TIETOTURVAOPAS YRITYKSILLE

ICC Cyber security guide for business

ICC FINLAND
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

KESKUS-
KAUPPAKAMARI

TIETOTURVAOPAS YRITYKSILLE

ICC Cyber security guide for business

Kiitokset

Kansainvälisen kauppakamarin (*International Chamber of Commerce*, ICC) Yrityksen kyberturvallisuusopas perustuu belgialaiseen kyberturvallisuusoppaaseen, joka on laadittu ICC:n Belgian osaston ja Belgian yrittäjäjärjestö VBO-FEB:n sekä EY Belgiumin ja Microsoft Belgiumin aloitteesta yhteistyössä Belgian kyberrikollisuuden osaamiskeskuksen B-CCENTRE:n ja ISACA Belgiumin kanssa. Belgiassa arvostettua opasta tarjottiin ICC:n digitaalitalouden asiantuntijaryhmälle (*Digital Economy Commission*) malliksi, josta voitaisiin muokata kansainvälinen versio oppaan laadintaan osallistuneiden yritysten ja yhteisöjen luvalla.

ICC kiittää belgialaisen oppaan laatijoita sekä kansainvälisen oppaan laatimiseen osallistuneita ICC:n kyberturvallisuustyöryhmän (*ICC Task Force on Cyber Security*) jäseniä heidän panoksestaan.

ISBN: ICC Cyber security guide for business ICC Publication No. 450/1081-5 | 978-92-842-0336-9
ISBN: TIETOTURVAOPAS YRITYKSILLE | 978-952-5620-84-9

SISÄLLYSLUETTELO

SAATESANAT

Kauppakamarien tehtävänä on edistää yritysten toimintaedellytyksiä ja kasvua. Keskuskauppakamari ja 19 alueellista kauppakamaria kattavat koko Suomen, kaikki toimialat ja kaikki yritysmuodot.

Keskuskauppakamari tarjoaa tämän Kansainvälisen kauppakamarin (International Chamber of Commerce, ICC) tuottaman Tietoturvaoppaan yrityksille kaikkien suomalaisten toimijoiden käyttöön. Opas on suunnattu yritysten omistajille, henkilöstölle ja johtajille - ei ainoastaan IT-tiimeille - ja sitä voi jakaa myös yritysten toimitusketjun kumppaneille.

Digitaalitalous yhdistää suomalaiset yritykset maailmanlaajuisiin verkostoihin, mutta samalla se altistaa yritykset missä päin maailmaa tahansa tehtäville tietoturvarikkomuksille.

Riskit ovat suuret. Siksi jokaisen yrityksen on syytä varmistaa, että sen tietoturva-ajattelu ja toiminta ovat ajan tasalla.

Risto E. J. Penttilä
toimitusjohtaja
Keskuskauppakamari

Avoin ja toimiva kansainvälinen liiketoiminta - perinteinen tai digitaalinen - tarvitsee moderneja pelisääntöjä. Niillä voidaan ennaltaehkäistä väärinkäytöksiä ja ohjata kauppatapoja.

Yrityselämän aidosti kansainvälinen, kaikki toimialat kattava yhteistyöjärjestö Kansainvälinen kauppakamari (International Chamber of Commerce, ICC) haluaa edistää kansainvälistä kauppaa ja vahvistaa luottamusta digitaalisuuteen sekä lisätä sen tarjoamia mahdollisuuksia yrityksille, kuluttajille, hallituksille ja koko yhteiskunnille.

Yritysten kansainvälisessä yhteistyössä syntynyt Tietoturvaopas tarjoaa selkeän ja yksinkertaisen mallin kaikenkokoisille yrityksille tietoturvahaasteiden ratkaisemiseksi. Digitaalisuus ei vain mullista markkinoita, vaan myös muuttaa yhteiskuntaa sekä haastaa perinteisiä toimintatapoja sekä niiden sääntelyä. Kaikkien yritysten on otettava asia vakavasti. Opas on mainio apu yrityksissä tietoturvan kartoittamisessa ja suunnittelussa.

Opasta jaetaan ICC:n yli 130 maata kattavassa kansainvälisessä verkostossa. Uskomme, että yrityselämän verkostojen yhteiset toimet voivat osaltaan vähentää niin yritysten kuin koko yhteiskunnan kohtaamia tietoturvariskejä. ICC ja Keskuskauppakamari haluavat tarjota oppaan nyt myös suomalaisten yritysten käyttöön.

Timo Vuori
maajohtaja
Kansainvälinen kauppakamari ICC

TURVALLISUUS LÄHTEE ITSESTÄ

Moderni tieto- ja viestintäteknologia tarjoaa kaikenkokoisille yrityksille mahdollisuuden innovoida, tavoittaa uusia markkinoita ja tuottaa entistä tehokkaampia ratkaisuja, jotka hyödyttävät niin asiakkaita kuin koko yhteiskuntaakin. Samalla kuitenkin tarve sopeutua kaikkialle ulottuvien tuotteiden ja palvelujen toimittamiseen tarvittavien viestintäympäristöjen ja tietovirtojen suoriin ja epäsuoriin vaikutuksiin on kasvava haaste yritysten käytännöille ja toimintatavoille. Monissa yrityksissä otetaan käyttöön modernia tieto- ja viestintätekniikkaa ymmärtämättä täysin, että se edellyttää myös uudenlaisten riskien hallintaa. Tässä oppaassa käsitellään näitä haasteita ja hahmotellaan, miten kaikenkokoiset yritykset voivat tunnistaa ja hallita tietoturvallisuusriskejä.

Tietoturvan pettämistä käsitellään jatkuvasti mediassa. Esille tuodaan tilanteita joissa vihamieliset toimijat ovat murtaneet niin suurten kuin pientenkin yritysten tietoturva-suojaukset – ilmeisen vaivatta ja saavuttaen omat tavoitteensa. Nykyään yritykset altistuvat yhä suuremmille riskeille[1] sitä mukaa kuin rikolliset, hakkerit, valtiolliset toimijat ja kilpailijat kehittävät yhä kekseliäämpiä keinoja hyödyntää modernin tieto- ja viestintätekniikan heikkouksia. Yritysten tietojärjestelmien yhdistäminen erilaisiin ulkoisiin laitteisiin[2] lisää järjestelmien monimutkaisuutta ja niihin kohdistuvia uhkia.

Ulkoisten uhkien lisäksi yritysten on myös pystyttävä hallitsemaan tietoverkkoihin kohdistuvia sisäisiä uhkia, joissa organisaatiossa toimivat henkilöt pystyvät turmelemaan tietoja tai käyttämään yrityksen resursseja hyväkseen kätevästi omasta kodistaan tai vaikka paikallisesta kahvilasta käsin. Liiketoiminnan kannalta on elintärkeää, että yritys – olipa se sitten suuri tai pieni – kykenee tunnistamaan omat tietoturvariskinsä ja hallitsemaan tehokkaasti tietojärjestelmiinsä kohdistuvia uhkia. Samanaikaisesti koko yritysjohdon, johtoryhmää ja hallitusta myöten, on tiedostettava, että tietoturvariskien hallinta on jatkuva prosessi, jossa ei koskaan saavuteta täydellistä turvaa.

Toisin kuin monet muut liiketoiminnan haasteet, tietoturvan riskienhallinta on edelleen ongelma, johon ei ole helppoa ratkaisua. Se vaatii johdolta jatkuvaa huomiota, kykyä sietää huonoja uutisia sekä järjestelmällistä ja selkeää viestintää. Vaikka keskeisiä tietoturvauhkia on selvitetty kattavasti lukuisissa erinomaisissa lähteissä, yritysjohdon tueksi soveltuvaa tietoturvan hallinnan aineistoa on edelleenkin saatavilla vähänlaisesti. **Tämä julkaisu auttaa** niin pienten kuin suurtenkin organisaatioiden **johtoa toimimaan vuorovaikutuksessa tietohallintopäälliköiden kanssa** ja **ohjaamaan tietoturvariskien hallintaan liittyvien käytäntöjen kehittämistä**.

1 Esimerkkejä kasvavista ulkoisista tietoturvauhista ovat haittaohjelmistot (kuten tunkeutumisohjelmistot (*intrusion software)*, haitallisen koodin lisääminen (*code injection*), haittaohjelmien jakelualustat eli exploit kit -sivustot, madot ja troijalaiset), palvelunestohyökkäykset, tietomurrot ja muut. Katso esimerkiksi ENISA:n tilannekatsaus *ENISA Threat Landscape 2014, EL 2014* osoitteessa https://www.enisa.europa.eu

2 Esim. matkapuhelimet, modeemit, maksupäätteet, automaattiset ohjelmistopäivitykset, teollisuuden ohjausjärjestelmät, myyjän ja asiakkaan väliset vuorovaikutusratkaisut sekä esineiden internet.

LUE TÄMÄ ENSIN

Organisaation tietoturvallisuutta voidaan parantaa riskienhallintaprosessilla, jossa painotetaan nimenomaisesti hallintaa. Jatkuvasti muuttuva tekniikka sekä uhkien moninaiset leviämisreitit ovat syy miksi yritysten tietojärjestelmät eivät ole koskaan valmiita tai täysin turvallisia. Tehokas toiminta muuttuvassa ympäristössä edellyttää sitoutumista pitkäjänteiseen päättymättömään riskienhallintaan. Yritysjohtajat saattavat turhautua tietoturvahankkeisiin, jos he eivät lähesty tehtävää oikein odotuksin. Ilman asianmukaista suunnitelmaa yritykset taas saattavat käyttää liikaa resursseja tietoturvariskien hallintaan. Siksi onkin välttämätöntä luoda sellainen tietoturvallisuusriskien hallintaprosessi, joka auttaa ymmärtämään ja priorisoimaan organisaation fyysisen ja tieto-omaisuuden kannalta tärkeät seikat.

On ratkaisevan tärkeää olla tietoinen, että **internet, yritystietoverkot ja laitteet eivät ole turvallisia ilman asianmukaisia varotoimia**. Nykyaikaiset yritystietojärjestelmät ovat monenlaisten vihamielisten toimijoiden kohteena. Tietoturvariskien hallintaan osallistuville voidaan odotusarvoksi asettaa yksinkertainen sanonta: "Jos verkossa on jotain arvokasta, se on uhattuna ja todennäköisesti jo vaarantunut." Onneksi yrityksen arvokkaana pitämä omaisuus (kuten raha, liikesalaisuudet ja asiakastiedot) ei välttämättä ole aina arvokasta yksittäiselle vihamieliselle toimijalle. Vaikka tietojen vaarantumisen riskiä voidaan vähentää erilaisilla tekniikoilla ja prosesseilla, määrätietoinen vihamielinen toimija voi hyödyntää toisiinsa liitettyjen järjestelmien heikointa lenkkiä. Yrityksessä voi olla lukuisia organisaatioon, ihmisiin ja tekniikkaan liittyviä haavoittuvuuksia. Teknologiatoimittajien, palveluntarjoajien ja oman henkilöstön hyvästä työstä huolimatta täydellistä turvallisuutta ei voida saavuttaa. Kyberturvallisuusriskien hallintaprosesseissa onkin arvioitava juuri oman yrityksen heikkouksia ja siihen kohdistuvia uhkia ja suhteutettava ne organisaation tärkeimpiin omaisuuksiin.

