmän johdon tarvitse noudattaa turvallisuuskäytäntöjä ja prosesseja. He saattavat saada myös erityiskohtelua, kuten organisaation IT-politiikasta poikkeavan laitteen. Tämä kuitenkin viestittää muulle organisaatiolle, että sääntöjä ei välttämättä pidetä tarkoituksenmukaisina tai niiden kiertäminen on hyväksyttävää.

Jos johto ja hallituksen jäsenet eivät itse noudata organisaatiossa sovittuja käytäntöjä, niitä tuskin noudattavat muutkaan. Jos jollakin käytännöllä on haitallinen vaikutus organisaatioon, sitä on muokattava paremmaksi.

Kulttuurin kehittyminen vie aikaa ja vaatii yhteisiä ponnisteluja. Hallituksen ja johdon vaatima turvallisuusasenne ei leviä itsestään ja automaattisesti koko organisaatioon.

Mitä organisaatiossa voidaan tehdä?

Henkilöstö turvallisuuden keskiöön

Joissakin organisaatioissa pidetään henkilöstöä kyberturvallisuuden heikkona lenkkinä. Tästä ajattelusta on päästävä eroon. Tehokas kyberturvallisuuden toteuttaminen edellyttää kaikkien eri tekijöiden tasapainottamista – ei pelkästään olettamusta, että ihmiset taipuvat aina teknologian vaatimuksiin. Jos henkilöstö pyrkii kiertämään sovittuja toimintamalleja, se voi kertoa käytäntöjen tai prosessien kaipaavan tarkistamista.

Koulutettu ja valpas henkilöstö on turvallisuuspoikkeamien havaitsemisessa keskeisessä roolissa. Organisaatiossa onkin varmistettava, että henkilöstö raportoi havaitsemistaan uhkista ja poikkeamista. Lisäksi niiden käsittelyyn on oltava selkeät prosessit.

Kohti avoimuuden kulttuuria

Varmistakaa, että henkilöstöä kannustetaan puhumaan ja raportoimaan huolenaiheistaan. Samalla on tähdennettävä, että niiden pohjalta tartutaan asianmukaisiin toimenpiteisiin eikä syyllisiä etsitä. Näin henkilöstö voi keskittyä organisaation turvallisuuden kehittämiseen sen sijaan, että he keskittyisivät suojelemaan itseään.

Kysymyksiä pohdittavaksi

Miten hallituksen jäsenet ja johto voivat näyttää esimerkkiä?

- Varmistakaa, että työntekijät kokevat voivansa vaikuttaa organisaation turvallisuuteen ja että heillä on välineet tuoda esiin turvallisuuteen liittyviä huolenaiheita.
- Sitoutukaa jo tehtyihin turvallisuutta koskeviin päätöksiin, noudattakaa niitä ja nostakaa esiin tehottomia käytäntöjä yhteistyössä työntekijöiden kanssa.
- Varmistakaa, että organisaatiossa puhutaan avoimesti ja myönteisesti henkilöstölle siitä, miksi kyberturvallisuus on tärkeää.

Vallitseeko organisaatiossamme hyvä turvallisuuskulttuuri?
Hyvästä turvallisuuskulttuurista kertoo esimerkiksi se, että:

- Henkilöstö tietää, miten ja kenelle huolenaiheista tai poikkeamista voi raportoida. He myös kokevat olevansa kannustettuja raportointiin.
- Henkilöstö ei pelkää negatiivisia seurauksia raportoidessaan huolenaiheista tai poikkeamista.
- Henkilöstö kokee voivansa kyseenalaistaa toimintamalleja rakentavalla tavalla.
- Henkilöstön näkemyksiä hyödynnetään aidosti turvallisuuskäytäntöjen muovaamisessa.
- Henkilöstö ymmärtää kyberturvallisuuden tärkeyden ja merkityksen organisaatiolle.
- Epäonnistumisten sijaan raportoinnissa ja sisäisessä viestinnässä keskitytään onnistumisiin (kerrotaan esimerkiksi moniko raportoi tietojenkalastelusähköposteista, eikä sitä moniko lankesi niihin).

VII OSA

Kyberturvallisuusosaaminen

Kyberturvallisuusosaajien kysyntä kasvaa jatkuvasti. Tämä aiheuttaa haasteita organisaatioiden tarvitseman osaamisen saatavuudelle. Sikäli on tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa sekä miten tuo osaaminen hankitaan.

Mitä hallitus voi tehdä?

Ymmärtäkää organisaation tilanne

Onko organisaatiossa tietoturvapäällikkö tai -johtaja? Entä tietoturvaryhmä? Poikkeamien hallinnasta vastaavia henkilöitä? Jos ei, niin pitäisikö olla?

Nämä tiedot antavat käsityksen organisaation kyberturvallisuuskyvystä. Ne auttavat myös ymmärtämään, mistä hallituksen saamat tiedot organisaation kyberturvallisuudesta ovat peräisin.

Hallituksen kannattaa myös pohtia omaa asiantuntemustaan. Onko hallituksessa tällä hetkellä riittävästi asiantuntemusta sen varmistamiseksi, että hallitus kykenee tekemään asianmukaisia strategisia päätöksiä kyberturvallisuuteen liittyen? Pysyykö hallitus kehityksen mukana, kun uudet teknologiat tuovat mukanaan uusia turvallisuushaasteita?

Global Information Security Workforcen tekemän tutkimuksen mukaan pelkästään Euroopassa tulee olemaan vuoteen 2022 mennessä 350 000 kyberturvallisuusammattilaisen saatavuusvaje.

Mitä organisaatiossa voidaan tehdä?

Laatikaa suunnitelma

Organisaatiossa tulee selvittää, millaista kyberturvallisuuteen liittyvää asiantuntemusta se tarvitsee. Kyberturvallisuuteen liittyy monia erilaisia taitoja, jotka vaihtelevat esimerkiksi tietoverkkojen turvallisuudesta aina riskien- ja poikkeamienhallintaan asti. Ensiksi onkin hyvä pohtia, mitä taitoja organisaatio tarvitsee tärkeimpien tavoitteiden saavuttamiseksi ja riskien hallitsemiseksi. Sen jälkeen voidaan arvioida, mitä näistä taidoista ei voida hankkia ulkoistettuna.

