# TIETOTURVAOPAS YRITYKSILLE

## *ICC Cyber security guide for business*

ICC FINLAND
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

KESKUS-
KAUPPAKAMARI

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?<br>Niitä ei ole tallennettu helposti saataviin tiedostoihin.<br>Ne eivät ole heikkoja tai tyhjiä, eikä oletussalasanoja ole jätetty vaihtamatta.<br>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