Edellä maalaillusta synkästä näkymästä huolimatta kaikenkokoiset yritykset voivat pyrkiä hallitsemaan kyberturvallisuusriskejä kehittämällä ja ylläpitämällä riskienhallinnan keskeisiä elementtejä omassa organisaatiossaan.

- Ensinnäkin yritysjohdon on toteutettava organisaation riskianalyysi ja priorisoitava ensisijaisesti suojattavat kohteet.
- Toiseksi johdon tulee ryhtyä tarvittaviin toimiin varmistaakseen, että yrityksessä noudatetaan parhaita tietoturvakäytäntöjä.
- Kolmanneksi organisaation on varauduttava havaitsemaan häiriöt tietoturvassa ja vastaamaan niihin – sekä sisäisesti että ulkoisesti – koko organisaatioon vakiinnutetuilla prosesseilla.

Vastatoimet edellyttävät entistä parempaa viestintää vertaisryhmien, asiaankuuluvien viranomaisten, asiakkaiden ja jopa kilpailijoiden kesken. Varautumalla kaikenlaisiin tietoturvahäiriöihin voidaan varmistaa, että ongelmatilannetta ei pahenneta entisestään niitä ratkaistaessa tekemällä estettävissä olevia virheitä. Loppujen lopuksi tietoturvariskien hallinnan parhaiden käytäntöjen jalkauttaminen koko yritykseen edellyttää institutionaalista muutosta, jonka aikaansaamiseksi tarvitaan järjestelmällisiä keinoja ottaa oppia verkkohyökkäyksistä ja mukauttaa käytäntöjä.

OPPAAN KÄYTTÖ

Viimeisen vuosikymmenen aikana viranomaiset, järjestöt ja yksilöt ovat laatineet lukuisia julkaisuja, joissa käsitellään kyberympäristön tietoturvahaasteisiin vastaamista. Erilaisia asiakirjoja ja suosituksia on niin paljon, että voi olla vaikeaa selvittää, mistä niihin perehtyminen pitäisi aloittaa ja mikä niistä soveltuu omalle organisaatiolle. Saatavilla olevien aineistojen kirjo on laaja (lueteltu yleisestä yksityiskohtaiseen):

- **Suositukset** – Korkean tason visioita, joissa kartoitetaan tietoturvan huolenaiheita, ja jotka tarjoavat suuntaviivat organisaatioille ja yksilöille. Esimerkkejä: *OECD Security Guidelines* (OECD:n turvallisuuden perusperiaatteet) jne.

- **Kansalliset strategiat** – Usein suosituksiin perustuvia asiakirjoja, joissa esitetään tiettyyn kansalliseen tai lainsäädäntöympäristöön räätälöity tapa käsitellä kyberturvallisuutta. Esimerkkejä: *International Strategy to Secure Cyberspace* (Kansainvälinen kyberympäristön turvaamisen strategia)[3], Euroopan ja muiden maiden kansalliset strategiat jne.

- **Viitekehykset** – Kansallisista strategioista johdetut viitekehykset kokoavat yhteen priorisoituja tai arvioituja aineistoja, joiden avulla organisaatiot voivat vertailla kehitystasoaan ja edistymistään tietoturvariskien käsittelyssä. Esimerkkejä: *National Institute of Standards and Technology (NIST) Cybersecurity Framework* (Yhdysvaltain standardisointiviraston Kyberturvallisuuden viitekehys)[5] jne.

- **Standardit** – Organisaation prosesseja ohjaavia tai sääteleviä vaatimuksia, joilla varmistetaan tietoturvan parhaiden käytäntöjen määrätietoinen ja johdonmukainen noudattaminen. Esimerkkejä: ISO 27001, 27002 ja 27032 -prosessistandardit, kansainväliset maksukorttialan tietoturvastandardit (PCI-standardit) jne.

- **Tekniset standardit** – Tiettyjen yhteentoimivuusvaatimusten mukaisten rajapintojen toteutuksen yksityiskohtaiset tekniset määrittelyt. Esimerkkejä: HTTPS, AES, EMV-sirukorttistandardi, PCI-standardit jne.

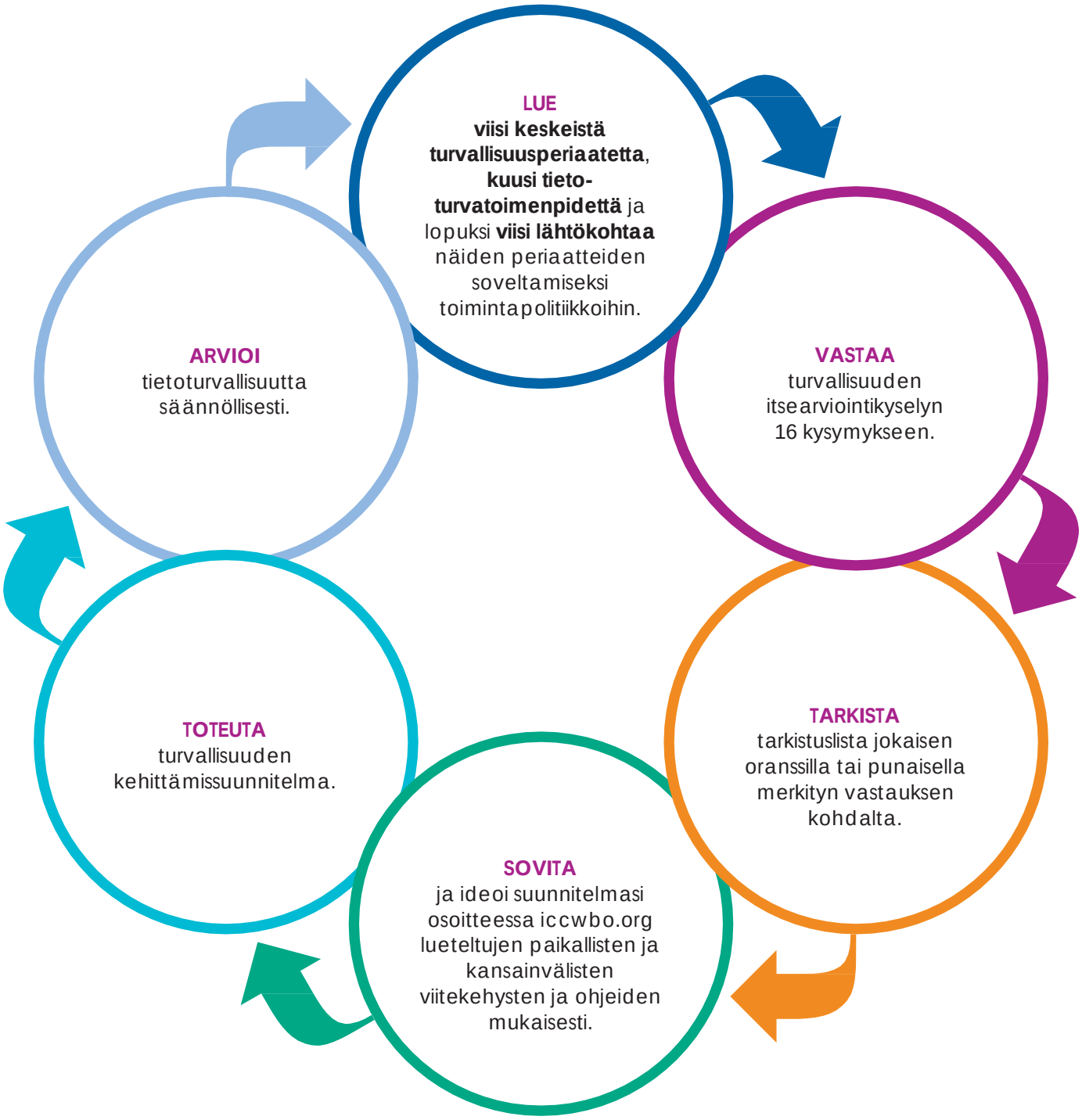
Tämä kansainvälisiin tietoturvasuosituksiin ja kansallisiin strategioihin perustuva perusopas tarjoaa yrityksille viitekehyksen jonka avulla pohtia verkkoympäristöjen turvallisuutta. Oppaassa esitellään aluksi kaikenkokoisille yrityksille soveltuvat tietoturvariskien käsittelyn **viisi periaatetta**. Seuraavaksi oppaassa luetellaan eri lähteiden ja parhaiden käytäntöjen pohjalta muodostetut **kuusi keskeistä tietoturvatoimenpidettä**, jotka yritysten pitäisi ehdottomasti toteuttaa. Tämän jälkeen käsitellään näiden **viiden periaatteen soveltamista toimintapolitiikkoihin** organisaatioiden tietoturvariskien hallinnan kehittämiseksi. Julkaisua täydentää jatkuvasti päivitettävä sähköinen liite, joka toimii ajantasaisena tausta-aineistona ja tarjoaa tarkempia ohjeita sitä mukaa kun niitä kehitetään – aina menettelyohjeista teknisiin standardeihin yms. Vaikka täydellistä turvaa ei voidakaan saavuttaa, tässä hahmotellut tietoturvariskien hallintaan liittyvät konseptit auttavat yrityksiä vastaamaan tietoturvan haasteisiin alati muuttuvassa toimintaympäristössä. Opas on hyödyllinen yksittäisille yrityksille, mutta sen ohjeita voi myös jakaa sidosryhmien kanssa omien järjestelmien ja toimintojen tiedonkulun ja -vaihdon turvaamiseksi.

3 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

4 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

5 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

OPPAAN KÄYTTÖ



Vaikka yritysten tietoturvaratkaisut voivat vaihdella useista tekijöistä[6] johtuen, järkevät tietoturvakäytännöt perustuvat muutamiin yleisluonteisiin periaatteisiin, jotka soveltuvat kaikille yrityksille koosta tai toimialasta riippumatta. Tässä oppaassa esitellään **viisi keskeistä periaatetta**, jotka jakautuvat kahteen luokkaan:

A. visio ja ajattelutapa

B. organisaatio ja prosessit.

Näitä viittä periaatetta täydentää kuusi keskeistä **tietoturvatoimea** ja **viisi lähtökohtaa näiden periaatteiden soveltamiseksi** yrityksen tietoturvapolitiikan tukena.

Yhdessä tässä esitetyt periaatteet ja toimet parantavat yrityksen varautumistasoa tietoturvauhkiin liittyen ja rajoittavat tietoturvaloukkauksiin liittyviä häiriöitä.

A. VISIO JA AJATTELUTAPA

Ensimmäinen periaate: Keskity tietoon, älä tekniikkaan

Yritysjohto toimii organisaatioon kohdistuvien tietoturvauhkien torjunnan etulinjassa ja vaikuttaa osaltaan siihen, miten organisaatiossa suhtaudutaan tietoturva-asioihin. Tietoturvallisuutta tuleekin ajatella sen laajimmassa merkityksessä eikä vain tietotekniikan näkökulmasta.