Määritelkää, miten nopeasti organisaatio tarvitsee näitä taitoja. Jos ajatuksena on kehittää nykyisen henkilöstön osaamista, kannattaa huomioida, että riittävän asiantuntemuksen saavuttaminen vie aina aikaa. Yksittäiset kurssit eivät vielä tee kenestäkään kyberturvallisuuden asiantuntijaa – sen lisäksi on oltava myös mahdollisuus kehittää käytännön osaamistaan. Jos asiantuntemusta tarvitaan nopeasti, konsultin tai asiantuntijan palkkaaminen on usein parempi vaihtoehto.

Kysymyksiä pohdittavaksi

Millaista kyberturvallisuusasiantuntemusta organisaatiomme tarvitsee ja millaista asiantuntemusta organisaatiollamme on?

- Millaista asiantuntemusta organisaatiomme tarvitsee kyberriskien hallitsemiseksi?
- Mitkä tehtävät on säilytettävä talon sisäisinä ja mitkä kannattaa ulkoistaa?
- Millaista osaamista kaikilla organisaation työntekijöillä on oltava kyberturvallisuudesta?
- Miten hyvin ja kuinka usein järjestämme henkilöstölle koulutusta turvallisuuskäytännöistä? Entä erityisistä uhkista, joille organisaatiomme voi olla haavoittuvainen?

Millainen suunnitelma organisaatiolla on puuttuvan asiantuntemuksen kehittämiseksi?

- Ketkä ovat vastuussa kyberturvallisuuteen liittyvän asiantuntemuksen kehittämisestä?
- Perustuuko kehittäminen suunnitelmaan ja kenelle/keille he ovat vastuussa sen toteuttamisesta?
- Mistä tarvittavat ihmiset löydetään? Työskentelevätkö he organisaatiossamme vai hankintaanko tarvittava osaaminen esimerkiksi ulkoistuksena?
- Miten hallitus voi tukea tätä työtä?

Onko hallituksella riittävä tietämys ja asiantuntemus, jotta se voi olla vastuussa kyberturvallisuutta koskevista päätöksistä?

- Ymmärretäänkö hallituksessa tarpeeksi hyvin organisaatiossa tehtävät kyberturvallisuutta koskevat päätökset?
- Jos ei, niin miten hallituksen jäsenet voivat parantaa ymmärrystään?
    - Voitte aloittaa lukemalla tämän oppaan. Monet tahot järjestävät myös koulutuksia kyberturvallisuudesta erityisesti hallituksen jäsenille.

Miten varmistamme, että meillä on tulevaisuuden kyberturvallisuushaasteiden ratkaisemiseen kykenevä henkilöstö?

- Saammeko tarvittavaa tietoa organisaation kyberturvallisuuteen liittyvistä osaamis- ja rekrytointitarpeista?
- Käytämmekö monipuolisesti erilaisia rekrytointikanavia?

VIII OSA

Toimenpiteiden seuranta

Jopa hyvin yksinkertaisten toimenpiteiden toteuttaminen auttaa vähentämään poikkeamien todennäköisyyttä tai vaikuttavuutta.

Mitä hallitus voi tehdä?

Perehtykää hieman teknologiaan

Perusymmärrys kyberturvallisuudesta auttaa esittämään oikeita kysymyksiä, joiden avulla hallituksen jäsenet voivat varmistaa organisaation kyberturvallisuuden tason. Voitte aloittaa keskustelemalla nykyisistä kyberturvallisuustoimenpiteistä organisaation asiantuntijoiden kanssa. Alla esitetyt kysymykset antavat suuntaa siitä, mitä kannattaa kysyä.

Mitä organisaatiossa voidaan tehdä?

Aloittakaa kyberturvallisuuden perustasosta

Hyökkääjät käyttävät usein tavanomaisia, julkisesti saatavilla olevia sovelluksia ja menetelmiä, joista monet ovat torjuttavissa varmistamalla kyberturvallisuuden perustaso. On olemassa useita kehyksiä, joissa määritellään, millaisia hyvät kyberturvallisuuden perustason toimenpiteet ovat. Niitä ovat esimerkiksi ISO/IEC 27000 -tietoturvastandardit ja NIST:n (National Institute of Standards and Technology) kyberturvallisuuskehys. Kyberturvallisuuskeskus julkaisee vuonna 2020 Kybermittarin. Se on kansallinen arviointimittaristo, jonka avulla organisaatio voi arvioida omaa kyberturvallisuuden tilaansa.

Räätälöikää toimenpiteet tärkeimpien riskien mukaisesti

Kyberturvallisuuden perustason toimenpiteet auttavat torjumaan yleisimpiä kyberhyökkäyksiä. Kun perustaso on määritetty ja saavutettu, on syytä toteuttaa tarvittavat toimenpiteet priorisoitujen riskien hallitsemiseksi. Nämä toimenpiteet tulee räätälöidä liiketoimintatavoitteiden, organisaation teknisen ympäristön ja organisaation uhkaprofiilin (suojautuminen tietyiltä uhkilta ja/tai hyökkääjiltä) mukaisesti.

Monikerroksisen tietoturva-arkkitehtuurin avulla varaudutaan siihen, että yksittäisen osa-alueen pettäessä tai murtautujan päästessä yhdestä kerroksesta läpi, estävät seuraavat kerrokset hyökkääjän etenemisen. Organisaatiossa tulisikin toteuttaa samanaikaisesti useita eri toimenpiteitä, jotka yhdessä käytettynä auttavat pienentämään kyberuhkien vaikutuksia. Kun organisaatiossa on määritelty kyberturvallisuuden tavoitteet, voidaan keskittyä suojatoimien kerrostamiseen tärkeimpien asioiden ympärille.

> Kyberturvallisuuskeskuksen HAVARO-palvelu havainnoi ja varoittaa organisaatiota vakavista tietoturvaloukkauksista. Tällaisia ovat esimerkiksi organisaation talouteen, sen hallussa olevaan tietoon tai liiketoiminnan jatkuvuuteen vaikuttavat tietoturvauhkat. Lisätietoa HAVARO-palvelusta https://www.kyberturvallisuuskeskus.fi/fi/havaro-palvelu

Suojautukaa myös sisäisiltä uhkilta

Suojaustoimenpiteet eivät pääty organisaation verkon rajalle. Hyvässä suojautumisessa oletetaan, että hyökkääjä voi koska tahansa päästä sisälle organisaatioon verkkoon. Sisäverkon suojauksella pyritään minimoimaan vahingot, joita hyökkääjä voi saada aikaan.

Tässä kohtaa yksi keskeisistä toimista on identiteetin- ja pääsynhallinta. Yleisiä menetelmiä ovat käyttäjien valtuuksien tehokas hallinta ja organisaation verkon jakaminen osiin eli segmentointi. Järjestelmään tunkeutumisen mahdollisimman nopea tunnistaminen vähentää hyökkääjän mahdollisuuksia aiheuttaa vahinkoa. Lokien kerääminen ja niiden seuranta ovat keskeisiä toimenpiteitä tällaisen haitallisen toiminnan havaitsemisessa.

Nämä toimenpiteet auttavat myös rajoittamaan organisaation sisältä tulevaa uhkaa. Tällä tarkoitetaan henkilöä, jolla on luvallinen pääsy järjestelmiin, mutta joka pyrkii aiheuttamaan organisaatiolle vahinkoa. Tämä uhka vaihtelee työntekijän luvattomista toimista aina suunnitelmalliseen yritysvakoiluun asti.

Tarkistakaa ja arvioikaa toimenpiteet

Hyvässä kyberturvallisuudessa on kyse jatkuvasta toiminnasta, johon kuuluvat oikean ja riittävän tiedon saatavuus, tietoon perustuvat päätökset ja toimenpiteet riskien vähentämiseksi. Organisaatiossa on arvioitava ja mukautettava suojatoimia sitä mukaa, kun organisaatio ja sen uhkaprofiili muuttuvat. Siksi on tärkeää omata välineet, joilla voi arvioida organisaation toteuttamien toimenpiteiden tehokkuutta.

Toimenpiteiden tehokkuutta voidaan arvioida eri tavoin, kuten esimerkiksi testaamalla organisaation verkkojen ja palvelujen turvallisuutta (ns. penetraatiotestaus) tai harjoittelemalla prosessien toimivuutta. On myös mahdollista yhdistää sisäisiä arviointitoimenpiteitä ulkoisen tahon tekemään arviointiin.

Henkilöstön osallistaminen auttaa saamaan tarkemman kuvan organisaation toteuttamien toimenpiteiden tehokkuudesta. Sen avulla voidaan myös saada arvokasta tietoa siitä, miten käytäntöjä tai prosesseja voitaisiin parantaa. Erilaiset mittarit ja indikaattorit voivat osoittaa, missä asioissa organisaation on muutettava tai kehitettävä toimintaansa.

Kysymyksiä pohdittavaksi

Kuinka organisaatiomme varmistaa, että toimenpiteemme ovat tehokkaita?

Organisaatiossa voidaan käyttää tämän varmistamiseen esimerkiksi seuraavia toimenpiteitä:

- Ulkoisen organisaation tekemä penetraatiotestaus ja sen tulosten perusteella toteutetut kehitystoimenpiteet.
- Suojaustoimenpiteiden automaattinen testaus ja verkossa tapahtuvan toiminnan lokitus ja seuranta.
- Tehtyjen toimenpiteiden arviointi soveltuvien kehysten perusteella. Kyseessä voi olla sisäinen tai riippumattoman konsultin tekemä arviointi. Soveltuvia kehyksiä voivat olla esimerkiksi ISO/IEC 27002 standardi, NIST:n kyberturvallisuuskehys tai Kyberturvallisuuskeskuksen kansallinen Kybermittari.
- Varmistetaan, että uhka-arvioinnit ja kyberturvallisuutta koskevat painopisteet tarkistetaan säännöllisesti ja suojatoimet päivitetään sen mukaisesti.
- Varmistetaan, että kyberturvallisuustoimenpiteiden painopisteet on yhdenmukaistettu hallituksen määrittelemien ja painottamien riskien kanssa.

Mihin toimenpiteisiin organisaatiomme on ryhtynyt minimoidakseen hyökkäyksestä aiheutuvat vahingot?

Varmistakaa, että organisaatiossa pohditaan esimerkiksi seuraavia asioita:

- Kuinka käyttäjät ja päätelaitteet todennetaan ja miten näille myönnetään käyttöoikeuksia?
- Kuinka hyökkääjän läsnäolo organisaation verkossa havaitaan?
- Onko organisaation verkot eriytetty siten, ettei hyökkääjä pääse yhden laitteen tai verkkoalueen kautta muihin organisaation verkkoalueisiin?

Millä tavoin organisaatiomme suojautuu tietojenkalasteluhyökkäyksiltä?

- Suodatamme tai estämme saapuvat tietojenkalastelusähköpostit.
- Varmistamme, että ulkoiset postit merkitään ulkoisiksi.
- Estämme hyökkääjiä väärentämästä omia sähköpostiviestejämme.
- Autamme henkilöstöämme tunnistamaan epäilyttävät sähköpostiviestit ja raportoimaan niistä.

Millä tavoin organisaatiomme valvoo tietoteknisten käyttäjätilien valtuuksien käyttöä?

- Sovellamme pienimmän valtuuden periaatetta, kun luomme henkilöstön käyttäjätilejä.
- Rajoitamme hyökkäysten vaikutusta valvomalla valtuutettuja käyttäjätilejä.

Millä tavoin organisaatiomme varmistaa, että ohjelmistomme ja laitteemme ovat ajan tasalla?

- Olemme määritelleet prosessit, joiden avulla havaitsemme, luokittelemme ja korjaamme hyödynnettävissä olevat haavoittuvuudet teknisessä ympäristössämme.
- Olemme laatineet elinkaaren päättymistä koskevat suunnitelmat laitteille ja ohjelmistoille, joiden käyttöä ei enää tueta.
- Verkkoarkkitehtuurimme minimoi vahingot, joita hyökkääjä voi aiheuttaa.
- Hyödynnämme asianmukaisesti kolmannen osapuolen palveluja tai pilvipalveluja ja keskitymme siihen, mihin voimme vaikuttaa eniten.

Miten henkilöiden tunnistaminen sekä pääsy järjestelmiin ja dataan on toteutettu?

- Organisaatiossa noudatetaan hyviä salasanakäytäntöjä.
- Organisaatiossa käytetään kaksivaiheista tunnistautumista, kun se on mahdollista.

IX OSA

Yhteistyö

Kyberturvallisuus on keskeinen asia tehtäessä yhteistyötä palveluntarjoajien ja kumppaneiden kanssa. Tämä johtuu siitä, että:

- Ulkoiset hyökkäysreitit organisaatioon lisääntyvät erilaisten yhteyksien ja palvelujen määrän kasvaessa. Jos joku niistä vaarantuu, myös organisaationne voi olla vaarassa.
- Organisaationne kautta voidaan yrittää tunkeutumista toiseen organisaatioon, jolle tarjoatte palveluja.
- Organisaatioonne voidaan yrittää tunkeutua palveluntarjoajanne kautta.
- Organisaationne saattaa käsitellä kumppaneillenne arkaluonteisia tai arvokkaita tietoja.