Tietoturvallisuudessa on kyse koko yritystä koskevasta ihmisten, prosessien ja tekniikan muodostamasta kokonaisuudesta, eikä se siis ole vain IT- eli tietotekniikkakysymys. Tietoturvatoimien toteutus ei saisi jäädä pelkästään IT-osaston vastuulle, vaan sen tulisi heijastua koko yrityksen toimintaan. Tietoturvallisuuden ulottuvuus ja visio koskee siis ihmisiä, tuotteita, tuotantolaitoksia, prosesseja, toimintapolitiikkoja, menettelytapoja, järjestelmiä, teknisiä ratkaisuja, laitteita, verkostoja ja tietoja.

Ihmiset ovat avainasemassa. Tieto-omaisuuteen kohdistuvien uhkien ja haavoittuvuuksien tunnistaminen ja hallinta voi olla valtava urakka. Kokemus kuitenkin osoittaa[7], että 35 prosenttia turvallisuushäiriöistä johtuu inhimillisestä virheestä eikä tahallisesta hyökkäyksestä. Lopuista turvallisuushäiriöistä yli puolet johtuu tahallisesta hyökkäyksestä, **joka olisi voitu välttää**, jos tietoa olisi käsitelty turvallisemmin.

Tietoturvatoimet tulee kohdistaa arvokkaimpien tietojen ja järjestelmien suojaamiseen, joiden luottamuksellisuuden, eheyden tai käytettävyyden vaarantuminen aiheuttaisi yritykselle vakavaa haittaa. Tämä ei tarkoita sitä, että muun tieto-omaisuuden turvallisuuteen ei tarvitsisi kiinnittää huomiota. Kyse on siitä, että organisaation ”kruununjalokiviin” keskittyvä riskiperusteinen tapa käsitellä tietoturvallisuutta on tehokas ja toimiva käytäntö. Samalla tunnustetaan, että riskien sataprosenttinen poistaminen ei ole kustannuksiin nähden sen enempää mahdollista kuin tarpeellistakaan.

6 Näihin lukeutuvat monien muiden muassa liiketoiminnan luonne, riskitaso, ympäristötekijät, verkottuneisuus, sääntelyvaatimukset sekä yrityksen koko.

7 EY – 2012 Global Information Security Survey – Fighting to close the gap

Toinen periaate: Tee varautumisesta ajattelutapa

Yrityksen tavoitteena tulee olla varautuminen tietojen menetykseen tai vaurioitumiseen. Yrityksiä säännellään lukuisilla laeilla ja määräyksillä, joista useissa vaaditaan asianmukaisten valvontatoimien toteuttamista. Lakien, määräysten ja normien noudattaminen voi parantaa tietoturvallisuutta, mutta se voi myös johtaa herpaantumiseen, kun vaaditut tavoitteet on kerran saavutettu. Turvallisuusuhat muuttuvat paljon nopeammin kuin lait ja sääntely, joten riskienhallinnan tavoitteetkin muuttuvat jatkuvasti. Niinpä yrityksen toimintatavat ja menettelyt voivat olla vanhentuneita tai käytännössä yksinkertaisesti tehottomia.

Yrityksen varautumiskykyä tietoturvauhkiin ja -haavoittuvuuksiin on arvioitava aika ajoin, jotta riskienhallinnan tavoitteiden saavuttamista ja tietoturva toimien riittävyyttä voidaan mitata. Arviointi voidaan toteuttaa sisäisillä ja/tai riippumattomilla ulkoisilla arvioinneilla ja auditoinneilla, joihin sisältyy mm. murtotestaus (penetration test) ja tunkeutumisen havaitseminen.

Vastuun tietoturvasta on ulotuttava myös IT-osaston ulkopuolelle, ja päätöksistä vastaavien sidosryhmien tulee osallistua ongelmien tunnistamisen lisäksi myös pitkäjänteiseen toimivan kokonaisuuden toteuttamiseen. Yrityksen ajoittaisen arvioinnin todellinen arvo konkretisoituu silloin, kun prosessia hyödynnetään tietoturvariskien hallintaan liittyvän yrityskulttuurin ja henkilöstön ajattelutavan kehittämisessä.

Tietojärjestelmien häiriönsietokykyyn perustuva ajattelutapa on erityisen tärkeä silloin, kun yrityksessä otetaan käyttöön uusia ratkaisuja ja laitteita. Tällöin on otettava huomioon asianmukaiset turvatoimet mahdollisimman varhaisessa käyttöönoton vaiheessa, mieluimmin jo yritystoiminnan vaatimuksia määriteltäessä. Tällainen ”sisäänrakennettu tietoturvallisuus” voi kannustaa yrityksen innovatiivisia työntekijöitä keskittymään tietoturvariskien hallintaan.

B. ORGANISAATIO JA PROSESSIT

Kolmas periaate: Ole valmis vastatoimiin

Kaikkein suojautuneinkin yritys joutuu ennen pitkää tietoturvaloukkauksen kohteeksi. Elämme ympäristössä, jossa kyse on siitä, **milloin** eikä **jos** näin sattuu. Niinpä **yritysjohtoa** arvioidaankin sen mukaan, miten yritys **vastaa** tietoturvaloukkaukseen.

Minimoidakseen tietoturvahäiriöiden vaikutukset toimintaansa yritysten on kehitettävä teknisten vastatoimien lisäksi myös organisaation varautumissuunnitelma. Suunnitelmassa tulee määrittää tunnusmerkit, jotka osoittavat yritysjohdolle, milloin turvallisuushäiriön hillitseminen ja korjaaminen edellyttää ulkopuolisia asiantuntijoita ja milloin on syytä ottaa yhteyttä muihin ulkopuolisiin tahoihin, kuten lainvalvontaviranomaisiin tai valtion valvontaelimiin. On syytä muistaa, että asianmukaisille viranomaisille ilmoittaminen parantaa osaltaan yleistä turvallisuustilannetta ja voi joissain tapauksissa olla määräysten mukaan pakollista. Toimiva tietoturvatapahtumien hallintasuunnitelma sisältää myös sisäisen ja ulkoisen viestintäsuunnitelman, joka voi vaikuttaa siihen, päätyykö tapaus noloksi otsikoksi sanomalehden etusivulle vai onnistuneeksi esimerkkitapaukseksi yliopiston opintoohjelmaan.

Vaikka sisäinen riskienhallinta on keskeistä, samalla on myös muistettava varata aikaa yhteyksien luomiseen omalla toimialalla toimiviin vertaisryhmiin ja kumppaneihin sekä laajemminkin yritysmaailmaan ja lainvalvontaviranomaisiin. Laaja verkosto auttaa pysymään ajan tasalla nykyisistä ja uusista uhista sekä samalla voidaan myös rakentaa suhteita, joihin tukeutua häiriön aikana.

Neljäs periaate: Osoita johdon sitoutuneisuus

Tietoturvallisuuden toimiva ja tehokas hallinta edellyttää sitä, että yritysjohto ymmärtää ja tukee riskienhallintaa organisaation keskeisenä menestystekijänä. **Yritysjohdon** pitää osallistua näkyvästi yrityksen tietoriskien hallintaan ja valvontaan. Johdon on varmistettava, että yrityksen omaisuuden suojaamiseen on kohdistettu riittävästi niin inhimillisiä kuin taloudellisiakin resursseja. Resurssit eivät kuitenkaan yksinään riitä, vaan sekä suurten että pienten yritysten tulee valtuuttaa tietoturvaorganisaationsa vastaamaan tietoturvauhkiin ja -haavoittuvuuksiin kaikkialla organisaatiossa.

Yrityksen tietoturvatoimien vaikuttavuudesta ja riittävyydestä tulee raportoida asianmukaisesti yrityksen ylimmälle johtajalle ja vähintään kerran vuodessa johtoryhmälle, tilintarkastajille ja hallitukselle. Näiden erilaisiin turvallisuus-indikaattoreihin ja -mittareihin perustuvien raporttien tulisi osaltaan vaikuttaa tietoturva-käytäntöjä ja -investointeja koskeviin päätöksiin sekä antaa käsitys siitä, kuinka hyvin yritys on suojannut omaisuutensa.

Vaikka henkilöstöä kutsutaan usein tietoturvan *heikoimmaksi lenkiksi*, työntekijöistä voi saada tieto*turvallisuuden parhaan takeen* kartuttamalla heidän tietojaan ja taitojaan tietoturva-asioissa.

Viides periaate: Toteuta visiosi

Pelkästään tämän oppaan lukeminen ei riitä – johdon on vietävä yrityksen tietoturvariskienhallinnan visio käytäntöön luomalla (tai muokkaamalla) erilaisia toimintatapoja tietoturvan varmistamiseksi. Yrityksen tietoturvaa koskevat käytännöt määrittävät peruslähtötason, jonka pohjalta yrityksen turvatoimia ohjataan kaikissa yksiköissä ja henkilöstöryhmissä. Lisäksi ne kasvattavat tietoturvatietoisuutta koko organisaatiossa.

Tietoturvallisuuteen liittyvät toimintatavat ja niitä tukevat suositukset ja standardit kootaan yleensä tietoturvapolitiikaksi, jonka pohjalta määritetään operatiiviset toimintatavat.

Kun ulkopuolisia palveluntarjoajia otetaan ja integroidaan entistä enemmän mukaan yritysten arvoketjuihin, organisaatioiden on ymmärrettävä omien tietojensa kulku erilaisten ulkoisten tahojen keskuudessa ja niihin liittyvät riippuvuussuhteet. Jos ulkopuolinen osapuoli ei suojaa riittävästi yrityksen tietoja (tai omia tieto-järjestelmiään, joiden varassa yritys toimii), **heihin** kohdistuvasta turvallisuushäiriöstä voi muodostua vakava rasite **oman** yrityksen toiminnalle, maineelle ja brändin arvolle.

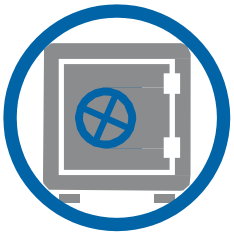
Toimittajia kannattaa kehottaa ottamaan käyttöönsä vähintäänkin yrityksen omat tietoturva-periaatteet, ja tarvittaessa on syytä suorittaa auditointeja tai pyytää palveluntarjoajilta selvitys niiden omista tietoturvakäytännöistä toimintatapojen varmistamiseksi.

Ulkopuoliset tahot eivät ole ainoastaan riski-tekijöitä, vaan jotkin niistä voivat myös osaltaan vähentää riskejä ja auttaa yritystä saavuttamaan tärkeitä tietoturvariskienhallinnan tavoitteita. IT-palveluntarjoajat voivat auttaa parantamaan yrityksen tietoturvariskienhallinnan infrastruktuuria esimerkiksi tarjoamalla turvallisuusarviointeja ja -auditointeja sekä tietoturvalaitteita, -ratkaisuja tai -palveluita, hallinnoidaan niitä sitten talon sisällä tai ulkopuolelta tai pilvestä[8] käsin.