Mitä hallitus voi tehdä?

Sisällyttäkää kyberturvallisuus päätöksiin

Kaikki organisaatiot ovat tekemisissä ainakin yhden muun organisaation kanssa. Näihin suhteisiin liittyy tavallisesti pääsy organisaation järjestelmiin, verkkoon tai tietoihin. Varmistakaa seuraavat kolme asiaa:

1. Hyökkääjälle ei saa tarjota reittiä, jota pitkin hän pääsee organisaatioonne sisälle.
2. Kaikkien kumppanien ja palveluntarjoajien on käsiteltävä organisaationne arkaluonteisia tietoja asianmukaisella ja turvallisella tavalla.
3. Kyberturvallisuuden tulee olla huomioituna kaikissa ostetuissa tuotteissa tai palveluissa.

Kyberturvallisuuden on oltava mukana uusia suhteita tai kumppanuuksia koskevissa päätöksissä. Tähän sisältyvät palveluntarjoajia, tavarantoimittajia, fuusioita, yritysostoja ja kumppaneita koskevat päätökset. Myös vanhoissa suhteissa kannattaa varmistaa kyberturvallisuuteen liittyvien vastuiden ja velvollisuuksien ajantasaisuus.

Mitä organisaatiossa voidaan tehdä?

Määritelkää palveluntarjoajilta ja kumppaneilta odotetut turvallisuusvaatimukset ja viestikää niistä heille selkeästi.

Tarkistakaa nykyiset palveluntarjoajia koskevat järjestelyt ja varmistakaa, että niihin liittyvät turvallisuusvaatimukset on huomioitu. Jos organisaationne on itse palveluntarjoaja, teidän on täytettävä myös asiakkaan asettamat turvallisuusvaatimukset.

Varmistakaa, että määrittelemänne turvallisuusvaatimukset ovat perusteltuja, oikeasuhteisia ja että ne sopivat yhteen arvioitujen riskien kanssa. Huomioikaa palveluntarjoajien nykyinen tilanne ja antakaa niille tarpeeksi aikaa tehdä tarvittavat parannukset.

Pyytäkää takeet

Turvallisuus on sisällytettävä alusta alkaen kaikkiin sopimuksiin. Organisaation on voitava luottaa siihen, että sovitut turvallisuusvaatimukset on täytetty. Tämä voidaan varmistaa esimerkiksi testien, tarkastusten tai standardien noudattamisen avulla. Kyberturvallisuuden ylläpidon ja poikkeamien hallinnan prosessien käyttöä kannattaa harjoitella kumppanien kanssa.

Huomioikaa palveluntarjoajan vaarantumisen seuraukset.

Riippumatta turvallisuutta koskevista sopimuksista tai kumppanienne kyberturvallisuustasosta, on oletettavaa, että kumppanit vaarantuvat jossain vaiheessa. Suunnitelkaa verkkojen, järjestelmien ja tietojen turvallisuus tämän olettamuksen mukaisesti. Tämä on hyvä huomioida myös turvallisuutta koskevissa sopimuksissa. Miten kumppanien odotetaan toimivan? Onko heidän esimerkiksi ilmoitettava poikkeamista organisaatiollenne?

Kysymyksiä pohdittavaksi

Millä tavoin organisaatio rajoittaa riskejä, jotka liittyvät tietojen, järjestelmien ja yhteyksien jakamiseen muiden organisaatioiden kanssa?

Varmistakaa seuraavat:

- Organisaatiolla on oltava hyvä ymmärrys palveluntarjoajistaan ja siitä, mihin tietoihin ja järjestelmiin heillä on pääsy. Lisäksi tarvitaan prosessi pääsyoikeuksien myöntämiselle ja poistamiselle.
- Määritelkää selkeästi odotukset siitä, miten kumppanien on suojeltava organisaationne tietoja ja käytettävä järjestelmiänne.
- Sisällyttäkää kyberturvallisuus kaikkiin sopimuksiin alusta alkaen.

Toimikaa seuraavasti:

- Jos toimitusketjuun kuuluu hyvin suuri määrä yrityksiä, sopikaa tärkeimpien palveluntarjoajien kanssa prosesseista, jotka ohjaavat niiden alihankintoja ja ilmoitusvelvollisuuksia teitä kohtaan.
- Valitkaa organisaatioita, jotka voivat osoittaa toimintansa turvallisuuden.
- Minimoikaa muiden organisaatioiden pääsy palveluihinne ja niiden kanssa vaihtamienne tietojen määrä.
- Todentakaa ja varmentakaa alihankkijoiden käyttäjät ennen käyttöoikeuksien myöntämistä.

Millä tavoin organisaatiomme varmistaa sen, että kyberturvallisuus otetaan huomioon liiketoimintaan liittyvissä päätöksissä?

- Varmistakaa, että turvallisuus on osa organisaation kulttuuria ja strategiaa.
- Huolehtikaa, että turvallisuus otetaan tietoisesti huomioon kaikissa hankintoja, fuusioita tai yritysostoja koskevissa päätöksissä.

Onko organisaatiomme varma siitä, että se täyttää siltä palveluntarjoajana edellytetyt turvallisuutta koskevat vaatimukset?

- Jos organisaatio tarjoaa palveluita muille organisaatioille, on sen riskit suuremmat. Varmistakaa, että organisaatio on valmistautunut vastaamaan tilanteisiin, joissa hallussanne oleva asiakastieto on vaarantunut.

Onko organisaatiolla selvät palveluntarjoajien käyttöä koskevat ehdot? Entä olemmeko tiedottaneet niistä? Onko seuraavat asiat selkeästi kuvattu palveluntarjoajia ja hankintoja koskevassa strategiassa tai ohjeistuksissa?

- Mitä riskejä organisaatio on valmis hyväksymään, kun se käyttää palveluntarjoajia? Esimerkiksi poikkeamatilanteista syntyvät maineriskit voivat olla pienempiä, jos vastuun kantaa palveluntarjoaja. Taloudellinen riski voi kuitenkin olla yhtä suuri kuin ilman palveluntarjoajaa.
- Mitä organisaatio odottaa palveluntarjoajien turvallisuudelta? Kuinka paljon se on valmis maksamaan paremmasta turvallisuuden tasosta?

X OSA

Kun pahin tapahtuu

Tietoturvaloukkauksilla voi olla merkittävä vaikutus organisaation talouteen, tuottavuuteen ja maineeseen. Poikkeama voi kehittyä myös koko organisaation toimintaan laajasti vaikuttavaksi häiriöksi. Valmistautuminen loukkausten havainnointiin ja nopeaan reagointiin auttaa rajoittamaan vahinkoja. Tämä puolestaan vähentää taloudellisia ja muita toimintaan liittyviä vaikutuksia.

Kyberturvallisuuskeskus auttaa kaikkia tietoturvaloukkauksen kohteeksi joutuneita suomalaisia organisaatioita. Kyberturvallisuuskeskuksen yhteystiedot löytyvät tämän oppaan takasivulta.

Mitä hallitus voi tehdä?

Varmistakaa, että organisaatiolla on suunnitelma

Suurella osalla suomalaisista organisaatioista ei ole suunnitelmaa siitä, miten se toimii tietoturvaloukkauksissa tai näistä johtuvissa vakavissa häiriötilanteissa. Varmistakaa, että organisaatiollanne on suunnitelma tietoturvaloukkausten ja vakavien häiriöitilanteiden varalle.

Ymmärtäkää roolinne tietoturvaloukkausten hallinnassa

Erityisesti laajojen häiriöiden kohdalla yksilöiden ja organisaatioiden päätöksentekokyky usein heikkenee. Tämän vuoksi kaikkien on sisäistettävä oma roolinsa ja organisaation toimintatapa jo etukäteen.

Hallituksen on tehtävä selväksi, milloin sille on raportoitava tietoturvaloukkauksista.

- Missä vaiheessa hallitukselle pitää ilmoittaa loukkauksesta?
- Entä millainen loukkaus ylittää ilmoituskynnyksen?

Osallistukaa harjoituksiin

Paras tapa testata organisaation prosesseja ja rooleja on harjoitella kyberhäiriötilanteiden hallintaa. Jos henkilön tehtäviin kuuluu osallistua todellisen häiriön hallintaan, sitä tulisi myös harjoitella. Harjoittelu yhdessä henkilöstön kanssa voi nostaa esiin esimerkiksi päätöksentekoon liittyviä ongelmia. Harjoitus voidaan mieltää organisaatiota kohtaavaksi kriisiksi, jonka ajankohta ja vaikutukset voidaan itse valita. Kriisitilanteista oppiminen on erittäin arvokasta. Harjoituksen avulla tätä oppimisen tapaa voidaan soveltaa ilman, että kriisi haittaisi organisaation toimintaa.

Edistäkää kulttuuria, jossa ei syytellä

Tietoturvaloukkauksen jälkeisellä analyysillä pyritään vähentämään loukkausten todennäköisyyttä ja vaikutuksia tulevaisuudessa. Tärkeintä on olla rehellinen ja objektiivinen siitä, mitä on tapahtunut. Tämä onnistuu organisaatiokulttuurissa, jossa ei pyritä löytämään syyllisiä. Hallituksen kannattaa huomioida, että suurin osa sääntelystä, kuten esimerkiksi EU:n yleinen tietosuoja-asetus, siirtää vastuun tietoturvaloukkauksista organisaatiolle eikä yksittäisille henkilöille. Siksi hallitus on hallintoelimenä lopulta vastuussa kaikista poikkeamista organisaation kyberturvallisuudessa.

Mitä organisaatiossa voi tehdä?

Selvittäkää, miltä tietoturvaloukkaus näyttäisi

Yksi yleisimmistä huomiotta jätetyistä asioista on kyky määritellä, mitä tietoturvaloukkauksella tarkoitetaan. Tähän liittyy kolme eri näkökohtaa:

- miten tapahtuma tai poikkeama alun alkaen havaitaan?
- missä vaiheessa tapahtumasta tai poikkeamasta tulee tietoturvaloukkaus?
- missä vaiheessa siitä kehittyy niin vakava häiriö, että tilanne vaatii normaaliprosessista poikkeavia toimintamalleja?

KUINKA TAPAHTUMA HAVAITAAN?

Seurannalla tarkoitetaan verkoista tai järjestelmistä kerättyjen tietojen tai lokien tarkkailemista sellaisten poikkeamien havaitsemiseksi, jotka voivat viitata haitalliseen toimintaan. Vaikka käytössä ei olisi varsinaista seurantamekanismia, on järjestelmä- ja verkkolokitietojen kerääminen tärkeää. Niitä voidaan käyttää poikkeaman selvittämiseen ja jatkossa myös niiltä suojautumiseen.

MILLOIN TAPAHTUMASTA TULEE TIETOTURVALOUKKAUS?

Tämä ei ole aina täysin selvää. Organisaatio voi yrittää kerätä mahdollisimman paljon tietoja ”tapahtumaa” koskevan arvioinnin pohjaksi, mutta sillä ei ole todennäköisesti kokonaiskuvaa siitä mitä on tapahtunut. Usein tapahtuman selvittäminen ja siihen reagointi voivat aiheuttaa kustannuksia. Mikäli tapahtuma on vakava, voi se vaikuttaa organisaation maineeseen ja tuottavuuteen. Organisaatiossa tuleekin määrittää etukäteen, kenellä on valtuudet tehdä päätös tapahtumaan reagoinnista ja mitkä ovat päätöksentekoon liittyvät kynnysarvot.

Lisäksi on suunniteltava, miten rajoitetaan kumppaneihin tai asiakkaisiin kohdistuvia vaikutuksia, jos organisaation kyberturvallisuus vaarantuu. Milloin heille on ilmoitettava? Millä keinoin heille aiheutuvia vahinkoja voidaan rajoittaa?

Lisäksi tulee pohtia, miten organisaatio toimii, jos palveluntarjoajan tietoturva vaarantuu. Organisaatio ei voi välttämättä vaikuttaa siihen, miten palveluntarjoaja käsittelee tietoturvaloukkauksen. Mitä organisaatio voi tehdä itsenäisesti vaikutusten rajoittamiseksi?

MIKÄ ON TIETOTURVALOUKKAUS?

Tietoturvaloukkauksella tarkoitetaan järjestelmän tai palvelun turvallisuuteen kohdistunutta loukkausta. Tavallisesti kyse on jostakin seuraavista:

- järjestelmään ja/tai tietoihin tunkeutuminen tai sen yritys
- tietojen käsittelyyn tai säilyttämiseen käytettyjen järjestelmien luvaton käyttö
- järjestelmien laiteohjelmistoihin, ohjelmistoihin tai laitteisiin ilman järjestelmän omistajan lupaa tehdyt muutokset
- palvelun tahallinen häirintä ja/tai estäminen.