8 Pilvipalvelut ovat ratkaisuja, joissa yritys käyttää ulkopuolisen palveluntarjoajan palveluja tiedon tallentamiseen, käsittelyyn tai hallintaan internetin kaltaisessa verkossa ja jotka ovat erittäin joustavia ja mahdollistavat reaaliaikaisen seurannan.

Tässä luettelossa on joukko käytännön toimenpiteitä, joita voidaan toteuttaa kaikenkokoisissa yrityksissä tietoturvahäiriöihin liittyvien riskien vähentämiseksi. Luettelo ei ole kattava tai tyhjentävä, mutta ryhtyminen siinä lueteltuihin toimenpiteisiin vie yritystä oikeaan suuntaan kohti erinomaista tietoturvallisuutta.

On syytä muistaa, että tietoturvariskien hallinta on jatkuva prosessi. Kun yrityksesi on saanut nämä ensimmäiset aktiviteetit tyydyttävästi liikkeelle, on suositeltavaa tutustua tähän oppaaseen liittyvään internet-portaaliin ja selvittää, mitkä standardit ja aineistot auttavat yritystäsi kehittämään tietoturvallisuutta vieläkin paremmalle tasolle.



Turvatoimenpide 1: Varmuuskopioi yrityksen tiedot ja varmista palautusprosessi

Varmista yrityksen tietojen suojaaminen tekemällä niistä varmuuskopiot jo ennen kuin yritys joutuu tietoturvaloukkauksen kohteeksi, jolloin tietoja voidaan varastaa, muuttaa, poistaa tai kadottaa. Varmuuskopiointi ei kuitenkaan yksin riitä[9]. Toimiva varmistusprosessi sisältää myös varmistustiedostojen tarkistamisen sekä palautusprosessien testaamisen. Jos tietojen säilyttämiseen käytetään ulkopuolisia tahoja (esim. pilvipalveluja), myös näiden tietojen varmuuskopiointi tulee varmistaa.

Lisäksi on syytä muistaa, että myös varmuustiedostojen tallentamiseen käytetyt fyysiset tallennusvälineet, kuten levyt, nauhat tai asemat, ovat alttiina riskeille. Koska varmuuskopiointivälineitä on helppo kuljettaa, niiden suojauksen pitää olla samalla tasolla lähdetietojen kanssa etenkin fyysisen turvallisuuden osalta.

Turvatoimenpide 2: Päivitä tietotekniset järjestelmät

Kaikenlaiset järjestelmät ja ohjelmistot sekä verkkolaitteistot ja laitteet tulee päivittää sitä mukaa kun korjauksia ja laiteohjelmistopäivityksiä on saatavilla. Ne korjaavat järjestelmien haavoittuvuuksia, joita hyökkääjät saattavat hyödyntää. Monet onnistuneet tietoturvaloukkaukset ovat johtuneet sellaisista järjestelmien haavoittuvuuksista, joihin olisi ollut saatavilla päivityksiä, usein jopa vuotta ennen häiriötilannetta.

9 Varmuuskopiointi on tekninen prosessi, jota on hallinnoitava huolella. Esimerkiksi ainoastaan useiden samanaikaisesti verkkoon yhdistettyjen tietovarastojen käyttö samassa toimipaikassa ei ole riittävä varmistusmenettely. Toimivassa varmistuspolitiikassa on otettava huomioon muiden seikkojen lisäksi monenlaisia riskejä, kuten tietojen ja toimipaikan menetys, mikä edellyttää tavallisesti sitä, että varmuuskopiot sijaitsevat fyysisesti toimipaikan ulkopuolella.

Automaattisia päivityspalveluja kannattaa käyttää mahdollisuuksien mukaan etenkin tietoturvajärjestelmissä, kuten haittaohjelmien torjuntasovelluksissa, sisällönsuodatusohjelmissa ja tunkeutumisenhavaitsemisjärjestelmissä.

Automaattisilla päivitysprosesseilla voidaan osaltaan varmistaa, että käyttäjät asentavat aidot päivitykset suoraan tietoturvaohjelmistojen alkuperäisiltä valmistajilta.

Turvatoimenpide 3: Panosta koulutukseen

Koko yrityksen henkilöstölle on tarpeen antaa perustason tiedot keskeisistä tietoturvauhista ja tietoturva-aiheista ja kerrata niitä jatkuvasti. Koulutuksella[10] varmistetaan, että kaikki tietoihin ja tietojärjestelmiin pääsevät työntekijät ymmärtävät jokapäiväisen vastuunsa yrityksen tietoturvatoimien hoitamisesta, suojaamisesta ja tukemisesta. Ilman asiallista koulutusta yrityksen työntekijät voivat toimia riskialttiisti aiheuttaen turvallisuushäiriöitä tai haavoittuvuuksia, joita vastapuoli voi sitten käyttää yrityksen suojauksen murtamiseen.

Yritysjohto **voi** luoda tietoturvariskien hallintakulttuurin omassa yrityksessään. Koulutukseen panostaminen vahvistaa ajan mittaan yrityksen henkilöstön tietoturvaymmärrystä ja kehittää haluttuja taitoja ja valmiuksia.

Turvatoimenpide 4: Valvo tietoympäristöäsi

Yritysten on otettava käyttöön järjestelmiä ja prosesseja, joilla varmistetaan, että organisaatiossa tapahtuvasta tietoturvahäiriöstä myös ilmoitetaan. Yritykset ovat aivan liian usein tietämättömiä turvallisuusloukkauksista; loukkaus tai tartunta on voinut tapahtua jopa kuukausia tai vuosia aikaisemmin, ennen kuin joku havaitsee tunkeutumisen.[11] Tietoturvaloukkauksien havaitsemiseen on tarjolla erilaisia teknisiä ratkaisuja kuten tunkeutumisen-havaitsemis- ja tunkeutumisenestojärjestelmät (IDS- ja IPS-järjestelmät) sekä turvallisuushäiriöiden hallintajärjestelmät. Näiden järjestelmien asentaminen ei kuitenkaan yksin riitä. Teknisten järjestelmien hyödyntäminen edellyttää myös niiden tuottamien tietojen jatkuvaa seurantaa ja analysointia.

10 Loppukäyttäjille suunnattua yleisluonteista tietoa ja tiedotusmateriaalia on saatavilla englanniksi osoitteesta www.staysafeonline.org ja Euroopan verkko- ja tietoturvaviraston (ENISA) aloitteen sivuilta osoitteesta http://www.enisa.europa.eu/media/multimedia/material. Niiden tietoja, videoita ja graafisia esityksiä saa käyttää yrityksissä koulutustarkoituksiin.

11 http://www.verizonenterprise.com/DBIR/

Monissa yrityksissä ei välttämättä ole elintärkeiden järjestelmien ja prosessien seurantaan tarvittavaa asiantuntemusta tai resursseja.

Useat palveluntarjoajat tarjoavat erilaisia tietoturvapalveluja paikan päällä, mukaan lukien pilvipohjaiset tekniset ratkaisut ja palvelut. Kannattaa etsiä omalle organisaatiolle sopiva palvelu ja pyytää kokeneilta tahoilta apua, neuvoa ja tukea asianmukaisten sopimusehtojen muotoiluun.

Jos yritys joutuu verkkohyökkäyksen kohteeksi, on syytä harkita asian ilmoittamista viranomaisille[12] ja toimialajärjestöille – yhteydenpito muiden kanssa voi auttaa selvittämään, onko kyseessä yksittäinen tapahtuma vai onko se osa laajempaa verkkohyökkäystä.[13] Yhteistyö voi usein poikia tietoja ja neuvoja, joiden avulla yritys kykenee ryhtymään tehokkaisiin vastatoimiin.

Turvatoimenpide 5: Vähennä riskejä monikerroksisella suojauksella

Verkon ulkorajojen suojaaminen ja perinteinen pääsynvalvonta eivät enää riitä etenkään silloin, kun yrityksen tietojärjestelmä on yhteydessä internetiin, internet-palveluntarjoajiin, ulkoistettuihin ja pilvipalveluihin, myyjiin ja kumppaneihin sekä kannettaviin laitteisiin, jotka ovat yrityksen valvonnan ulottumattomissa. Toimiva suojaus viruksia, haittaohjelmia tai -laitteita ja hakkereita vastaan edellyttää monikerroksisia suojatoimia tietoturvahäiriöiden vähentämiseksi. Tietoturvariskien hallitseminen yhdistämällä useita ratkaisuja[14] voi pienentää merkittävästi vähäisen tietoturvaloukkauksen vaikutusten laajenemisen mahdollisuutta.

Monikerroksiset tietoturvaratkaisut rajoittavat vastapuolen toimintamahdollisuuksia ja lisäävät yrityksen valvontajärjestelmien mahdollisuuksia havaita tunkeutujat.

Tietoturvavakuutuksella yritys voi puolestaan vähentää häiriön taloudellisia vaikutuksia, mutta myös hallita riskialttiutta ennakoivasti ja vahvistaa yrityksen sisäistä riskienhallintaa.

12 Lisäksi (kyber-)rikosten uhrien tulee tehdä ilmoitus asianmukaisille lainvalvontaviranomaisille. Perinteisissä rikosasioissa paikallinen poliisiasema on usein paras osoite, mutta lainvalvontaviranomaisissa voi olla myös nimenomaan kyberrikollisuuteen (hakkerointi, vahingonteot, vakoilu) erikoistuneita toimijoita.

13 Hyökkäys voi olla horisontaalinen (jolloin kohteena ovat samalla toimialalla toimivat yritykset) tai vertikaalinen (jolloin kohteena ovat alihankkijat) tai yksittäiseen ohjelmistoon tai laitteistoon kohdistuva turvallisuusuhka.

14 Näihin lukeutuvat monien muiden muassa sisällönsuodatus, virustorjunta, ennakoiva haittaohjelmien torjunta, palomuurit, vahvat tietoturvapolitiikat sekä käyttökoulutus.

Turvatoimenpide 6: Varaudu tietoturvaloukkauksiin

Riskienhallinnassa ei ole kyse ainoastaan todennäköisyyden vähentämisestä vaan myös toteutuneen tapahtuman mahdollisesti aiheuttamien vahinkojen minimoimisesta. Tämä tarkoittaa varautumista tapauksen nopeaan selvittämiseen varmistamalla, että tarvittavat resurssit ovat käytettävissä ja että järjestelmät ja prosessit on säädetty tallentamaan kriittistä tietoa. Jos tietoturvaloukkaus johtuu haittaohjelmasta, se pitää saada tuhottua.

Varautuminen tarkoittaa myös sitä, että organisaatiolla on suunnitelma, jonka avulla voidaan tehdä nopeasti oikeita päätöksiä ja toteuttaa tarvittavat toimenpiteet tilanteen hallintaan saamiseksi. Kuka toimii ja miten? Oma tiimi voi vaikuttaa lopputulokseen hyvin suunnitelluilla toimenpiteillä ja tehokkaalla viestinnällä.