Hyödyntäkää jo valmiiksi olevia tietoja

Uhkista ja teknisestä ympäristöstä kerätyt tiedot tarjoavat tärkeitä tietoja kahdella tavalla:

- Ne tarjoavat tietoja loukkauksen vaikutuksista. Mihin hyökkääjällä voi olla pääsy, jos hän on päässyt johonkin tiettyyn laitteeseen? Voiko hyökkääjä päästä käsiksi organisaatiosi kriittisiin tekijöihin?

- Ne auttavat määrittelemään tarvittavat toimenpiteet. Jos hyökkääjä on päässyt sisään tiettyyn verkkoon, onko kyseinen verkko mahdollista eristää? Jos eristäminen on mahdollista, mitä vaikutusta sillä on organisaation toimintaan?

Ryhtykää ennaltaehkäiseviin toimenpiteisiin

Ottakaa käyttöön toimenpiteet, jotka auttavat rajoittamaan hyökkäyksen aiheuttamia vahinkoja. Tällaisia toimenpiteitä voivat olla:

- organisaation verkkoon päässeiden hyökkääjien etenemisen rajoittaminen
- hyökkäysten vaikutuksen ennaltaehkäisevä rajoittaminen – esimerkiksi tietojen varmuuskopiointi auttaa rajoittamaan kiristyshaittaohjelman vaikutusta.

Kuten muissakin suojatoimissa, näissä toimenpiteissä on keskityttävä suojelemaan organisaatiolle tärkeimpiä asioita.

Laatikaa suunnitelma tietoturvaloukkausten ja niiden aiheuttamien kyberhäiriöiden hallitsemiseksi

Suunnitelman on katettava teknisten osa-alueiden lisäksi:

- ihmiset ja prosessit, kuten tiedotusvälineet sekä viestintä asiakkaille ja sidosryhmille
- ilmoituksen tekeminen Kyberturvallisuuskeskukselle
- raportointi sääntelyviranomaisille
- rikosilmoituksen tekeminen Poliisille.

Yleisimpiä poikkeamia varten voi olla hyödyllistä laatia erityinen suunnitelma, jossa määritellään organisaation toimenpiteet.

Muistakaa myös harjoitella!

Saadut kokemukset

Tietoturvaloukkauksen jälkeinen arviointi jää usein tekemättä. Loukkaus voi tarjota arvokkaita tietoja organisaation kyberturvallisuudesta. Esimerkiksi:

1. Organisaatioon kohdistunut uhka
   - Kuka teki hyökkäyksen? Oliko se kohdistettu?
   - Tehtiinkö hyökkäys odotetulla tavalla?
   - Oliko hyökkäyksen kohteena odotetut asiat?

2. Suojaustoimien tehokkuus
   - Mitä suojaustoimet suojasivat?
   - Mitä ne eivät suojanneet?
   - Voidaanko niitä parantaa?

3. Loukkaukseen reagointiin liittyvien toimenpiteiden tehokkuus
   - Mitä olisi pitänyt tehdä toisin?
   - Auttoivatko toimenpiteet rajoittamaan loukkauksen vaikutuksia?
   - Pahensivatko tai vaikeuttivatko ne joitakin asioita?

Kyberturvallisuuskeskus tukee organisaatioita harjoitusten järjestämisessä. Palvelujemme avulla organisaatio voi käynnistää oman harjoitustoimintansa tai saada asiantuntijoiltamme apua jo olemassa olevan harjoitusohjelman sisällön suunnitteluun. Lisätietoa harjoitustoiminnasta: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/harjoitustoiminta

Kysymyksiä pohdittavaksi

Onko organisaatiollamme käytössään poikkeamienhallintasuunnitelma? Miten varmistamme, että suunnitelma toimii tehokkaasti? Suunnitelmaan täytyy sisältyä ainakin seuraavat asiat:

- Keskeiset sisäiset ja ulkoiset yhteystiedot.
- Selvät eskalointireitit (esimerkiksi ylemmälle johdolle) ja määritellyt prosessit kriittisiä päätöksiä varten.
- Selvä vastuunjako ja maininta siitä, koskeeko se tavallisia työaikoja vai onko se aina voimassa.
- Yleinen vuokaavio tai prosessikuvaus tapahtuman ja tietoturvaloukkauksen koko elinkaarta varten.
- Ohjeet sääntelyvaatimuksista – esimerkiksi siitä, milloin tietoturvaloukkauksista on ilmoitettava ja kenelle.

Tiedetäänkö organisaatiossamme, mistä voi pyytää apua tietoturvaloukkauksen yhteydessä?

- Onko organisaatiossa listattu tärkeät yhteystiedot?
- Ovatko yhteystiedot oikeiden henkilöiden saatavilla myös tilanteessa, jossa pääsy tietojärjestelmiin on estynyt?

Opimmeko organisaationa tietoturvaloukkauksista ja läheltä piti tilanteista?

- Kerätäänkö organisaatiossa opit ja kokemukset?
- Kehitetäänkö organisaation toimintaa niiden perusteella?

Miten tietoturvaloukkaukset tulevat organisaatiomme tietoon?

- Miten organisaatiossa seurataan kriittisiä tietoja (esimerkiksi henkilötiedot), joiden vaarantuminen, häviäminen tai muuttuminen on oleellista?
- Kuka tarkastaa lokitiedot? Onko tällaisilla henkilöillä riittävä koulutus poikkeavan toiminnan tunnistamiseksi?
- Miten henkilöstö voi raportoida epäilyttävästä toiminnasta?
- Onko hälytyskynnykset määritelty oikealle tasolle? Ovatko ne riittävän matalia soveltuvan varoituksen antamiseksi mahdollisista poikkeamista? Tai riittävän korkeita, ettei niitä käsitteleviä henkilöitä kuormiteta merkityksettömillä tiedoilla?

Organisaatiossa tulee huomioida seuraavat asiat, kun pohditaan tietoturvaloukkauksien sisäistä tiedonjakoa:

- Mikä on tietoturvaloukkaus?
- Kenellä on valtuudet päättää, onko kyseessä tietoturvaloukkaus?
- Kenen on saatava tarkemmat tiedot tietoturvaloukkauksesta?
- Onko hallitus ilmoittanut selvästi kynnyksen, jolloin sille on tiedotettava tietoturvaloukkauksesta?