Lisäksi varautumalla ennakkoon voidaan minimoida hyökkäyksen haitallisimpia tekijöitä, kuten laitteiden ja ohjelmistojen käytön ja tietojen käytettävyyden estyminen sekä liiketoiminnan jatkamisen viivästyminen. Liiketoiminnan jatkuvuuden ja tietoturvaloukkauksesta toipumisen suunnittelulla voidaan vähentää mahdollisia menetyksiä keskittymällä olennaiseen ja varautumalla tilanteisiin ennakolta.

PERIAATTEIDEN SOVELTAMINEN TIETOTURVAPOLITIIKKAAN

Yritysjohdon tehtäviin kuuluu usein tämän oppaan kaltaisten asiakirjojen sisältämien periaatteiden siirtäminen toimintatapoihin ja käytäntöihin organisaationsa kannalta järkevässä muodossa. Tämän osion tarkoitus on helpottaa tätä tehtävää. Seuraavat, edellä esitettyjen viiden keskeisen turvallisuusperiaatteen mukaisesti järjestetyt, osa-alueet tarjoavat lähtökohtia organisaatiosi kyberturvallisuusriskien hallintatavan ja -käytäntöjen kehittämiselle.

Keskity tietoon, älä tekniikkaan

- Perusta tehtävä tietoturvahankkeiden johtamiseksi ja toteuttamiseksi ja nimitä siihen henkilö, mutta jätä kuitenkin vastuu turvallisuudesta yhä koko yritykselle.
- Suunnitellessaan tietoturvatavoitteidensa saavuttamistapoja organisaation tulee määrittää
  - tehtävät
  - tarvittavat resurssit
  - vastuuhenkilöt
  - toteutusaikataulut
  - tulosten arviointimenetelmät.[15]
- Mikäli yrityksen sisällä ei ole riittävää tietoturva-asiantuntemusta, kannattaa hakea lisätietoa ja pyytää tietoturva-asiantuntijoita auttamaan tietoturvallisuuden juurruttamisessa liiketoimintaprosessien ja tietojärjestelmien suunnitteluun.

Tee tietohäiriöihin varatutumisesta ajattelutapa

- Tietoturvatoimet tulee sovittaa – ja mahdollisuuksien mukaan integroida – määräysten noudattamiseen ja muihin riskien vähentämiseen tähtääviin toimiin päällekkäisten hankkeiden ja vastuiden minimoimiseksi.
- Riskien välttämisen ei tulisi estää uusien teknisten ratkaisujen käyttöönottoa. Tietoturvariskienhallinnan tavoitteiden saavuttamisen lisäksi tietoturvatoimet voivat myös mahdollistaa uusien ja innovatiivisten teknisten ratkaisujen käyttöönoton yrityksessä.
- Varmista, että tietoturvallisuus otetaan huomioon joka ikisessä yrityksen hankkeessa ja etenkin uusissa projekteissa. Kun tietoturvallisuus otetaan mukaan hankkeisiin alusta asti ja oikeanlaisella panostuksella, se ei lisää niiden kustannuksia tai kestoa merkittävästi. Jos taas turvallisuusasiat lisätään myöhemmin tai – pahimmassa tapauksessa – vasta häiriön jo tapahduttua, kustannusten ylitykset, myöhästymiset ja muut vaikutukset ovat moninkertaisia.

15 15 ISO/IEC 27001:2013

- Määritä laitteet, joille annetaan pääsy yrityksen verkkoon ja/tai tietoihin[16] – painottaen mobiililaitteita, kuten henkilöstön tai liikekumppanien laitteita – ja mieti, miten yrityksen laitteistojen ohjelmistoja ja turvallisuusasetuksia hallinnoidaan.
- Arvioi tietojen käyttöoikeudet varmistaaksesi, että käytössä olevat valvontakeinot turvaavat tietojen luottamuksellisuuden, eheyden ja käytettävyyden.
- Kunkin osaston johtajan tulee saada, tarkistaa ja vahvistaa ne sisäiset ja ulkoiset käyttäjät, jotka pääsevät käyttämään osaston sovelluksia ja tietoja. Käyttöoikeuksiin sisältyy vastuu ja riski, joten työntekijöiden mahdollisuutta päästä käsiksi tietoihin ja tietojärjestelmiin on syytä valvoa.
- Kehitä menettelytavat, joilla ilmoitetaan kadonneista tai varastetuista laitteista, ja ota mahdollisuuksien mukaan käyttöön etätyhjennystoiminnot, joilla yrityksen tiedot voidaan poistaa kadonneilta tai varastetuilta laitteilta.

Ole valmis vastatoimiin

- Jokainen tekee virheitä. Yritykset, jotka kääntävät tietoturvavahingot mahdollisuudeksi arvioida turvallisuushäiriöitä avoimesti, voivat luoda kulttuurin, jossa työntekijät uskaltavat ilmoittaa häiriöistä niiden tapahtuessa.
- Valtuuta valitsemasi henkilöstön jäsenet jakamaan asianmukaista tietoa kollegoilleen ja muille toimialalla toimiville sidosryhmille. Näin voit sekä edistää kaikkein parhaiden käytäntöjen luomista että varoittaa mahdollisista tulevista hyökkäyksistä.
- Osoita vastuutaho, joka varmistaa alusta alkaen todistusaineiston asianmukaisen turvaamisen tietoturvatapahtumien ja etenkin verkkorikosten käsittelyn aikana[17].
- Määritä, miten ja milloin tietoturvahäiriöistä ilmoitetaan CERT-kriisiryhmille (cyper emergency response), valtion virastoille tai lainvalvontaviranomaisille.

16 Vaadi käyttäjiä määrittämään tarvittavat mobiililaitteen turvallisuusasetukset, jotta rikolliset eivät pääse varastamaan tietoja laitteen kautta.

17 ICT-henkilöstölle on tarjolla suosituksia tiedonhankintaan turvallisuushäiriöiden selvittämistä tai haittaohjelmatartuntojen käsittelyä varten osoitteessa http://cert.europa.eu/cert/plainedition/en/cert_about.html.

Johtajuudella on merkitystä

- Henkilöstön tulee olla vastuussa tiedoista ja niiden suojaamisesta, ja sillä tulee olla riittävät valtuudet, yhteydet ylimpään johtoon, työkalut ja koulutus varautuakseen tehtäviinsä ja mahdollisiin uhkiin.[18]
- Pienyrityksillä tulisi olla joko talon sisältä tai ulkopuolelta nimetty vastuuhenkilö, joka tarkistaa säännöllisesti tietoturvallisuuden riittävyyden ja on muodollisesti vastuussa tietoturvallisuudesta. Vaikka kyseessä ei välttämättä ole kokoaikainen tehtävä, rooli on tärkeä ja voi osoittautua ratkaisevaksi koko yrityksen selviytymisen kannalta.
- Suurissa yrityksissä toiminnot, tehtävät ja vastuut tulee jakaa harkitusti yksilöiden sekä (virtuaalisten) työryhmien ja toimikuntien kesken. Jokaisen tiimin jäsenen tulee olla täysin selvillä tehtävästään ja vastuustaan. Tässä on keskeistä asianmukainen dokumentointi ja viestintä.

Toteuta visiosi

- Valvo pääsyä sisäverkkoon (ja siitä ulos) ja priorisoi liiketoiminnan ja työntekijöiden tarpeiden kannalta keskeisiä palveluita ja resursseja. [19]
- Edellytä vahvojen salasanojen käyttöä ja harkitse vahvojen tunnistautumismenetelmien[20] käyttöönottoa, jolloin verkkoon pääsy edellyttää salasanan lisäksi muuta tietoa.
- Käytä tarvittaessa salausta tietojen suojaamiseksi säilytyksen ja siirron aikana[21] painottaen etenkin julkisia verkkoyhteyksiä ja kannettavia laitteita, kuten kannettavia tietokoneita, USB-avaimia ja älypuhelimia, joita kadotetaan tai varastetaan helposti.

18 Keskeinen uhka on sosiaalinen urkinta, josta tulisi järjestää henkilöstökoulutusta. Sosiaalinen urkinta tarkoittaa käyttäjien manipuloimista paljastamaan arkaluonteisia tai luottamuksellisia tietoja.

19 Sisällönsuodatuksella voi estää yrityksen resurssien turvallisuusriskejä kasvattavat palvelut ja sivustot, kuten vertaisverkkojen tiedostonjakopalvelut ja pornosivustot. Suodatussääntöjen tulee olla läpinäkyviä kaikille käyttäjille, ja suodatukseen tulee sisältyä prosessi, jolla tahattomasti estettyjen yrityssivustojen eston voi poistaa.

20 Vahvassa eli monitasoisessa tunnistautumisessa yhdistellään useita elementtejä, jotka voivat olla käyttäjän tiedossa (esim. salasana tai henkilökohtainen tunnusluku eli PIN-koodi), hallussa (esim. älykortti tai tekstiviesti) tai ominaisuuksia (esim. sormenjäljen tai iiriksen skannaus).

21 Koska esimerkiksi sähköposti kulkee usein internetissä selväkielisessä muodossa, yritysten tulisi harkita sähköpostin salaustekniikoiden käyttöä arkaluonteisia tietoja lähetettäessä.

PERIAATTEIDEN SOVELTAMINEN TIETOTURVAPOLITIIKKAAN

- Laadi yksityiskohtainen varmistus- ja arkistointitapa, joka täyttää säännösten ja määräysten mukaiset tietojen säilyttämisvaatimukset ja jossa määritellään
  - varmuuskopioitavat tiedot ja varmistusmenetelmät
  - kuinka usein varmuuskopioita otetaan
  - varmuuskopioiden ottamisen ja sisällön varmistamisen vastuuhenkilö
  - varmuuskopioiden säilytyspaikka ja -tapa
  - varmuuskopioiden käyttöoikeudet
  - palautusprosessien toiminta ja niiden testausmenetelmät.
- Kehitä tietoturvallisuutta käsitteleviä koulutusohjelmia, joissa käsitellään seuraavia aiheita:
  - turvallinen ja vastuullinen viestintä
  - sosiaalisen median järkevä käyttö
  - sähköisten tiedostojen turvallinen siirto
  - salasanojen oikea käyttö
  - tärkeän tiedon katoamisen välttäminen
  - tietojen käytön rajaaminen ainoastaan asianosaisille
  - viruksilta ja muilta haittaohjelmilta suojautuminen
  - mahdollisesta turvallisuushäiriöstä ilmoittaminen oikeille henkilöille
  - urkintahuijauksiin lankeamisen välttäminen.

TURVALLISUUDEN ITSEARVIOINTI

Tämä osio sisältää yksinkertaisen tarkistuslistan, jonka avulla johto voi ohjata yrityksensä tietoturvauhkiin valmistautumisen sisäistä arviointia ja kysyä oikeita kysymyksiä näihin hankkeisiin osallistuvilta tiimeiltä. Tarkistuslistan kysymysten avulla johto voi tunnistaa oman yrityksensä vahvuudet ja heikkoudet sekä löytää polkuja niiden kehittämiseen.