Onko hallituksella tiedossa, kuka johtaa toimintaa tietoturvaloukkauksissa ja kenellä on valtuudet tehdä päätöksiä?

Tämä riippuu organisaatiorakenteesta. Valtuudet voivat olla hallituksen jäsenellä, toimitusjohtajalla tai jollakulla johtajista tai ne on voitu jakaa eri tehtäville. Varmistakaa organisaatiossa mahdollisuuksien mukaan seuraavat asiat:

- Kuka voi tehdä päätöksiä mistäkin asiasta? Jos mahdollista, välttäkää ohjeissa vastuun henkilöimistä. Sen sijaan vastuu tulee antaa tehtävälle tai toiminnolle.
- Laatikaa varasuunnitelmat siltä varalta, että kyseiset päätöksentekijät eivät ole tavoitettavissa.
- Harjoitelkaa organisaatiossa päätöksentekomenettelyn toimivuutta.

Liite I

Keskeinen lainsäädäntö

Laki sähköisen viestinnän palveluista (917/2014)

Keskeisin sähköisen viestinnän säädös Suomessa on laki sähköisen viestinnän palveluista (917/2014). Laissa säädetään kattavasti mm. tietoturvaan ja luottamuksellisen viestinnän suojaan liittyvistä asioista. Sääntely koskee teleyrityksiä, viestinnän välittäjiä, yhteisötilaajia ja verkkotunnusvälittäjiä. Suurimmalle osalle suomalaisista organisaatioista tärkeitä ovat lain yhteisötilaajia koskevat säädökset. Yhteisötilaajalla tarkoitetaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja. Siten yhteisötilaaja voi olla esimerkiksi elinkeinonharjoittaja, osuuskunta, osakeyhtiö, yhdistys, oppilaitos tai valtion virasto. Yhteisötilaaja voi olla esimerkiksi yritys, joka hankkii ja tarjoaa puhelin- ja laajakaistaliittymät työntekijöilleen ja WLAN-yhteyden toimitiloissaan vieraileville henkilöille. Yhteisötilaajia koskevista toimivuudesta, tietoturvasta ja luottamuksellisen viestinnän suojasta huolehtimisen velvoitteista säädetään erityisesti lain osissa VI ja X.

EU:n verkko- ja tietoturvadirektiivi (ns. NIS-direktiivi)

EU:n verkko- ja tietoturvadirektiivillä pyritään varmistamaan korkeatasoinen verkko- ja tietojärjestelmien turvallisuus koko unionissa. Direktiivissä säädetään tietoturvavelvollisuuksista ja häiriöraportoinnista.

Sääntelyllä velvoitetaan keskeiset palveluntarjoajat sekä tietyt digitaalisten palvelujen tarjoajat kattavaan verkko- ja tietoturvallisuusriskienhallintaan, palveluiden jatkuvuuden hallintaan poikkeamatilanteissa sekä raportoimaan vastuuviranomaisille turvallisuuspoikkeamista, jotka haittaavat tai uhkaavat toiminnan jatkuvuutta.

Direktiivin velvoitteet kohdistuvat yhteiskunnan toimivuuden kannalta tärkeille toimialoille. Suomessa velvoitteet on saatettu voimaan sektorikohtaisessa lainsäädännössä, ja niiden noudattamista valvovat toimialakohtaiset viranomaiset.

- Liikenne - Traficom
- Energiahuolto - Energiavirasto
- Terveydenhuolto - Valvira
- Finanssiala - Finanssivalvonta
- Finanssialan infrastruktuuri - Finanssivalvonta
- Vesihuolto - ELY-keskukset
- Digitaalinen infrastruktuuri - Traficom
- Digitaaliset palvelut – Traficom

EU:n yleinen tietosuoja-asetus

Yleisessä tietosuoja-asetuksessa asetetaan yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevia vaatimuksia. Vaatimuksia sovelletaan sekä eurooppalaisiin organisaatioihin, jotka käsittelevät ihmisten henkilötietoja Euroopan unionissa, että Euroopan unionin ulkopuolisiin organisaatioihin, joiden suorittama tietojen käsittely kohdistuu EU:n alueella asuviin ihmisiin. Yleistä tietosuoja-asetusta sovelletaan, jos yritys käsittelee henkilötietoja ja sijaitsee EU:ssa. Näin tehdään riippumatta siitä, missä itse henkilötietojen käsittely tapahtuu tai jos yritys sijaitsee EU:n ulkopuolella, mutta käsittelee henkilötietoja, jotka liittyvät tavaroiden tai palvelujen tarjoamiseen henkilöille EU:ssa, tai yritys seuraa yksilöiden käyttäytymistä EU:ssa.

Tietosuojalaki (1050/2018)

Tietosuojalaki täsmentää ja täydentää Euroopan unionin yleistä tietosuoja-asetusta. Laki on henkilötietojen käsittelyyn sovellettava yleislaki. Yleistä tietosuoja-asetusta täydentävänä ja täsmentävänä se ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain tietosuoja-asetuksen kanssa.

Rikoslaki (39/1889)

Suomen rikoslaki ei tunne käsitettä kyberrikos, vaan kyberrikokset määritellään tyypillisesti tietotekniikka- tai tietoverkkorikoksiksi. Näistä on säädetty erityisesti rikoslain 38 luvussa. Lisäksi kyberrikoksiin liittyvistä rikoksista on säädetty myös muissa rikoslain luvuissa. Esimerkiksi yrityssalaisuuden rikkomisesta ja väärinkäytöstä säädetään erikseen elinkeinorikoksia käsittelevässä rikoslain 30 luvussa.

Liite II

Viranomaistoimijat Suomessa

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, jonka tehtävinä on:

- kerätä tietoa tietoturvaloukkauksista ja niiden uhkista
- tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta;
- selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia
- teleyritysten tietoturvallisuuden ja varautumisen valvonta ja ohjaus
- järjestelmien ja verkkojen tarkastus ja hyväksyntä
- sähköisen viestinnän yksityisyyden- suojaan liittyvien velvoitteiden valvominen

Yksityiset henkilöt, yritykset ja muut organisaatiot voivat ilmoittaa luottamuksellisesti Kyberturvallisuuskeskukselle niihin kohdistuneista tietoturvaloukkauksista, kuten haittaohjelmaepäilyistä, tietojen kalastelusta tai palvelunestohyökkäyksistä sekä näiden yrityksistä. Yhteydenottojen perusteella Kyberturvallisuuskeskus voi tarjota tarvittaessa tietoturvaloukkauksen selvittämiseksi ja tutkimiseksi apua sekä koordinoida tarvittavia toimenpiteitä.