Tätä itsearviointikyselyä voidaan myös käyttää yrityksissä, joissa on vastikään ryhdytty toteuttamaan tietoturvahankkeita ja halutaan hyödyntää sen tuottamia tietoja tietoturvauhkiin suojautumisen suunnittelun pohjana.

Vastaajan tulee valita jokaisen kysymyksen kohdalla annetuista vaihtoehdoista se, joka kuvastaa parhaiten oman yrityksen nykyisiä käytäntöjä. Kukin vaihtoehdoista on merkitty erivärisellä luettelomerkillä seuraavasti:

- Tämä on vähiten toivottava vastaus. Yrityksessä on selvästi syytä harkita kehittämistoimia.
- Yrityksen suojauskäytännöissä on vielä parantamisen varaa.
- Vastaus kuvastaa parasta kyberuhkien sietokyvyn tasoa.

Kyselyn vastaukset ovat kunkin arvioijan omia näkemyksiä, ja *kunkin kysymyksen alla oleva yksityiskohtaisempi tarkistuslista* on tarkoitettu helpottamaan yrityksen tietoturvallisuuden hallinnan nykytilan tunnistamista ja dokumentointia. Kyselyssä kerätyt tiedot auttavat nostamaan esiin puutteita tai haavoittuvuuksia, joiden perusteella opasta käyttävät yritykset voivat selvittää, mihin toimiin niiden tulee seuraavaksi ryhtyä.

1

Arvioidaanko yrityksessä luottamuksellisten tietojen käsittelyä?

- Ei, mutta meillä on palomuuri, joka suojaa tietovarkauksilta.
- Kyllä, ymmärrämme tietojemme tärkeyden ja toteutamme yleisiä tietoturvatoimia.
- Kyllä, ja meillä on tiedonluokitusmalli ja tiedämme, missä luottamuksellisia tietojamme säilytetään ja käsitellään. Tietoturvatoimia toteutetaan tietojen luottamuksellisuuden mukaisesti.

Seuraavat kysymykset toimivat perustason tietoturvantarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksen luottamukselliset tiedot tunnistettu ja luokiteltu?		
Tiedostetaanko yrityksessä sen vastuu luottamuksellisiksi määritellyistä tiedoista?		
Onko arkaluonteisimmat tiedot hyvin suojattu tai salattu?		
Onko menettelytavoissa otettu huomioon henkilötietojen hallinnointi?		
Osaavatko kaikki työntekijät tunnistaa ja suojata oikein luottamuksellisia ja muita tietoja?		

2

Tehdäänkö yrityksessä tietoturvaanliittyviä riskiarviointeja?

- Emme tee riskiarviointeja.
- Teemme riskiarviointeja, mutta ne eivät koske erityisesti tietoturva-asioita.
- Teemme riskiarviointeja erityisesti tietoturva-asioista.

Seuraavat kysymykset toimivat perustason tietoturvantarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Käsitelläänkö haavoittuvuusskannausten tuloksia riskien vakavuusasteen mukaisessa järjestyksessä?		
Onko yrityksessä tunnistettu tilanteet, jotka voivat aiheuttaa häiriöitä liiketoimintaprosesseissa, ja onko mahdollisten häiriöiden vaikutukset arvioitu?		
Onko yrityksellä ajantasainen toiminnan jatkuvuussuunnitelma, jota testataan ja päivitetään säännöllisesti?		
Suoritetaanko yrityksessä säännöllisesti riskiarviointeja, joiden pohjalta tietojen suojaustasoa päivitetään tarvittaessa?		
Onko tietojen korruptoitumista tai tahallista väärinkäyttöä pyritty estämään arvioimalla riskitekijät yrityksen kaikissa toimintaprosesseissa?		

3

Millä tasolla tietoturvanhallinta on?

- Yrityksellä ei ole tietoturvahallintoa.
- Tietoturvanhallinta on sijoitettu IT-osastolle, koska se vastaa tietojen suojaamisesta.
- Tietoturvanhallinta on sijoitettu organisaation ylätasolle, jotta sen vaikutukset kattavat koko yrityksen.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Ovatko hallitus ja toimitusjohtaja varanneet tietoturvaa koskevan oman budjetin?		
Kuuluuko tietoturvallisuus johdon nykyiseen riskienhallintaan?		
Hyväksyykö johto yrityksen tietoturvapolitiikan, ja tiedottaako se politiikasta asianmukaisesti henkilöstölle?		
Informoidaanko hallitusta ja johtoa säännöllisesti tietoturvaa koskevien toimintatapojen, standardien, käytäntöjen ja suositusten kehityksestä?		
Onko johtotasolla vähintään yksi henkilö, joka vastaa tietojen suojauksesta ja henkilötietojen suojasta?		

4

Onko yrityksellä tietoturvatiimi tai tietoturvasta vastaava toiminto?

Yrityksellä ei ole tietoturvatiimiä eikä tietoturvaa koskevia tehtäviä ja vastuita ole erikseen määritelty.

Yrityksellä ei ole tietoturvatiimiä, mutta tehtävät ja vastuut on erikseen määritelty.

Yrityksellä on tietoturvatiimi tai tietoturvatoiminto.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksellä nimetty tietoturva-asiantuntija tai -tiimi, joka koordinoi yrityksen omaa osaamista ja avustaa johtoa päätöksenteossa?		
Vastaako nimetty tietoturva-asiantuntija tai -tiimi tietoturvapolitiikan tarkistamisesta ja järjestelmällisestä päivittämisestä merkittävien muutosten tai häiriöiden pohjalta?		
Saako nimetty tietoturva-asiantuntija tai -tiimi riittävästi näkyvyyttä ja tukea voidakseen ottaa kantaa tietojen käsittelyyn liittyviin hankkeisiin yrityksessä?		
Onko eri tyyppisten datojen käsittely ja suojaus hajautettu omille vastuuhenkilöilleen?		
Arvioiko riippumaton elin tai auditoija säännöllisesti tietoturvapolitiikan toteuttamiskelpoisuutta ja vaikuttavuutta sekä tietoturvatiimin tehokkuutta?		

5

Miten yrityksessä käsitellään luottamuksellisiin tietoihin pääsevien kumppaneiden aiheuttamia tietoturvariskejä?

✖ Meillä on molemminpuoliseen luottamukseen perustuvat suhteet kumppaneiden kanssa.

! Joihinkin sopimuksiin sisällytetään tietoturvaan liittyviä ehtoja.

✔ Meillä on käytössä prosessit, joilla validoidaan kumppaneiden pääsy tietoihin, ja erilliset turvallisuusohjeet, jotka annetaan kumppaneille tiedoksi ja allekirjoitettavaksi.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Käytetäänkö alihankkijoiden ja kumppaneiden tunnistamiseen kulkukortteja, joissa on tuore valokuva?		
Onko yrityksellä toimintatapoja alihankkijoiden ja kumppaneiden taustojen tarkistamiseksi?		
Estetäänkö alihankkijan tai kumppanin pääsy tiloihin ja tietojärjestelmiin automaattisesti toimeksiannon päätyttyä?		
Tietävätkö kumppanit, kenelle ja miten yrityksessä tulee ensimmäiseksi ilmoittaa tietojen katoamisesta tai varkaudesta?		
Varmistetaanko yrityksessä, että kumppanit pitävät ohjelmistojensa ja sovellustensa tietoturvapäivitykset ajan tasalla?		
Sisältyykö alihankkijoiden tai kumppanien kanssa solmittaviin sopimuksiin selvästi määriteltyjä tietoturvavaatimuksia?		

6

Arvioidaanko yrityksessä säännöllisesti tietokoneiden ja verkon turvallisuutta?

- Emme arvioi tietokoneiden ja verkon turvallisuutta tarkistuksilla tai tunkeutumistesteillä.
- Meillä ei ole järjestelmällistä menettelytapaa tietoturvatarkastusten ja/tai tunkeutumistestien suorittamiselle, mutta niitä toteutetaan satunnaisesti.
- Säännölliset tietoturvatarkastukset ja/tai tunkeutumistestit kuuluvat järjestelmällisesti yrityksen tietokoneiden ja verkon turvallisuusarviointeihin.

Seuraavat kysymykset toimivat perustason tietoturvantarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Suoritetaanko yrityksessä säännöllisiä testejä ja pidetäänkö havaituista uhista kirjaa?		
Onko yrityksellä menettelyä, jolla arvioidaan ihmisistä johtuvia uhkia tietojärjestelmille, kuten epärehellisyys, sosiaalinen urkinta ja luottamuksen väärinkäyttö?		
Pyytääkö yritys tietoturvatarkastustenraportteja tietopalvelujen tarjoajiltaan?		
Arvioidaanko tietoturvatarkastusten yhteydessä myös erityyppisten tallennettujen tietojen hyödyllisyyttä?		
Auditoidaanko yrityksessä informaatioprosessien ja -menettelyjen yhdenmukaisuutta yrityksen muiden toimintatapojen ja standardien kanssa?		

7

Arvioidaanko yrityksessä mahdollisia tietoturvariskejä uusien teknisten ratkaisujen käyttöönoton yhteydessä?

- Tietoturva ei sisälly uusien teknisten ratkaisujen käyttöönottoprosessiin.
- Tietoturva sisältyy uusien teknisten ratkaisujen käyttöönottoprosessiin vain satunnaisesti.
- Tietoturva sisältyy uusien teknisten ratkaisujen käyttöönottoprosessiin.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Arvioidaanko uusien teknisten ratkaisujen käyttöönottoa harkittaessa niiden mahdollisia vaikutuksia yrityksen tietoturvapolitiikkaan?		
Onko yrityksellä suojaustoimia, joilla vähennetään riskejä uusien teknisten ratkaisujen käyttöönoton yhteydessä?		
Onko uusien teknisten ratkaisujen käyttöönottoprosessit dokumentoitu?		
Onko yrityksellä kumppanuussuhteita, jotka mahdollistavat yhteistyön ja kriittisen turvallisuustiedon vaihdon uusien teknisten ratkaisujen käyttöönoton yhteydessä?		
Onko yrityksessä ymmärretty, että tietoturvapolitiikka ei ole este teknisille mahdollisuuksille?		
Hallinnoidaanko yrityksessä uutta tekniikkaa tietoturvajärjestelmien kehitysmenetelmillä järjestelmien elinkaaren aikana?		

8

Järjestetäänkö yrityksessä tietoturvakoulutusta?

- Meillä luotetaan työntekijöihin eikä pidetä tietoturvakoulutusta lisäarvona.
- Ainoastaan IT-henkilöstöä koulutetaan yrityksen tietoteknisen ympäristön suojaamiseen.
- Kaikille työntekijöille järjestetään säännöllisiä tiedotustilaisuuksia tietoturva-asioista.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Mukautetaanko osa tietoturvaa käsittelevistä koulutustilaisuuksista työntekijöiden tehtäviä vastaaviksi?		
Opastetaanko työntekijöitä tarkkailemaan tietoturvaloukkauksia?		
Onko yritys ohjeistanut käyttäjiä ilmoittamaan järjestelmien tai palvelujen turvallisuuteen liittyvistä heikkouksista tai uhista?		
Osaavatko työntekijät käsitellä luottokorttitietoja ja luottamuksellisia henkilötietoja asianmukaisesti?		
Saavatko myös ulkopuoliset käyttäjät (soveltuvin osin) tarvittavaa tietoturvakoulutusta ja säännöllisiä tietoiskuja organisaation toiminta- ja menettelytavoista?		

9

Miten yrityksessä käytetään salasanoja?

Salasanoja jaetaan kollegojen kesken, ja/tai yrityksellä ei ole salasanojen turvallista käyttöä tai niiden säännöllistä vaihtamista koskevaa toimintaohjetta.

Kaikilla työntekijöillä ja johtajilla on oma salasana, mutta salasanoille ei ole määritetty vahvuusvaatimuksia. Salasanojen vaihtaminen on mahdollista, mutta ei pakollista.

Jokaisella työntekijällä ja johtajalla on henkilökohtainen salasana, jonka on täytettävä salasanoille määritetyt vaatimukset ja joka on vaihdettava säännöllisesti.

Seuraavat kysymykset toimivat perustason tietoturvantarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksessä laadittu ja toimeenpantu yleisesti hyväksytyt salasanaohjeistukset?		
Täyttävätkö kaikki yrityksessä käytetyt salasanat seuraavat edellytykset? Niitä ei ole tallennettu helposti saataviin tiedostoihin. Ne eivät ole heikkoja tai tyhjiä, eikä oletussalasanoja ole jätetty vaihtamatta. Niitä ei jätetä vaihtamatta tai vaihdeta vain harvoin, etenkään mobiililaitteissa.		
Onko yrityksen järjestelmät mielestäsi hyvin suojattu tunkeutumiselta?		
Ovatko käyttäjät ja alihankkijat tietoisia omasta vastuustaan suojata laitteet myös silloin, kun ne jäävät ilman valvontaa (esim. kirjautumalla ulos)?		
Onko työntekijöille kerrottu, miten tunnistetaan sosiaalisessa urkinnassa käytetyt tavat, joilla ihmisiä huijataan paljastamaan tietoja, ja osaavatko he reagoida tällaiseen uhkaan?		

10

Onko yrityksellä internetin ja sosiaalisen median asianmukaista käyttöä koskevat toimintaohjeet?

Ei, yrityksellä ei ole internetin ja sosiaalisen median asianmukaista käyttöä koskevaa toimintaohjetta.

Kyllä, yrityksellä on keskitetysti kaikkien työntekijöiden saatavilla oleva toimintaohje, mutta heidän ei tarvitse allekirjoittaa sitä.

Kyllä, internetin asianmukaista käyttöä koskeva toimintaohje sisältyy sopimukseen, tai kaikki työntekijät ovat allekirjoittaneet sen.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksellä työntekijöille suunnattuja yleisiä lehdistösuhteita ja sosiaalista mediaa koskevia viestintäohjeita ja -prosesseja?		
Onko yrityksessä kurinpitomenettely työntekijöille, jotka rikkovat yrityksen viestintäohjeita?		
Seuraako nimetty viestintäpäällikkö tai -tiimi internetin sisältöjä arvioidakseen yrityksen verkkomainetta ja siihen liittyviä riskejä?		
Onko yrityksessä arvioitu vastuukysymyksiä, jotka liittyvät työntekijöiden tai muiden sisäisten käyttäjien toimiin, tai järjestelmää laittomiin tarkoituksiin hyödyntävien hyökkääjien tekoihin?		
Onko yritys ryhtynyt toimiin estääkseen työntekijöitä tai muita sisäisiä käyttäjiä hyökkäämästä muihin kohteisiin?		

11

Mitataanko, raportoidaanko ja seurataanko yrityksessä tietoturva-asioita?

Meillä ei tarkkailla, raportoida tai seurata yrityksessä toteutettujen turvatoimien tehokkuutta ja riittävyyttä.

Yrityksessä on otettu käyttöön työkalut ja menetelmät, joilla tarkkaillaan, raportoidaan ja seurataan joidenkin yrityksessä toteutettujen turvatoimien tehokkuutta ja riittävyyttä.

Yrityksessä on otettu käyttöön työkalut ja menetelmät, joilla tarkkaillaan, raportoidaan ja seurataan kaikkien yrityksessä toteutettujen turvatoimien tehokkuutta ja riittävyyttä.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Ylläpidettäänkö yrityksessä häiriöihin liittyviä kirjausketjuja ja lokeja ja pyritäänkö häiriöiden toistumista ehkäisemään?		
Varmistetaanko yrityksessä, että säännöksiä ja määräyksiä noudatetaan esimerkiksi tietosuoja-asioissa?		
Onko yrityksessä kehitetty omia työkaluja, joilla johto voi arvioida turvallisuusasennetta ja joilla voidaan tehostaa yrityksen kykyä vähentää mahdollisia riskejä?		
Onko yrityksellä tietoturvasuunnitelma, joka kattaa tavoitteet, edistymisen arvioinnin ja yhteistyömahdollisuudet?		
Toimitetaanko seurantaraportteja ja häiriötietoja viranomaisille ja eturyhmille, kuten toimialajärjestölle?		

12

Miten yrityksen järjestelmiä pidetään ajan tasalla?

- ✖ Meillä luotetaan pääosin myyjän tarjoamaan automaattiseen päivitysten hallintaan.
- ! Turvallisuuspäivitykset asennetaan järjestelmällisesti kuukausittain.
- ✔ Meillä on prosessi tietoturvahaavoittuvuuksien hallintaan. Mahdollisista haavoittuvuuksista etsitään jatkuvasti tietoa (esim. käyttämällä tilauspalvelua, josta lähetetään automaattisesti varoituksia uusista haavoittuvuuksista), ja turvallisuuspäivitykset asennetaan aina tarpeen mukaan.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko haavoittuvuusskannaus yrityksessä säännöllisesti aikataulutettu ylläpitotehtävä?		
Tarkistetaanko ja testataanko järjestelmä aina, kun siihen tulee muutoksia?		
Voivatko käyttäjät tarkistaa itse, onko järjestelmässä päivittämättömiä sovelluksia?		
Tietävätkö käyttäjät, että heidän tulee pitää ajan tasalla myös mobiililaitteidensa käyttöjärjestelmä ja sovellukset, mukaan lukien tietoturvaohjelmistot?		
Onko käyttäjiä koulutettu tunnistamaan aidot varoitusviestit, kuten päivitysten lupapyynnöt (erotuksena tekaistuista virustorjuntailmoituksista) ja ilmoittamaan turvallisuustiimille asianmukaisesti haitallisista tai kyseenalaisista tapahtumista?		

13

Tarkistetaanko ja hallinnoidaanko sovellusten ja järjestelmien käyttöoikeuksia säännöllisesti?

Sovellusten ja järjestelmien käyttöoikeuksia ei poisteta eikä tarkisteta johdonmukaisesti.

Sovellusten ja järjestelmien käyttöoikeudet poistetaan ainoastaan työntekijän lähtiessä yrityksestä.

Yrityksellä on käyttöoikeuspolitiikka, joka kattaa yrityksen kaikkiin keskeisiin sovelluksiin ja tukijärjestelmiin myönnettyjen käyttöoikeuksien säännölliset tarkistukset.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko pääsy sähköisiin tietojärjestelmiin ja toimitiloihin rajoitettu toimintatavoilla ja käytännöillä?		
Onko yrityksellä tietosuojapolitiikka, jossa ilmoitetaan, mitä tietoja se kerää (esim. asiakkaiden katu- ja sähköpostiosoitteet, selaushistoria jne.) ja mitä niillä tehdään?		
Onko toimintaohjeissa ja käytännöissä määritetty menetelmät, joilla valvotaan pääsyä suljetuille alueille, kuten ovien lukot, kulunvalvontajärjestelmät tai videovalvonta?		
Estetäänkö työntekijän pääsy tiloihin ja tietojärjestelmiin automaattisesti työsuhteen päättyessä?		
Onko arkaluonteiset tiedot luokiteltu (erittäin luottamuksellinen, arkaluonteinen, vain sisäiseen käyttöön), ja onko käyttöoikeuksien haltijat luetteloitu?		
Onko yritys kehittänyt prosessit sähköisten tietojärjestelmiensä etäkäytön säätelyyn?		

14

Voivatko työntekijät tallentaa tai siirtää yrityksen tietoja omille laitteilleen, kuten matkapuhelimille ja tablettitietokoneille?

Kyllä, yrityksen tietoja voi tallentaa tai siirtää omille laitteille ilman ylimääräisiä turvatoimia.

Yrityksellä on toimintaohje, jossa kielletään yrityksen tietojen tallentaminen tai siirtäminen omille laitteille, mutta se on teknisesti mahdollista käyttämättä ylimääräisiä turvatoimia.

Yrityksen tietoja voi tallentaa tai siirtää omille laitteille ainoastaan sitten, kun ne on suojattu, ja/tai käytössä on ammattikäyttöön soveltuva ratkaisu.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksellä laajasti hyväksytty omien laitteiden käyttöä koskeva toimintaohje?		
Onko mobiililaitteet suojattu luvattomilta käyttäjiltä?		
Tunnistetaanko kaikki laitteet ja yhteydet pysyvästi verkossa?		
Asennetaanko jokaiselle mobiililaitteelle salaus tietojen luottamuksellisuuden ja yhteneväisyyden turvaamiseksi?		
Ollaanko yritystasolla tietoisia siitä, että vaikka yksittäinen työntekijä voi olla vastuussa laitteesta, yritys on silti vastuussa tiedoista?		

15

Onko yrityksessä tehty tallennettujen tietojen menetyksen ehkäisemiseen tähtääviä toimia?

- Yrityksellä ei ole varmistus- tai käytettävyysprosessia.
- Yrityksellä on varmistus- tai käytettävyysprosessi, mutta palautustestejä ei ole tehty.
- Yrityksellä on varmistus- tai käytettävyysprosessi, joka kattaa palautus- ja sietokykytestit. Varmuuskopiot säilytetään turvallisessa paikassa toimipaikan ulkopuolella, tai yrityksessä käytetään muita käytettävyyden varmistusratkaisuja.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Onko yrityksessä riittävästi henkilöstöä, joka osaa tehdä palautettavia varmuus- ja arkistokopioita?		
Onko laitteistot suojattu sähkökatkoilta turvaamalla sähkönsyöttö esimerkiksi usealla virtalähteellä, katkottomilla virtalähteillä eli UPS-laitteilla (uninterruptible power supply) tai varavoimakoneilla?		
Testataanko varmuuskopiointivälineet säännöllisesti sen varmistamiseksi, että tiedot voidaan palauttaa palautusmenettelylle varatussa ajassa?		
Onko yrityksessä käytössä kadonneiden tai varastettujen mobiililaitteiden ilmoitusmenettely?		
Onko henkilöstö koulutettu toimimaan tilanteissa, joissa tietoja on poistettu vahingossa, ja hakemaan tietoja poikkeustilanteissa?		
Onko varmuuskopioiden luottamuksellisuus ja eheys turvattu niiden varastointipaikassa?		

16

Onko yrityksessä varauduttu hoitamaan tietoturvahäiriöitä?

Meillä ei esiinny häiriöitä, ja jos esiintyy, työntekijöillä on riittävästi osaamista niiden hoitamiseen.

Yrityksellä on sovitut menettelyt häiriötilanteisiin, mutta niitä ei ole mukautettu käsittelemään tietoturvahäiriöitä.

Meillä on nimenomaan tietoturvahäiriöiden käsittelyyn tarkoitettu prosessi, joka kattaa tarvittavat eskalointi- ja viestintäjärjestelyt. Pyrimme käsittelemään häiriöt mahdollisimman tehokkaasti oppiaksemme, miten voimme suojautua vastaisuudessa entistä paremmin.

Seuraavat kysymykset toimivat perustason tietoturvan tarkistuslistana, jonka avulla yritys voi arvioida omaa edistymistään.	KYLLÄ	EI
Kattaako yrityksen prosessi erityyppiset häiriöt palvelunestohyökkäyksistä luottamuksellisuuden rikkomuksiin jne. sekä niiden käsittelytavat?		
Onko yrityksellä häiriönhallinnan viestintäsuunnitelma?		
Tiedetäänkö yrityksessä, mille viranomaisille häiriöistä ilmoitetaan ja miten?		
Onko yrityksellä erityyppisiä häiriöitä varten lajitellut ja yksilöidyt yhteystiedot?		
Ovatko yhteydet työntekijöihin ja heidän perheenjäseniinsä yrityksen viestintäpäällikön vastuulla?		
Onko yrityksellä oppimisprosessi häiriönhallinnan kehittämiseksi tietoturvahäiriöiden jälkeen?		

LÄHTEET JA AINEISTOT

Oppaan rinnalle on tarjolla sähköinen liite, joka sisältää lisämateriaalia menettelyohjeista teknisiin standardeihin. Osoitteesta www.iccwbo.org/cybersecurity löytyy luettelo keskeisistä kansainvälisistä viitekehyksistä, aineistoista ja yhteystiedoista sekä aikanaan myös paikallisia viitekehyksiä, sitä mukaa kun ICC:n kansalliset osastot ja jäsenet niitä toimittavat. Sivusto antaa yleiskatsauksen oppaan julkaisuajankohtana tarjolla oleviin aineistoihin, mutta sitä päivitetään ja laajennetaan jatkuvasti.

www.iccwbo.org/cybersecurity

Kansainvälisen kauppakamarin tietoturvaopas on saatavilla myös verkossa, kattavassa aineistoportaalissa, johon on koottu kansainvälisiä ja kansallisia normeja, käytäntöjä ja neuvoja tietoturvallisuuden teknisiin ja toiminnallisiin puoliin liittyvistä aiheista.

Portaali sisältää

- *Tietoturvaopas yrityksille* -julkaisun ladattavana tiedostona
- oppaan käännökset ja/tai lokalisoidut versiot
- linkkejä kansainvälisesti hyväksyttyihin hyviin käytäntöihin, standardeihin ja viitekehyksiin
- luettelon maailmanlaajuisesti tieto- ja kyberturvallisuuden alalla vaikuttavista julkisista elimistä ja järjestöistä
- linkkejä yritysten, valtion viranomaisten ja muiden tahojen laatimiin maakohtaisiin aineistoihin.

KANSAINVÄLINEN KAUPPAKAMARI (ICC)

Kansainvälinen kauppakamari (*International Chamber of Commerce*, ICC) on maailmanlaajuinen elinkeinoelämän etujärjestö, joka edustaa vaikutusvaltaisesti kaikilla toimialoilla ja kaikkialla maailmassa toimivia yrityksiä.

ICC:n tehtävänä on edistää avointa kansainvälistä kauppaa ja sijoitustoimintaa sekä auttaa yrityksiä vastaamaan globalisaation haasteisiin ja mahdollisuuksiin. Järjestön vakaumus, jonka mukaan kauppa on vahvasti rauhaa ja vaurautta edistävä voima, on peräisin sen syntyajoilta 1900-luvun alusta. Tuolloin ICC:n perustanut pieni kaukonäköisten yritysjohtajien joukko kutsui itseään ”rauhan kauppiaiksi”.

ICC:llä on kolme päätehtävää: sääntöjen laatiminen, riitojen ratkaisu ja poliittinen edunvalvonta. Koska ICC:n jäsenyritykset ja -järjestöt harjoittavat itsekin kansainvälistä liiketoimintaa, sen vaikutusvalta rajat ylittävää liiketoimintaa ohjaavien menettelytapasääntöjen laatijana hakee vertaistaan. Vaikka säännöt ovatkin vapaaehtoisia, niitä noudatetaan päivittäin tuhansissa liiketoimissa ja niistä on tullut osa kansainvälisen kaupan kokonaisuutta.

ICC tarjoaa myös tärkeitä palveluja, joista merkittävin on ICC:n kansainvälinen välimiesoikeus (*ICC International Court of Arbitration*), maailman johtava välityselin. Sen palveluihin lukeutuu myös kauppakamarien maailmanjärjestö *ICC World Chambers Federation*, joka edistää vuorovaikutusta ja parhaiden käytäntöjen jakamista kauppakamarien välillä. Lisäksi ICC tarjoaa erikoistuneita koulutuksia ja seminaareja ja on alan johtava kansainvälistä yritys-, pankki- ja välitystoimintaa koskevien käytännönläheisten apuvälineiden ja koulutusaineistojen julkaisija.

ICC:n jäsenistöstä valitut yritysjohtajat ja asiantuntijat muodostavat elinkeinoelämän kannan kauppa- ja investointipolitiikan laajoihin kysymyksiin sekä niihin liittyviin erityisaiheisiin. Näihin lukeutuvat mm. korruption vastainen toiminta, pankkitoiminta, digitaalitalous, markkinoinnin etiikka, ympäristö ja energia, kilpailupolitiikka sekä immateriaalioikeudet.

ICC tekee tiivistä yhteistyötä Yhdistyneiden kansakuntien, Maailman kauppajärjestön sekä hallitustenvälisten foorumeiden, kuten G20-ryhmän, kanssa.

ICC on perustettu vuonna 1919. Nykyään sen maailmanlaajuinen verkosto muodostuu yli 6 miljoonasta yrityksestä, kauppakamarista ja elinkeinoelämän järjestöstä yli 130 maassa. ICC:n kansalliset osastot käsittelevät maansa suorien jäsenten asioita ja välittävät ICC:n muotoilemia elinkeinoelämän näkemyksiä oman maansa hallitukselle.

INTERNATIONAL CHAMBER OF COMMERCE

The world business organization

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 **F** +33 (0)1 49 53 28 59
E icc@iccwbo.org www.iccwbo.org

ISBN: TIETOTURVAOPAS YRITYKSILLE
978-952-5620-84-9

DITTMAR & INDRENIUS

What Are You Storing?

Microsoft

Käyttäjä, sinä olet uudessa tietoturvaympäristössä keskiössä

Elämme ajassa, jossa ihmiset ovat liikkuvia ja haluavat käyttää palveluita ajasta ja paikasta riippumatta niin työssä kuin vapaa-ajallakin. Myös liiketoiminta hyötyy, kun tehtäviä voi hoitaa kaikkialla. Perinteisten tietotekniikkapalvelujen rinnalle on tullut julkisia pilvipalveluita. Menestyksekäs ja vastuullinen liiketoiminta tässä muuttuneessa ympäristössä vaatii uudenlaisen lähestymisen myös tietoturvaan.

Aikaisemmin yritysten tietoturvaratkaisut rakennettiin hyvin rajattuun ympäristöön, kun käyttäjät pääsääntöisesti olivat fyysisesti samassa paikassa ja käyttivät paikallisen verkon palveluita. Uudessa mobiilissa ja verkottuneessa maailmassa tietoturvan kehityksessä täytyy ottaa huomioon neljä ulottuvuutta: laitteiden tietoturva, dokumenttien ja sisällön tietoturva, käyttäjän identiteetin tietoturva ja uhkien ennaltaehkäisy.

Laitteistot ja käyttöjärjestelmä

Ennen käyttäjien päätelaitteet eivät sisältäneet merkittävissä määrin tietoturvaa lisääviä toimintoja, ja käyttöjärjestelmätasolla tietoturvasta vastasi lähinnä palomuuri. Uusimmissa laitteissa käyttäjien tietoturvaa parantavat esimerkiksi tietoturvasirut ja virtualisoinnilla eriytetyt käyttäjätiedot ja sovellukset. Windows 10 -käyttöjärjestelmän edistyneet tietoturvaominaisuudet hyödyntävät täysimääräisesti modernien laitteiden tietoturvatoiminnot. Windows suojaa laitteet, käyttäjät ja datan.

Dokumentit ja sisältö

Modernissa työympäristössä ihmiset haluavat pääsyn dokumentteihin laitteesta ja paikasta riippumatta. Tietoturva täytyy siis lisätä osaksi dokumenttia, oli se ladattuna ja tallennettuna vaikka puhelimelle. Windows 10:ssä dokumentit voidaan salata tallennussijainnin, tietoturvaluokituksen ja sisällön perusteella, vaikkapa henkilötietoja sisältävät dokumentit automaattisesti.

Käyttäjän identiteetin tietoturva

Identiteetin tietoturva vaatii perinteisen käyttäjätunnuksen ja salasanan rinnalle vahvempia tunnistautumiskeinoja. Modernit laitteet sisältävät tähän käyttäjäystävällisiä ratkaisuja, kuten kasvo-, iiris- ja sormenjälkitunnisteiden käytön. Niitä käyttäen myös sovelluksiin kirjautuminen on helppoa, nopeaa ja turvallista.

Uhkien ennaltaehkäisy

Ennaltaehkäisyssä korostuvat riskien tunnistaminen ja tunnistettuihin riskeihin perustuvat toimintamallit. Näin esimerkiksi Windows 10 Defender suojaa laitetta ja käyttäjää haittaohjelmilta. Jos kuitenkin tapahtuu jotain, Windows 10 Defender Advanced Threat Protection pystyy tarkalla tasolla selvittämään, miten ongelma on syntynyt ja mihin asti se on levinnyt.

”Windows 10:n uudet ominaisuudet tekevät siitä todennäköisesti kaikkien aikojen turvallisimman Windows-alustan.”

– Amerikkalaisen autourheilutiimin tietohallintojohtaja

Lue lisää osoitteessa: microsoft.com/security

Lisätietoja: **Aki Siponen**
Teknologiajohtaja, Microsoft Oy
aki.siponen@microsoft.com
+358 50 351 2690

SECRAYS.FI PRESENTS

DO WHAT YOU LOVE

LET US GIVE YOU
PEACE OF MIND.

Secrays
INFORMATION SECURITY

DITTMAR & INDRENIUS