Kyberturvallisuuskeskukselle voi ilmoittaa tietoturvaloukkauksista sähköpostitse cert@traficom.fi sekä internetsivustolla https://www.kyberturvallisuuskeskus.fi/fi "Ilmoita tietoturvaloukkauksesta" -painikkeesta.

Lisätietoa Kyberturvallisuuskeskuksesta https://www.kyberturvallisuuskeskus.fi/

Poliisi

Tietoverkkorikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa toimivaltaisena viranomaisena toimii poliisi. Tietoverkkorikoksista valtaosa tutkitaan paikallispoliisissa. Kaikissa poliisilaitoksissa toimii digitaalisen todistusaineiston käsittelyyn ja analysoimiseen erikoistuneita yksiköitä. Poliisin valtakunnallinen neuvontapalvelu toimii numerossa 0295 419 800 (arkisin 08-16.15) / neuvontapalvelu@poliisi.fi

Keskusrikospoliisi (KRP) on poliisin valtakunnallinen yksikkö, jonka toimialueena on koko Suomi. Keskusrikospoliisissa toimii tietoverkkorikosten esitutkintaan erikoistunut yksikkö, Poliisin kyberrikostorjuntakeskus, jossa tutkitaan pääasiallisesti tietoverkkoympäristöihin kohdennettuja laajoja, ennakkotapausluonteisia ja yhteiskunnallisesti merkittäviä tietoverkkorikoskokonaisuuksia.

Rikosilmoitus tulee tehdä sähköisellä rikosilmoituslomakkeella tai ilmoittamalla asiasta paikallispoliisille. Rikosilmoituksen voi tehdä verkossa osoitteissa https://www.poliisi.fi/rikokset/sahkoinen_rikosilmoitus tai käymällä paikallisella poliisiasemalla. Nettivinkki (https://www.poliisi.fi/nettivinkki) on ilmoituskanava, jonne voi tehdä ilmoituksen pienimmistäkin, ei rikoksen tunnusmerkistön täyttävistä, kyberhäiriöistä tai havainnosta.

Organisaatio vastaa itse havaitsemansa tietoturvatapahtuman ensivasteesta sekä rajoittamis- ja muista toimenpiteistä. Poliisin suorittamaa tutkintaa varten organisaation on syytä varmistaa todistusaineiston turvaaminen myöhempää mahdollista rikostutkintaa varten. Käytännössä tämä tarkoittaa kohteiden, tapahtumien, toimenpiteiden ja ajankohtien mahdollisimman tarkkaa dokumentointia. Järjestelmien ja tietoliikennelokien mahdollisimman laaja ja kattava talteenotto on ensisijaisen tärkeää. Lokitedot tulee ottaa talteen sekä säilyttää alkuperäisinä ja muuttumattomina.

Suojelupoliisi

Suojelupoliisi on turvallisuus- ja tiedustelupalvelu, joka tiedustelee ja estää ennalta kansalliseen turvallisuuteen kohdistuvia uhkia. Lisäksi se tuottaa valtiojohdolle ja muille viranomaisille päätöksentekoa tukevaa turvallisuustietoa.

Suojelupoliisin yhtenä tehtävänä on paljastaa ja torjua ulkovaltojen Suomeen kohdistuvaa vakoilua tietoverkoissa ja estää ennalta sitä aiheutuvia vahinkoja. Kybervakoilu kohdistuu valtionhallinnon ohella myös yrityksiin. Kybervakoilun torjunnassa Suojelupoliisi tekee yhteistyötä sekä kansallisten että kansainvälisten kumppaneiden kanssa. Yhteistyötä tehdään viranomaisten ohella myös elinkeinoelämän kanssa.

Suojelupoliisin pyrkii ennaltaehkäisemään kybervakoilua tietoisuutta lisäävällä sidosryhmäyhteistyöllä, muun muassa kouluttamalla kriittistä infrastruktuuria ylläpitäviä sekä huoltovarmuuteen liittyviä yrityksiä.

Suojelupoliisin vaihteen numero on 0295 48013 ja sähköpostiosoite suojelupoliisi@supo.fi.

Tietosuojavaltuutetun toimisto

Tietosuojavaltuutettu on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Tietosuojavaltuutetun tehtävinä on mm. valvoa tietosuojalainsäädännön ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista, edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista, velvollisuuksista ja oikeuksista, tehdä selvityksiä ja tarkastuksia sekä määrätä hallinnollisia seuraamuksia tietosuoja-asetuksen rikkomisesta.

Tietosuojavaltuutetulle voi tehdä ilmoituksen henkilötietojen tietoturvaloukkauksesta osoitteessa https://tietosuoja.fi/ilmoitus-tietoturvaloukkauksesta

Huoltovarmuuskeskus ja poolit

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Tehtävinään Huoltovarmuuskeskus sovittaa yhteen elinkeinoelämän ja julkishallinnon yhteistyötä varautumisessa, hoitaa valtion varmuusvarastointia sekä turva- ja velvoitevarastointia, varmistaa välttämättömien teknisten järjestelmien toimivuutta ja turvaa kriittistä tavara- ja palvelutuotantoa sekä seuraa kansainvälistä kehitystä ja pitää yhteyttä ulkomaisiin viranomaisiin ja laitoksiin.

Poolit vastaavat operatiivisesta varautumisesta elinkeinoelämän johdolla toimivina toimieliminä. Niiden tehtävänä on yhdessä alan yritysten kanssa seurata, selvittää, suunnitella ja valmistella toimenpiteitä omien alojensa huoltovarmuuden kehittämiseksi. Digipooli on tietotekniikka-ja tietoverkkoalan sekä viranomaisten välinen yhteyselin, jonka toiminnassa ovat mukana kyseisten alojen yritykset ja eri viranomaisia. Pooliin kuuluvat merkittävät tietotekniikkapalveluiden tuottajat, ohjelmisto- ja laitetoimittajat, tietoturva-alan yrityksiä sekä teleyritykset. Viranomaisista tärkeimmät ovat valtiovarainministeriö, Traficom, Pääesikunta ja Huoltovarmuuskeskus.

Lisätietoa kyberturvallisuudesta saat ottamalla meihin yhteyttä:
cert@traficom.fi

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus