STRATEGIA22

TUTKIMUSRAPORTTI

Digitalisaatioaiheiden ja kyberriskien huomioiminen yrityksien strategioissa

3.11.2021

Digipooli ja Cyberwatch Oy

Tiivistelmä

STRATEGIA22-projektin vaiheen 2 tehtävänä oli selvittää yritysten kyberturvallisuuteen liittyvä nykytila. Selvitys suoritettiin kyselytutkimuksena ja haastatteluilla. Samalla laadittiin taustaselvitys kattaen vuodet 2019–2021.

Kyselytutkimuksen tavoitteena oli selvittää, mitä yritysjohtajat ajattelevat, tuntevat, kokevat tai uskovat oman yrityksen strategisen tason kyberturvallisuudesta. Tulosten perusteella laaditaan toimenpidesuosituksia ja parhaita käytäntöjä yritysjohdolle, joiden avulla voidaan parantaa nykyistä vallitsevaa tilannetta.

Tutkimus toteutettiin standardoituna survey-tutkimuksena, jolloin asiat kysyttiin kaikilta vastaajilta täsmälleen samalla tavalla monivalintakysymyksinä, joissa oli valmiit vaihtoehdot ja vastaaja merkitsi yhden tai useamman vaihtoehdon. Täydentävät haastattelukysymykset laadittiin erikseen noudattaen ao. periaatetta ja vapaamuotoisuutta.

Taustaselvityksen mukaan kaupallisten toimijoiden tarkoituksena on myydä kyberturvallisuuspalveluja, joiden sisältö sovitaan asiakkaan kanssa. Varsinaisia malleja kyberstrategioiden laatimiseksi ei esiinny, mutta on tulkittavissa niiden sisältyvän mahdollisiin yhteistyöprojekteihin asiakkaan tarpeiden mukaisesti. Kyberturvallisuuskeskus on tuottanut 2 hyvää opasta yritysten käyttöön. Toinen ohjaa isompien yritysten ajattelua kyberturvallisuuteen kysymysten asettelun kautta. Toinen taas pienempien yritysten käytännön toimenpiteiden huomioimista. Tiedeyhteisö tukee strategisen tason tutkimusta, mutta toistaiseksi tämän aihepiirin tutkimuksia on lukumääräisesti vähän Suomessa. Laajemmin tarkasteltuna hallintomallien käsittely on toimialakohtaista ja perustuu usein olemassa olevien standardien (esim. ISO27001, Katakri) käyttöön tai soveltamiseen.

Kokonaistutkimuksen johtopäätöksenä toimintasuosituksien kehittämisessä ja laadinnassa tulisi ottaa huomioon seuraavat aiheet:

1. Digi- ja kyberturvallisuustavoitteet ja menestystekijät osaksi tuotteita ja palveluita.
2. Digiturvallisuuden taloudelliset/tehokkuus tavoitteet/vaatimukset.
3. Strategiatyön vakiointi suuryrityksistä pienempiin, standardien tai vastaavien käyttö.
4. Toimintaympäristön seuranta: PK-yritysten ja pienempien kybertilannekuvan sisältö ja laatu.
5. Riskien hallinta ja jatkuvuuden kehittäminen, resilienssin kasvattaminen, digitaalisen turvallisuuden mittarit.
6. Digitaalisen turvallisuuden yhteistoiminnan kehittäminen toimitusketjuissa.
7. Viestinnän ja harjoittelun kehittäminen poikkeustilanteissa.

Sisällys

Johdanto

Kyberturvallisuuden strateginen johtaminen on digitaalisen toimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamista, asettamista, toiminnan ja varautumisen yhteensovittamista sekä laajamittaisten häiriöiden hallinnan johtamista. (Lehto et al, 2018)

Yksityisen sektorin merkitys ja haasteet on ymmärrettävä kyberturvallisuuden ja sen kansallisen strategisen johtamisen osana. On kiinnitettävä huomiota alihankintaketjujen muodostamiin riskeihin. Keskeinen haaste on vakuuttaa yksityinen sektori siitä, että digitaalisessa maailmassa tieto- ja kyberturvallisuus on aito kilpailutekijä ja tietoturvallisten tuotteiden sekä palveluiden saatavuutta tulee edistää sekä EU:ssa että globaalisti. Yksityinen sektori on saatava tähän mukaan ennen kaikkea tuotteiden ja palveluiden loppukäyttäjien näkökulmasta. (Lehto et al, 2018)

STRATEGIA22-projektin kokonaistavoitteena on tuottaa toteuttamiskelpoisia kehittämis- ja toimeenpanoehdotuksia tukemaan yrityksien johtajia ja johtoryhmiä yrityksen kyberturvallisuuden johtamisessa.

Projektin tehtävänä on selvittää yritysten kyberturvallisuuteen liittyvä nykytila. Selvitys suoritettiin kyselytutkimuksena ja haastatteluilla. Samalla laaditaan olemassa olevista tutkimustuloksista katsaus kattaen vuodet 2019–2021.

Kyselytutkimuksen tavoitteena oli selvittää, mitä yritysjohtajat ajattelevat, tuntevat, kokevat tai uskovat oman yrityksen strategisen tason kyberturvallisuudesta. Tulosten perusteella laaditaan toimenpidesuosituksia yritysjohdolle parantamaan nykyistä vallitsevaa tilannetta.

Tutkimusmenetelmät

Tutkimus toteutettiin standardoituna survey-tutkimuksena, jolloin asiat kysyttiin kaikilta vastaajilta täsmälleen samalla tavalla. Kysymykset laadittiin monivalintakysymyksinä, joissa oli valmiit vaihtoehdot ja vastaaja merkitsi yhden tai useamman vaihtoehdon. Haastattelukysymykset laadittiin erikseen noudattaen ao. periaatetta ja vapaamuotoisuutta. Nettikysely toteutettiin ajanjaksolla 9.9.- 15.10.2021, vastauksia yhteensä 69 kpl. Haastattelut suoritettiin ajanjaksolla 7.10.- 4.11.2021, yhteensä haastateltavia oli 10 kpl.

Tutkimus kohdistettiin yritysjohdolle sekä strategian suunnittelijoille, liiketoiminnan suunnittelijoille, ja näistä vastaaville. Strategiakysymykset ja operatiiviset kysymykset eroteltiin. Tavoitteena oli löytää asioita strategisten puutteiden korjaamiseksi.

Kyselytutkimuksen vaiheet olivat seuraavat (Hiltunen, 2009):

1. tutkimuksen suunnittelu
2. kysymysten laadinta ja tarvittavien taustamuuttujien määrittäminen
3. kysymyslomakkeen laadinta (nettikysely)
4. kyselyn toteuttaminen
5. aineiston analyysi ja tulkinta, jatkohaastattelut
6. tutkimuksen arviointi ja raportin laadinta

Toimittaja laati kysymyssarjan, joka sisälsi tulosten käsittelyyn ja tilastointiin liittyviä taustakysymyksiä 9 kpl ja varsinaisia kysymyksiä 56 kpl. Kysymyssarja on liitteessä 1.

Kysymyssarja laadittiin modulaarisesti seuraavasti:

i. Taustatiedot
ii. Yrityksen strategiantyön lähtökohdat
iii. Yrityksen strategiatyö
iv. Yrityksen strategian toimeenpano ja tulosten mittaaminen
v. Yrityksen digi- ja kyberturvallisuustoimenpiteiden nykytilanne

Kysely- ja haastatteluaineistojen analyysissä ja tulkinnassa pyrittiin selittävään lähestymistapaan, jolloin käytettiin tilastollista analyysia ja päätelmien tekoa, sekä ymmärtämiseen pyrkivään lähestymistapaan, jossa käytetään tavallisesti laadullista analyysia ja päätelmien tekoa. Analyysissä käytettiin kyselyalustan *LimeSurvey* tilastollisia menetelmiä.

Haastateltavat yritykset valittiin vapaaehtoisuuden perusteella. Haastattelukysymykset ovat liitteessä 2.

Haastattelukierroksen yhteydessä selvitettiin yhden yrityksen liiketoimintaketjun tarkastelu kyberturvallisuuden näkökulmasta konkreettisena esimerkkinä, joka on liitteessä 3.

Taustaselvitys

Taustaselvitys laadittiin kirjallisuus- ja asiakirjakatsauksena ajanjaksolta 2019–2021. Katsaukseen valittiin keskeisiä Suomessa vaikuttavia kyberturvallisuuden edistämiseen liittyviä tai osallistuvia yrityksiä, organisaatioita ja yhteisöjä. Tarkoitus oli etsiä suoraan tutkimuksen aiheeseen liittyviä toimintamalleja. Jos jokin tarkasteltava kohde ei täyttänyt tätä tavoitetta, niin tarkasteltiin kohteen lähestymiskulmaa ja tavoiteltua kohdetta. Erityisesti yritysten avoimista lähteistä saadut tiedot jäävät hyvinkin puutteellisiksi.

1. Taustaa kyberstrategiatyölle

Andrews (1997) kuvaa strategiaprosessin ylintä päätasoa, eli yritysstrategiaa, yrityksen päätöksentekomallina, joka määrittää yrityksen päämäärät sekä tarkoituksen. Yritysstrategia tuottaa periaatteelliset käytännöt ja suunnitelmat näiden päämäärien saavuttamiseen sekä lopulta määrittää ne toimialat ja markkinat, jossa yritys haluaa toimia omistajiensa eduksi. Johnson et al (2008) mukaan yritysstrategia määrittelee yrityksen koko toiminnan alan, ja sen miten arvoa lisätään yritysorganisaation eri liiketoimintayksiköissä.

Kasvavan paineen edessä yritysten on koordinoitava päätoimintojaan johdonmukaisen strategian puitteissa. Kaikki toiminnalliset panokset ja oivallukset ovat välttämättömiä strategisen suunnan ymmärtämiseen, ratkaisemiseen ja sopimiseen. Yritystason strategia koskee yrityksen niitä kilpailualoja, joita se pitää tärkeinä tulojen ja voittojen kasvun kannalta, sekä kullekin alalle annettavaa etusijaa investointien ja resurssien muun kohdentamisen kannalta. (Hill & Hill, 2009)

Koska yritystason strategia kiinnostaa ennen kaikkea yrityksen omistajia ja osakemarkkinoita odotusten suhteen, tulisi myös kyberturvallisuuden näkyä tässä kohtaa. Kyberturvallisuuden tuottaminen ja ylläpito on jatkuvaa toimintaa, joka yritysten ja erehdysten kautta kehittyy ja jalostuu kunkin yrityksen tarpeisiin ja haasteisiin. Yrityksen tulisi jatkuvasti kehittää

kyberturvallisuusstrategiaansa, toimintaansa ja teknologioitaan (Kim, 2007). Kybertoimintaympäristöt ovat suurilta osin yksityisten yritysten hallussa. Verkottuneiden palveluketjujen luonteesta johtuen hyökkäys yhdelle liike-elämän sektorille voi aiheuttaa ongelmia toisilla sektoreilla.

Boonen (2017) mukaan kyberturvallisuuden tulisi olla ylimmän johdon prioriteetti, sillä ylin johto on kuitenkin lopulta vastuussa kaikesta, mitä yrityksessä tapahtuu. Kyberturvallisuutta tulisi myös johtaa koko organisaation laajuisesti, keskitetysti ja johdonmukaisesti. Kyberturvallisuutta tulisi johtaa yrityksen ylimmän johdon tasolta siitäkin syystä, että mikäli liiketoimintayksiköille annetaan vastuu oman kyberturvallisuutensa toteuttamisesta, he priorisoivat liiketoimintayksikön oman ydintoimintansa kyberturvallisuuden toteuttamisen edelle. Ylimmän johdon sitoutuminen yrityksen tietoturvallisuuden hallintajärjestelmään on näkyvin tapa, jolla se osoittaa sitoutumisensa koko yrityksen tietoturvallisuuteen (von Solms & von Solms, 2004).

Von Solms (2001) mukaan yrityksen ylimmällä johdolla ei ole muuta vaihtoehtoa, kuin olla sitoutunut ja vastuullinen tietotuvallisuuden suhteen. Perusteluissaan hän vetoaa lakiin, joka edellyttää, että yrityksen johto on sitoutunut ja vastuussa hyvästä hallinnosta yrityksessään viitaten siis epäsuorasti siihen, että hyvä hallinto sisältää myös tietoturvallisuuden huomioimisen. Suomessa Osakeyhtiölakiin 2006/624 § 8 on kirjattu: “yhtiön johdon on huolellisesti toimien edistettävä yhtiön etua”. Tämän lisäksi tieto- ja kyberturvallisuuden näkökulmasta yritysten toimintaa velvoittaa muun muassa GDPR, joka ohjaa yritysjohdon sitoutumista tietosuojan ja -turvallisuuden toteuttamiseen myös sanktioilla.

Kyberturvallisuuden strategisella suunnittelulla tulee varmistaa, että yrityksen ylin johto ymmärtää täysin, miten teknologiat auttavat liiketoimintatavoitteiden saavuttamisessa ja millainen sietokyky organisaatiolla on kestää teknologiasta johtuvia menetyksiä. Tämä on suora keino sitouttaa yritysjohtoa kyberturvallisuuden huomioimiseen strategiassa (Islam & Stafford, 2017).

Yrityksien kohtaamat kyberturvallisuushaasteet liittyvät liikesalaisuuksien ja teollisen omaisuuden varastamiseen kyberhyökkäysten kautta. Siksi hallintomallin soveltaminen on välttämätöntä, jotta voidaan vaikuttaa kyberhyökkäysten torjuntaan. Kyberturvallisuudesta on tullut välttämätön vaatimus. Tehokkaan kyberturvallisuusstrategian kehittämiseksi kyberturvallisuusriskit olisi otettava huomioon työprosesseissa, ja yrityksille olisi yksilöitävä strategiset tavoitteet. Kyberturvallisuustarpeiden ja keskeisten suorituskykyindikaattoreiden asettaminen on edellytys kyberturvallisuusstrategian toteuttamiselle. Yritysjohtajien tulisi noudattaa hyväksyttyä menetelmää kyberturvallisuuden hallinnassa. (Alashi & Badi, 2020)

Tieto- ja kyberturvallisuuden johtaminen ilmenee turvallisuuspolitiikkojen määrittelynä ja toimeenpanona organisaation operatiiviseen toimintaan (Posthumus & von Solms, 2004).

Strategisen tason päätöksentekijöillä on ensisijainen vastuu tietoturvaohjelmien toteuttamisesta, organisaation laajuisten suojauskäytäntöjen julkaisemisesta ja turvallisuuspolitiikan toteutuksen valvonnasta. Heitä on tiedotettava asianmukaisesti, heille on annettava koulutusta ja tarvittavat välineet strategisten johtamisvelvollisuuksien täyttämiseksi (Garcia-Granados, 2020).

2. Kaupalliset toimijat

Accenture

Turvallisuusraportissaan 2021 Accenture näkee ennennäkemättömän epävarmuuden aikakauden, jossa laitteita on niin paljon hajallaan yritysverkoissa, että tietoturva-ammattilaisten on haastavaa pysyä vaatimusten tahdissa.

Viimeaikaiset tapahtumat sekä kiristyshaittaohjelmien toiminnan laajamittaiset häiriöt ja kustannukset kuvaavat kyberuhkatoiminnan kasvavaa vaikutusta yritysriskiin kaikilla toimialasegmenteillä. Tätä riskiä on yhä vaikeampi hallita ja lieventää sekä IT- että OT-ympäristöissä.

Vaikka virtualisointi pilvessä ja internetiin kytkettyjen laitteiden yleistyminen helpottavat teollisuusjärjestelmiä, nämä teknologiat ottavat käyttöön myös uusia haavoittuvuuksia ja riskejä. Erityisesti laitteet, kuten IoT (Internet of Things) -objektit, -kytkimet ja reitittimet, ohjaavat organisaatiossa ja organisaatiosta ulos virtaavia tietoja. IT- ja OT-ympäristöjen varmistaminen on tärkeää OT-tietoturvan kannalta, ja virheet voivat tarjota suoran pääsyn OT-ympäristöihin ohittaen it-verkot kokonaan.

Turvallisuusjohtajien on osoitettava johtoryhmille ja hallituksille ymmärtävänsä sekä toiminnan jatkuvuuden että yhteistyön merkityksen koko liiketoiminnan kanssa riskien tehokkaaksi hallitsemiseksi.

Arvio*/johtopäätös*: Accenture myy kyberturvallisuutta palveluna ja puhuttelee ict-johtoa.

Deloitte

Deloitten kyselyn perusteella joka kolmas (29 %) suomalaisista luottaa, että yritykset varmistavat koko alihankintaketjunsa vastuullisuuden. Vastaavasti 25 % ei luota yritysten varmistavan asiaa ja lähes puolet vastaajista (45 %) ei ole asiasta varma. Yrityksille ainoa seuraus sen alihankintaketjussa tapahtuvista rikkomuksista on tällä hetkellä vain mainehaitta.

Arvio*/johtopäätös*: Deloitte myy palveluna kyberturvallisuutta, korostaa riskienhallintaa.

Fujitsu

Fujitsun artikkelin perusteella tietoturvapäälliköiden on aina ollut tärkeää tuottaa arvoa yrityksen lopputulokselle. Mutta uudet vaatimukset nostavat rimaa paljon korkeammalle. Avain näihin vaatimuksiin, asiakkaiden säilyttämiseen, liiketoiminnan kasvattamiseen ja organisaatioiden turvallisuuden varmistamiseen on tietoturvastrategioiden uudelleenkalibrointi integroidumpaa, suuren kuvan ajattelua varten. Se tarkoittaa asiakkaiden tarpeiden ja liiketoimintatavoitteiden pitämistä mielessä. Se edellyttää parempaa ennakoivien tietoturvatietojen käyttöä ja nopeampia vasteaikoja sekä asiakkaille aiheutuvien riskien ymmärtämistä, jotta voidaan paremmin valmistella tietoturvatoimenpiteitä.

Vaikka riskiin ja tiedusteluun perustuva lähestymistapa turvallisuuteen edellyttää jatkuvia toimenpiteitä ja muutoksia olosuhteiden muuttuessa, seuraava etenemissuunnitelma auttaa tämän strategian laatimisessa:

1. Aloita liiketoimintatavoitteistasi
2. Mieti sitten, miten turvallisuus mahdollistaa nämä tavoitteet.

3. Määritä tämän perusteella tietoturvatavoitteesi versus suuremmat liiketoimintatavoitteet.
4. Huomioi myös muut projektit, ohjelmat ja sovellukset, jotka voisivat tulla käyttöön.
5. Toinen tärkeä askel on tunnistaa mahdolliset sidosryhmät, joilla voi olla sananvaltaa tietoturvamuutoksessasi.
6. Mieti sitten, mitä muita toimia tarvitaan sen varmistamiseksi, että turvallisuustavoitteesi saavutetaan.
7. Tämän jälkeen voit määrittää tietyt tulokset, jotka haluat saavuttaa työskennellessäsi liiketoiminta- ja turvallisuustavoitteiden saavuttamiseksi.
8. Kun noudatat tätä etenemissuunnitelmaa, muista seurata, miten tavoitteiden ja tulosten saavuttaminen voi vaikuttaa turvallisuusoperaatiosi kypsyyteen.
9. Päätä lopuksi, miten tietoturvaorganisaatiosi seuraa ja mittaa edistymistä liiketoimintatavoitteiden saavuttamisessa.

Seuraavan sukupolven CISO:iden on siirryttävä lähemmäs liiketoiminnan johtamista. Sen on ymmärrettävä perusteellisesti liiketoimintaprosesseja, määräyksiä ja riskejä, jotka eivät ole pelkkää teknologiaa. Yritysturvallisuuden perusrooli säilyy aina samana: asiakkaiden ja muiden sidosryhmien luottamuksen varmistaminen ja säilyttäminen, jotta yritys voi pysyä liiketoiminnassa ja jatkaa kasvuaan.

Arvio/johtopäätös: Fujitsu puhuttelee CISOa laajentuneesta toimenkuvasta ja miten puhuttelee ylempää johtoa. Samalla annetaan toimintamalliin liittyviä suosituksien oman toiminnan kehittämiseen.

Gardner

Panetta (2020a) näkee haasteena, että yrityksen johto näkee investointien jatkuvan tarpeen negatiivisena asiana. Siksi turvallisuusinvestointien perustelut tulee tehdä viiteen kysymykseen heidän omalla kielellään, liiketoiminnan käsitteiden avulla vastattuna.

Olemmeko 100 % turvassa? Vuonna 2019 Gartnerin turvallisuus- ja riskijohtajien kysely osoitti, että neljä viidestä vastaajasta totesi riskin vaikuttavan hallituksen päätöksiin.

Yksittäisten tavoitteiden ja huolenaiheiden lisäksi hallitukset huolehtivat yleensä kolmesta asiasta:

1. Tulot/operaatio: Liiketoiminnan tai ei -toiminnalliset tulot ja tehostamattomat tulotavoitteet
2. Kustannukset: Kustannusten välttäminen tulevaisuudessa ja toimintamenojen välitön aleneminen
3. Riski: Rahoitus, markkinat, säännösten noudattaminen ja turvallisuus, innovointi, brändi ja maine

Useimmat hallituksen kysymykset voidaan luokitella viiteen alueeseen.

1. Tapahtumakysymys (Kuinka tämä tapahtui? Luulin, että hallitsit tämän? Mikä meni pieleen?)
2. Kompromissikysymys (Olemmeko 100 % turvassa? Oletko varma?)

3. Ympäristökysymys (Kuinka huono tilanne on? Entä mitä tapahtui X-yrityksessä? Miten meitä verrataan muihin?)
4. Riskikysymys (Tiedämmekö, mitkä riskimme ovat? Mikä pitää sinut hereillä yöllä?)
5. Suorituskykykysymys (Jaammeko resursseja asianmukaisesti? Käytämmekö tarpeeksi? Miksi käytämme niin paljon?)

Lisäksi tulisi kiinnittää huomiota seuraaviin aiheisiin:

1. Siirtyminen reaktiivisesta aktiiviseen sitoutumiseen yritysten sidosryhmien kanssa
2. Luodaan oikeat osaamisalueet vastaamaan sidosryhmien odotuksia ja ylitetään ne
3. Kehitetään suhteiden hallintaa osaamisena, ei vain roolina

Toisessa esityksessään Panetta (2020b) pitää erittäin tärkeänä, että turvallisuus- ja riskienhallintajohtajat toimittavat hallitukselle käyttöön sopivaa sisältöä, joka ei sisällä liian teknistä tietoa.

Heidän tulee varmistaa, että esitys vastaa keskeisiin kysymyksiin siitä, miten kyberturvallisuus tukee yrityksen päätehtävää ja liiketoimintaa, ottaa huomioon ympäristötekijöitä ja missä määrin olennaisia riskejä hallitaan.

Määrittelee esitystavan johtoryhmälle tai hallitukselle:

1. Avaintekijät: Liitetoiminta, materiaali riskit, ympäristöriskit/tapahtumat, vaikutus strategiaan
2. Vaikutukset (esim. liikennevalomalli): Talous, asiakas, tuotanto, oppiminen ja kasvu
3. Seuraavat toimenpiteet (miten avaintekijöihin vastataan)

Arvio/johtopäätös: Ei ole turvallisuuden johtamisen toimintamalli, vaan avustaa turvallisuudesta vastuussa olevia johtajia vastaamaan ylemmän johdon hankaliin kysymyksiin, käyttäen esimerkiksi BSC-pohjaa.

IBM

IBM näkee liiketoiminnan haasteet riskienhallinnan kautta. IBM auttaa asiakastaan saavuttamaan tietoturvatavoitteet arvioimalla, vähentämällä ja hallitsemalla riskejä. Tarjottujen palveluiden lista on pitkä ja kattava:

Hallituksen neuvontapalvelut**:** perusohjeet, riskinottokyvyt, turvatoimet ja hallituksen raportointi.

Turvallisuusriskin kvantifiointi**:** Tietoturvariskien hallinnan yhdistäminen yleiseen liiketoimintastrategiaan integroimalla tietoturvatiedot sektorikohtaisiin, kvantifioituihin liiketoimintariskeihin ja mittareihin. Priorisoi turvallisuusriskit asiayhteydessä ja välittää suojausinvestointien tuotto liiketoiminnalle.

Fuusiot, yrityskaupat, investoinnit, turvallisuusriskien arvioinnit**:** Datan ja tietoturvan merkitys edellyttää, että hankintakohteen tietoturvaohjelmasta ja riskistä on ymmärrys.

Se on otettava huomioon hankintaan liittyvissä näkökohdissa, ja sitä on tarkasteltava suhteessa jälkihankinnan korjaamiseen, hankintamenoon, ajoitukseen ja riskitoimiin.

Multi cloud -tietoturvastrategia ja yhteensopivuus: Tarjoaa jatkuvia näkyvyys-, havaitsemis- ja korjausominaisuuksia koko julkisessa pilviympäristössä, joka on integroitu uhkatiedustelu- ja hallintajärjestelmiin.

Tietosuojastrategia ja riskiohjelmapalvelut: Kattava tietosuojapalvelua, jonka avulla voidaan arvioida tietosuojariskejä ja saada tietoa yrityksen tietosuoja- ja vaatimustenmukaisuusriskien vähentämisestä.

Säädösten noudattaminen ja hallinnointi: Kyky osoittaa, että NIST SP-800:n ja Euroopan unionin direktiivin kaltaisia säännöksiä koskeva turvallisuusriskien arviointi on säädösten mukaista, ja sen jälkeen on täytäntöönpanoprosessien täytäntöönpano vaatimusten noudattamiseen liittyvien riskien vähentämiseksi.

Kolmannen osapuolen turvallisuusriskien arviointi ja hallinta: Hallitaan ennakoivasti kolmannen osapuolen tietoturvariskiä suunnittelemalla ja rakentamalla parhaita käytäntöjä tietoturva- ja yksityisyysriskien arvioimiseksi liiketoiminnan aikana ja vaihtamalla tietoja kolmansien osapuolten kanssa.

GRC-strategia ja automaatio: Arviointi asiakkaiden hallinto-, riski- ja vaatimustenmukaisuusohjelmasta ja laaditaan automaation etenemissuunnitelma, autetaan järjestelmäintegraatiossa sekä hallitaan ja käytetään GRC-alustoja.

Kriittisen infrastruktuurin suojaus: Autetaan asiakkaita, jotka käyttävät teollisuuden ohjausjärjestelmiä tai muita operatiivisia teknologioita päivittämällä infrastruktuurin kyberturvallisuutta, mukaan lukien kriittiset resurssit, järjestelmät ja verkot.

SAP-tietoturvastrategia ja arvioinnit: Kehitetään mukautettua tietoturvastrategiaa, joka sopii asiakkaalle. Hankitaan yrityksen laajuinen käsitys riski- ja compliance-toiminnoista ja siitä, miten ne vaikuttavat kokonaisriskiin.

Työntekijöiden tietoturvatietoisuuden hallinta: Kattavan ohjelman kehittäminen ja turvallisuustietoisuuden ja tietojenkalastelukoulutuksen jatkuva mukautuminen, jotta voidaan edistää riskitietoista kulttuuria, valmistaa työvoimaa suojaamaan organisaatiotaan kohdennetuilta hyökkäyksiltä ja noudattaa niitä.

Arvio/johtopäätös: IBM myy kyberturvallisuutta palveluna ja puhuttelee yritysjohtoa ja ict-johtoa. Varsinaiset mallit eivät ole nähtävissä, vaan muotoutuvat asiakkaiden tilanteiden ja tarpeiden mukaisesti.

KPMG

KPMG:n esiin tuomat pääkohdat ovat:

- Kyberriskeillä on oikeita vaikutuksia liiketoimintaan ja fyysisen maailman tapahtumiin.
- Kyberturvallisuus ei ratkea yhdellä tuotteella, ratkaisulla tai palvelulla.
- Kyberturvallisuus luodaan tekemällä asioita pitkäjänteisesti ja suunnitelmallisesti.

Lähestymistapa perustuu yhteistyöhön asiakkaan kanssa, kun etsitään organisaation tarpeisiin sopivia tietoturvaratkaisuja

Tyypillisimmät heidän asiakkaiden tarpeet ja projektit liittyvät:

- Tietoturvallisuuden, tietosuojan ja digitaalisen identiteetinhallinnan strategioiden ja hallintamallien kehittämiseen ja tarkastamiseen
- Muutos- ja kehityshankkeiden tukeen ja läpiviemiseen
- Erilaisten suojaratkaisujen suunnitteluun, käyttöönottoon ja auditointiin
- Tietomurtoihin ja tietovuotoihin varautumiseen, tutkimiseen sekä vahinkojen rajaamiseen.

Arvio/johtopäätös: KPMG myy palveluna kyberturvallisuutta yrityksille, käytettävien toimintamallien sisältö jää avoimeksi. Ylläpitää kyberturvallisuusasiaa blogeilla.

TietoEVRY

TietoEVRYn mukaan ”hyvä turvallisuus rakentaa luottamusta”. Kyberturvallisuus on välttämätöntä yrityksen pyörittämisen ja kehittämisen kannalta. Hyvän turvallisuuden ylläpitäminen on päättymätön prosessi. Kun tehdään muutoksia, on myös tarkasteltava, miten ne vaikuttavat turvallisuuteen. On tärkeää, että johtajalla on kokonaisvaltainen näkemys yrityksen turvallisuustilanteesta.

Kyseisessä oppaassa luodaan yleiskatsaus:

1. Miksi kyberturvallisuus on tärkeämpää kuin koskaan ennen
2. Näkyvyyden, yksinkertaisuuden ja suojauksen tärkeä triadi
3. Kyberturvallisuuden merkittävimmät trendit
4. Miten tietoturva sopii yhteen it:n kanssa
5. Ensisijaiset turvallisuusalueet
6. Miten me TietoEVRY:llä tarkastelemme tietoturvaa

Vain muutama vuosi sitten kyberturvallisuudesta keskustelivat enimmäkseen vain IT-ihmiset. Nykyisin on vaikea löytää toimitusjohtajaa tai talousjohtajaa, jolla ei ole turvallisuutta korkealla asialistallaan. Se on valtava muutos. Näkymä on paljon kokonaisvaltaisempi. Turvallisuus on olennainen osa kaikkea yritystoimintaa.

Pohjimmiltaan kyse on kahdesta asiasta: liiketoimintaan vaikuttavien riskien perusteellisesta arvioinnista ja luottamusverkoston rakentamisesta. Asian ydin on se, että digitaalisen liiketoimintaan harjoittaakseen tarvitaan tervettä kyberturvallisuutta.

Arvio/johtopäätös: TietoEVRYn sanoma on kohdennettu yrityksen johdolle, ehkä tietoturvajohtajan kautta. Selkeä motiivi oppaalle on kyberturvallisuustietoisuuden jakaminen, mutta erityisesti kiinnostavuuden lisääminen heidän palveluihinsa.

3. Julkishallinnolliset toimijat

Traficom

Kansallinen turvallisuusviranomainen on julkaissut standardinomaisen ”Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille”. Katakri 2020 on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset.

Katakri on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen. Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittelyympäristölle asetetut turvallisuusvaatimukset.

Turvallisuusjohtamisen osa-alueessa käsitellään niitä menetelmiä, joilla turvallisuus ja sen hallinta jalkautetaan osaksi koko organisaation toimintaa. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi, että viranomaisen turvallisuusluokiteltuja tietoja käsittelevä henkilöstö toimii asianmukaisesti.

Arvio/johtopäätös: Johdon tuki, ohjaus ja vastuu ilmenevät sillä, että organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation tietoturvallisuustoimenpiteiden kytkeytymistä organisaation toimintaan. Tällä osoitetaan, että johto on sitoutunut organisaation turvallisuusperiaatteisiin ja periaatteet edustavat johdon tahtotilaa sekä tukevat organisaation toimintaa. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina, osana yleisiä toimintaperiaatteita, politiikkaa tai **strategiaa**.

Kyberturvallisuuskeskus

Kyberturvallisuuskeskus on julkaissut vuonna 2020 oppaan ”Kyberturvallisuus ja yrityksen hallituksen vastuu”, joka antaa yritysten hallituksille työkaluja ja tukea oman organisaation kyberturvallisuuden edistämiseen keskittymättä teknologiaan, auttaa hallituksen jäseniä kysymään oikeat ja kriittiset kysymykset johdolta ja henkilöstöltä.

Opas on suunnattu erityisesti suurten ja keskisuurten organisaatioiden hallitusten jäsenille, mutta se toimii myös kyberturvallisuudesta vastaavien henkilöiden arjen työkaluna. Sisällön kohteena on sisäinen ja ulkoinen kyberturvallisuus.

Toimintamalli:

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

Arvio/johtopäätös: Tässä oppaassa kyberturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla organisaatio suojaa liiketoiminnassa tarvittavat järjestelmät, ohjelmistot, laitteet ja tietoliikenneyhteydet kyberuhkilta. Ajatuksena on perinteinen asetelma: ulkoiset uhat ja sisäinen suojaus. Tosin lopussa avataan myös liiketoimintasuhteisiin liittyvää riskien hallintaa.

Kyberturvallisuuskeskus julkaisi toisen oppaan vuonna 2021 nimellä ”Pienyritysten kyberturvallisuusopas”, joka auttaa pienyrittäjiä ja pienyrityksiä – alle 50 työntekijän yrityksiä – suojautumaan yleisimpiä kyberuhkia vastaan. Pienyrityksiin kohdistuvat kyberuhkat voivat toteutuessaan aiheuttaa yritystoiminnalle merkittävää haittaa ja pahimmillaan johtaa liiketoiminnan keskeytymiseen. Oppaaseen on kerätty muutamia yleisimpiä yritysten kyberturvallisuutta vaarantavia tekijöitä, sekä keinoja suojautua niitä vastaan.

Arvio/johtopäätös: Opas on hyvä koonnos kyberturvallisuuteen liittyvistä käytännön toimenpiteistä yrityksessä. Se ei kuitenkaan käsittele strategian tai politiikan tekemiseen liittyviä kysymyksiä.

SFS

ISO/IEC 27000 Tietoturvallisuuden standardisarja kuvaa, miten tietoturvallisuuden johtamisjärjestelmällä organisaatio suojaa tieto-omaisuuttaan. Standardisarja tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin, kun rakennetaan johtamisjärjestelmää.

SFS-EN ISO/IEC 27001:2017 on tietoturvallisuuden hallintajärjestelmän päästandardi, jossa esitetään tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset. Standardi sisältää myös organisaation tarpeisiin mukautettua tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. Vaatimukset ovat yleisluonteisia ja ne soveltuvat kaikentyyppisille ja -kokoisille organisaatioille.

ISO 27001:n keskeiset vaatimukset ovat:

1. Toimintaympäristön määritys
2. Suojattava omaisuus
3. Johtajuus
4. Tietoturvapolitiikka
5. Riskienhallinta
6. Soveltuvuuslausunto
7. Dokumentaatio
8. Mittarit
9. Auditoinnit ja johdon katselmukset
10. Jatkuva parantaminen

Arvio/johtopäätös: Standardisarja on kattava kuvaus niistä vaatimuksista, mitä järjestelmän rakentaminen vaatii. Yritykselle itselleen jää vastuu toteutuksen laajuudesta ja toimeenpanosta. Markkinat vaativat yhä useammin standardin sertifiointia.

4. Tieteelliset toimijat

Jyväskylän yliopisto

Vidgrenin (2019) tutkimus on selkeä kuvaus aiheesta ”Kyberturvallisuus yritysstrategiassa”. Yritysjohdon tärkeimpänä työkaluna yrityksen ohjaamiseen on yritysstrategia, joka on yrityksen kattavin kokonaissuunnitelma siitä, miten yritys suorittaa kokonaistehtäväänsä, eli missiota. Tutkielman tarkoituksena oli selvittää, miten kyberturvallisuus ilmenee yritysstrategiassa ja millaisia hyötyjä kyberturvallisuuden integroinnilla yritysstrategiaan voidaan saavuttaa.

Tutkijan keskeisenä johtopäätöksenä todetaan, että kyberturvallisuuden implementointi yrityksen kokonaisstrategiaan

1. viestii tehokkaalla tavalla koko yritysorganisaation henkilöstölle, että ylin johto on vastuullisesti sitoutunut yrityksen kyberturvallisuuden jatkuvaan ylläpitoon ja kehittämiseen
2. parantaa suojausta kyberhyökkäyksiä vastaan
3. ylläpitää toimintakykyä muuttuvissa olosuhteissa, valmiutta kohdata häiriöitä ja kriisejä
4. parantaa koko organisaation tasoista tietoisuutta yrityksen kyberturvallisuudesta
5. parantaa yritysimagoa ja sitä kautta vaikuttaa yrityksen arvostukseen myös osakemarkkinoilla.

Yritysjohdon tulee yksiselitteisesti ymmärtää turvallisuuden ja resilienssin avaintekijät sekä hyväksyä luottamustehtäviensä sisältämät vastuukysymykset. Tehtäviensä hoitamiseen johtajat tarvitsevat koulutusta, joka tarjoaa riittävästi tietoa ja ymmärrystä kyberturvallisuudesta, yrityksen kyvystä ylläpitää toimintakykyä muuttuvissa olosuhteissa, valmiudesta kohdata häiriöitä ja kriisejä sekä toiminnan palautumisesta. Johtajien tulee ymmärtää myös kyberturvallisuusriskien oikeudelliset vaikutukset.

Arvio/johtopäätös: Hyvä ja ytimekäs katsaus, hyvät johtopäätökset.

Tammelinin (2021) tutkimuksessa ”Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa” tutkittiin kahta onnistunutta kyberhyökkäystä ja selvitettiin, miten kaupunkien tietoturvapolitiikka vaikutti hyökkäysten torjuntaan, rajaamiseen sekä niistä palautumiseen, eli auttoiko tutkimuskohteissa muodostettu tietoturvastrategia ja -politiikka kyberhyökkäyksen torjunnassa, mikä oli niiden merkitys kyberhyökkäyksen rajaamisessa sekä selvittämisessä ja kehittyykö strategia ja politiikka hyökkäyksen jälkeen.

Molemmilla kaupungeilla oli muodostettu tietoturvapolitiikka, mutta **ei strategiaa**.

Tietoturvastrategia kertoo, miten organisaation tavoitteisiin päästään. Tavoitteet tulevat joko organisaation liiketoimintastrategiasta tai voidaan muodostaa tietoturvallisuuden tavoitteita erikseen määrittämällä.

Suomessa tietoturva rakennetaan tietoturvariskien tunnistamisen pohjalle. Tietoturvastrategialla tarkoitetaan johdon linjausta siitä, mitkä ovat tietoturvan tavoitteet ja keinot, joilla näihin pyritään. Tietoturvastrategia rakentuu osaksi toimintastrategiaa.

ISO27001 itsessään ei ole tietoturvallisuuden hallintajärjestelmä vaan kuvaus sen vaatimuksista. Standardi kuvaa vaatimukset organisaatioin ylimmän johdon sekä tietoturvapolitiikan muodostavat ja toteuttavan tason näkökulmasta.

Kyberhyökkäyksen selvittämisestä olennaisimpina nousivat esiin omien fyysisten ja loogisten verkkojen tuntemus, yhteyshenkilön merkitys sekä varautumissuunnitelma.

Merkittävää on, ettei yksikään kohdeorganisaatio ollut tehnyt erillistä tietoturvastrategiaa ohjaamaan ja resursoimaan tietoturvan toteuttamista. Kaikissa kohdeorganisaatioissa oli päädytty ratkaisuun, **jossa tietoturvapolitiikkaan oli kirjoitettu sisälle strategiatyyppiset linjaukset**.

Arvio/johtopäätös: Kattava selvitys tapahtuneista kyberrikoksista.

5. Johtopäätökset

Johtopäätöksenä kaupallisten toimijoiden aineistoista voidaan todeta, että

1. ensisijaisesti viestinnän kohderyhmänä on tietoturva- ja ict-johto
2. korostetaan riskienhallintaa
3. annetaan työkaluja tietoturva- ja ict-johdolle kertoa turvallisuudesta ylimmälle johdolle liiketoimintakielellä
4. joidenkin osalta annetaan toimenpideohjeita oman toiminnan kehittämiseen
5. kaikkien tarkoituksena on myydä kyberturvallisuuspalveluja, palvelujen sisältö sovitaan asiakkaan kanssa
6. varsinaisia malleja kyberstrategioiden sisältämiseksi ei esiinny, mutta on tulkittavissa niiden sisältyvän mahdollisiin yhteistyöprojekteihin asiakkaan tarpeiden mukaisesti

Kyberturvallisuuskeskus on tuottanut 2 hyvää opasta yritysten käyttöön. Toinen ohjaa isompien yritysten ajattelua kyberturvallisuuteen kysymysten asettelun kautta. Toinen taas pienempien yritysten käytännön toimenpiteiden huomioimista. Molemmissa tapauksissa vastuu on yrityksellä itsellään laittaa kyberturvallisuus ajan tasalle.

Tiedeyhteisö tukee strategisen tason tutkimusta, mutta toistaiseksi tämän aihepiirin tutkimuksia on lukumääräisesti vähän Suomessa. Laajemmin tarkasteltuna hallintomallien (governance) käsittely on toimialakohtaista ja perustuu usein olemassa olevien standardien (esim. ISO27001) käyttöön tai soveltamiseen. Vidgrenin tutkimus on aiheeltaan tämänkin tutkimuksen mukainen ja antaa parhaat tulokset jatkon kannalta tarkasteltuna.

Tulokset

1. Nettikyselyn tulokset

Yrityksen strategiset tavoitteet

Yrityksen kokonaistoiminnan näkökulmasta tuotanto- ja palvelutoiminnalle on asetettu tehokkuustavoitteet sekä tuotteille ja palveluille digiturvallisuustavoitteita. Yrityksen strategiassa (tai vastaavassa) on asetettu keskeiset tavoitteet turvallisuuden osatekijöille pl. kyberturvallisuus.

Strategisten tavoitteiden näkökulmasta puutteita on seuraavissa kokonaisuuksissa:

- Yrityksen digitalisaatioon liittyvät mahdollisuudet ja menestystekijät.
- Digiturvallisuudelle asetetut taloudelliset tavoitteet.
- Kyberturvallisuuden tehokkuusvaatimukset (kustannus - vaikuttavuus).

  Esimerkkejä sanallisista vastauksista:

  1. *Ajatuksellisesti on, mutta sitä ei ole kirjoitettu suoraan kustannusvaikuttavuutta arvioiden.*
  2. *Joitain mittareita on mutta vähemmän liittyen kustannus/tehokkuus/vaikuttavuus puolelle.*
  3. *Suoranaisia tehokkuusvaatimuksia ei ole, mutta tiekartan edistymistä ja riskien mitigoimista seurataan hyvinkin tarkasti*

Yrityksen strategioiden toteutumisen turvaaminen

Yrityksillä on säännöllinen ja toimiva strategiaprosessi tai toimintamalli yrityksen strategian (tai vastaavan tason ohjauksen) laatimiseen. Yrityksillä on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi. Yrityksen strategian (tai vastaavan) laatimisesta vastaa yleisimmin toimitusjohtaja / johtoryhmä.

Yleisesti voidaan todeta, että yrityksillä tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa. Yrityksillä on toteuttamiskelpoinen varautumisen ja jatkuvuuden hallinnan suunnitelma, sekä näihin liittyvä häiriö- ja kriisitilanteiden viestintäsuunnitelma.

Yrityksen johto on sitoutunut digitaalisen turvallisuuden kehittämiseen. Toimeenpanoon käytetään johdon hyväksymää tietoturvapolitiikkaa tai vastaava tietoturvallisuuden toteuttamista ohjaavaa asiakirjaa. Yrityksellä on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.

Strategiatyössä on määritelty viestinnän linjaukset ja avoimuusperiaatteet mahdollisen kriisitilanteen varalta. Yrityksissä viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko yrityksen laajuisesti.

Kehitettävää

- strategiatyön laadinnassa tulisi käyttää standardoitua tai muuta vastaavaa menettelyä.

- yksittäisillä yrityksellä ei ole kykyä arvioida riittävä resurssointi ja budjetti digi- ja kyberturvallisuuteen.
- Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja ei tehdä säännöllisesti.

Esimerkkejä sanallisista vastauksista:

1. *Ketteryyttä ja kokeilullista toimintatapaa. Digitalisaation mahdollisuuksien hyödyntäminen.*
2. *digitalisaatioasteen nostaminen ja asiakaskokemuksen parantaminen (helppokäyttöisyyden lisääminen)*
3. *ICT strategia omana kokonaisuutena yrityksen strategiassa*
4. *Yrityksen strategiassa ei välttämättä juurikaan puhuta tietoturvasta, mutta yrityksen turvallisuus-/tietoturvatoiminta perustuu yrityksen strategian toteuttamiseen.*
5. *Moni asia on mietitty ja toteutettu muuten, mutta EI strategiatyössä. Esim. viestinnän linjaukset.*

Yrityksen ympäristöanalyysit

Kyselyn perusteella voidaan todeta, että yritykset tekevät digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt (kyberturvallisuus), toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.

Yritykset kartoittavat digitaalista turvallisuutta ohjaavaa lainsäädäntöä ja tunnistavat siitä aiheutuvat velvoitteet. Samoin kartoitetaan keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.

Yrityksessä on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten yritysten tai yhteiskunnan toimintaan. Yrityksellä on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta yrityksen toimintaan.

Kehitettävää PK-yritysten ja pienempien osalta

- menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät uhkatekijät.
- kyberturvallisuuskatsauksien (tilannekuva) hyödyntäminen strategisessa suunnittelussa.

Yrityksen sisäisen tehokkuuden analyysi

Vastausten mukaan yrityksillä on riittävästi osaavaa henkilöstöä kyberturvallisuuden eri osa-alueilla. Heillä on riittävät resurssit ja osaaminen digitaalisen turvallisuuden ylläpitoon ja kehittämiseen osana yrityksen prosesseja, toimintamalleja ja järjestelmiä.

Yrityksen digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia. Yrityksissä kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella. Yrityksillä on kyky valita toiminnan edellyttämät kyberturvalliset teknologiat.

Yrityksessä tietoturvasta ja tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi.

Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa, (toimitusketjun hallinta).

Yrityksellä on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti yrityksen johdolle.

Kehitettävää PK-yritysten ja pienempien osalta

- digitaaliseen turvallisuuteen liittyvien mittareiden määrittäminen
- auditointien säännöllistäminen tietoturvallisuuteen ja tietojärjestelmiin.
- harjoitustoiminta säännölliseksi toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista varten.

Kyselyn tulokset graafisessa muodossa on liitteessä 4 (erillinen tiedosto: STRATEGIA22 Kyselyn tulokset.pdf).

2. Haastattelutulokset

Yrityksen strategiset tavoitteet

Konkreettisimmillaan yritys huomioi strategiset tavoitteet kirjoittamalla ne strategiaan tai kyberstrategiaan esimerkiksi ”tuotantovarmuutta kehitetty kyberturvallisen toimintatavan avulla” tai ” halutaan turvata turvallinen palvelukokemus”. Toisena käytettynä vaihtoehtona on välillinen jatkuvuuden hallinta ja jatkuvuuden turvaaminen.

Yrityksen hallituksilla on puutteita kyberturvallisuuden osaamisessa. Vastuu asioista on yleensä esittelijöillä. Toisaalta tähän vaikuttaa myös toimialan regulaatiot, jolloin osaamista on olemassa tai on oltava toimialan säännöstön perusteella. Yleensä alkuvaiheessa vastuut yrityksessä ovat olleet epämääräiset, mutta tietoisuus ja kiinnostus kyberturvallisuudesta selvästi noussut ja kasvanut. Edistyneimmillä on digijohtaja johtoryhmän jäsenenä tuomassa osaamista asioiden hallintaan.

Toimenpiteiden tehokkuus varmistetaan operatiivisella harjoittelulla toimialoittain, sisäisten ja ulkoisten auditointien perusteella laaditaan kehittämiskohteet. Useimmilla yrityksillä on käytössään riskipohjainen toimintamalli, jossa johdon päätökset tehdään riskien kautta yhteistoiminnassa liiketoimintaosapuolen kanssa, keskitytään kriittisiin tekijöihin. Toimintaan liittyy hyvät kumppanit, sovitut periaatteet, riskienhallinta ml. ulkopuoliset kumppanit. Koulutus on useimmilla vielä kesken.

Kyberuhkia seurataan monien kanavien kautta. Joillakin voi olla uhkatiedustelu osana organisaatiota, yleisimmin toimialakohtainen yhteistoiminta ja verkostoituminen tuottaa suurimman osan, lisäksi tiivis yhteistyö Kyberturvallisuuskeskuksen kanssa. Raportointi johdolle tapahtuu yleisemmin viikoittain tai kuukausittain tilanteen mukaan. Säännöllisimmin kerran kuukaudessa.

Kyberturvallisuus on jo nyt kilpailuetu. Se on osoitettu käytännössä liiketoimintaetuna kilpailutilanteissa, kun vaaditaan sertifikaattia tai vastaavaa, joka on tuotava esille tarjouksissa. Jos tuotteet ovat osittain ”monopolituotteita”, kyberturvallisuus vaaditaan toimitusvarmuuden ja yhteiskuntavastuun kautta. Myös hyvä asiakaskokemus liittyy tähän.

Lopuksi voidaan todeta, että kyberturvallisuus on liiketoiminnan ajatusmallin muutos (ei pelkkää teknologiaa), kyberturvallisuus on käsiteltävä liiketoimintariskinä. Se on myös tapa johtaa. Strategiatavoitteen jalkauttaminen koetaan tärkeänä arvona. Tietoturva on haasteellista, osaaminen ostettuna on kallista, mutta siitä huolimatta useat yritykset ostavat sen palveluna. Erilaiset kumppanuusohjelmat nähdään tärkeänä osana yrityksen toimintaa, erityisesti jos ne ovat viranomaisten järjestämiä (uskottavuus). Myös yrityksen toimialan regulaatiot vaikuttavat kyberturvallisuuden tarpeeseen ja toteutukseen.

Voisiko kybertiedotus (Kyberturvallisuuskeskus) olla yhteiskunnan peruspalvelua? (vrt. esim verotus)

Strategioiden toteutumisen turvaaminen

Yritykset käyttävät toiminnassaan riskienhallintamenetelmiä, joissa arvioidaan riski, niiden euromääräinen vaikutus ja merkitys liiketoimintaan. Kyberturvallisuus on osa liiketoimintariskien arviointia. Tuloksista raportoidaan keskimäärin kerran kuukaudessa. Arvioinnin perusteella päätetään tehtävistä toimenpiteistä.

Yrityksen tärkeimmistä tavoitteista viestitään yleensä ylemmän johdon taholta, mutta ohjauksessa on vielä kehitettävää. Asiat jalkautuvat viestinnällä, arkisina toimenpiteinä, toistaminen koetaan tärkeänä. Yksittäinen toteamus: Toimitusjohtajan ei pitäisi olla strategian laatija, hallituksen tulee vetää strategiaa.

Useimmissa yrityksissä turvallisuuskulttuuri koetaan hyväksi, joillakin perinteet ovat niin pitkät ja työn vaarallisuusaste korkea, että turvallisuus on jokapäiväinen asia. Kyber- ja tietoturva tulisi asettaa työturvallisuuden rinnalle.

Riskien rajoittamiseen yritykset käyttävät laadittuja tietoturvapoliitikkoja ja niistä johdettuja sisäisiä tarkastuksia. Palvelunhallinta ja sopimushallinta (esim. SOPIVA) on merkittäviä tekijöitä digitalisaatiossa ja toimittajan valinnassa. Se on paljolti sopimushallintaa, luottamuksen hallintaa ja keskustelua. Niillä, joilla on jokin standardi käytössä, säännöllinen ulkoinen auditointi on merkittävä tekijä.

Liiketoimintaprosessit huomioivat kyberturvallisuuden. Ei välttämättä holistisesti, mutta tässä liiketoiminnan omistaja on ratkaisevassa asemassa. Kyberturvallisuus koetaan kuitenkin tukitoimintona.

Poikkeustilanteita on yrityksissä harjoiteltu, osassa jopa toteutettu käytännössä. Vastuut ja tehtävät on kirjattu toimintamalleihin, joita myös on päivitetty.

Lopuksi voidaan todeta, että yritykset arvostavat yritysten keskinäistä ja viranomaisyhteistyötä, uhkakuvakentän avaamista (open source), jopa investointina, sekä yhteistä uhkakuvaa.

Jatkuvuuden suunnittelu, toipumissuunnitelma ja harjoittelu ovat keskeisiä elementtejä kyberturvallisuusstrategian toimeenpanossa.

Yritysten vastaukset kysymykseen: *Mikä olisi teidän yrityksenne oppi tai esimerkki, jota voisi kertoa/käyttää esimerkkinä muillekin?*

- oma uhkatietokyvykkyys ja raportointi
- johdon tuki, tuen kantajaa tarvitaan, pitkän matkan juoksu, vaatii aikaa
- toimialaringit harjoituksissa
- dokumentaation tärkeys tietojärjestelmissä
- tietoturva työturvallisuuden rinnalle, järjestelmäverkkojen säännöllinen auditointi -> kehittäminen
- strateginen taso ei ole vielä konkreettinen ”parhaiten viesti mene perille oikean tapauksen kautta”, ”oikean uhkatilanteen viestintä”

3. Tulosten johtopäätökset

Toimintasuosituksien kehittämisessä tulee huomioitava erityisesti seuraavat sisällölliset kokonaisuudet:

1. Digi- ja kyberturvallisuustavoitteet ja menestystekijät osaksi tuotteita ja palveluita
2. Digiturvallisuudelle taloudelliset/tehokkuus tavoitteet/vaatimukset
3. Strategiatyön vakiointi suuryrityksistä pienempiin, standardit ja/tai vastaavat menettelyt
4. Toimintaympäristön seuranta, PK-yritysten ja pienempien kybertilannekuvan sisältö ja laatu.
5. Riskien hallinnan ja jatkuvuuden kehittämiseen, resilienssin kasvattamiseen, digitaalisen turvallisuuden mittarit.
6. Digitaalisen turvallisuuden yhteistoiminnan kehittäminen, toimitusketjut
7. Viestinnän ja harjoittelun kehittäminen poikkeustilanteisiin liittyen

Toimintasuosituksien toimintamalli voidaan valita seuraavista erilaisista tutkimuksen osoittamista malleista:

1. Standardeihin perustuva vaatimuksia asettava normatiivinen malli
2. Keskusteluun ohjaava kysymysperusteinen malli
3. Selkeä ja käytännönläheinen ”to do -list” tyyppinen malli

Lähteet

Kirjallisuus

Accenture, Cyber threat intelligence report 2021, https://www.accenture.com/fi-en/insights/security/cyber-threat-intelligence-report-2021.

Alashi S. A., Badi D. H. (2020) The Role of Governance in Achieving Sustainable Cybersecurity for Business Corporations, Department of Information Science, King Abdulaziz University, Jeddah, Saudi Arabia.

Andrews, K. R. (1997). A reader in the resource-based perspective. Foss, N. J. (toim.), (pp. 52-59). New York, NY, United States: Oxford University Press.

Boone, A. (2017). Cyber-security must be a C-suite priority. Computer Fraud & Security, 2017(2), 13–15.

Deloitte, Yritysvastuu alihankintaketjun vastuullisuus, https://www2.deloitte.com/fi/fi/pages/risk/articles/yritysvastuu-alihankintaketjun-vastuullisuus.html

Fujitsu, Customer-first security: What it is and best practices for success, Fujistu_Customer_First_Security_Whitepaper123.pdf, fujitsu.com.

Garcia-Granados, F (2020) Cybersecurity Knowledge Requirements for Strategic Level Decision Makers, Conference Paper, Tallinn University of Technology.

Hill, A & Hill, T (2009) Manufacturing operations strategy. Palgrave Macmillan.

Leena Hiltunen, Metodina kyselytutkimus, Jyväskylän Yliopisto, 2009.

IBM, IBM Security Strategy, Risk and Compliance Services, https://www.ibm.com/downloads/cas/GKN51N92

Islam, M. & Stafford, T. (2017). Information Technology (IT) integration and cybersecurity/security: the security savviness of board of directors. 23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation.

Johnson, G., Scholes, K. & Whittington, R. (2008). Exploring corporate strategy (8. ed.). Harlow; Munich: Prentice Hall Financial Times.

Kansallinen turvallisuusviranomainen, Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille, Traficomin julkaisusarja, ISSN 2669-8757, verkkojulkaisu.

Kim, J. (2017). Cyber-security in government: reducing the risk. Computer Fraud & Security, 2017(7), 8–11.

KPMG, Kyberturva kohtaa fyysisen maailman turvallisuuden, 2021, https://home.kpmg/fi/fi/blogs/home/posts/2021/05/kyberturva-kohtaa-fyysisen-maailman-turvallisuuden.html, sekä https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologiakonsultointi/tietoturva.html

Kyberturvallisuuskeskus, Kyberturvallisuus ja yrityksen hallituksen vastuu, (alkuperäinen Cyber Security Toolkit for Boards, NCSC, 2019, ncsc.gov.uk), Kyberturvallisuuskeskus 2/2020, kyberturvallisuuskeskus.fi

Kyberturvallisuuskeskus, Pienyritysten kyberturvallisuusopas, Traficomin julkaisuja 228/2020. (Opas perustuu Australian kyberturvallisuusviranomaisen tuottamaan materiaaliin Small Business Cyber Security Guide.)

Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen, Kyberturvallisuuden strateginen johtaminen Suomessa, Maaliskuu 2018, Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 28/2018.

Kasey Panetta, 5 Security Questions Your Board Will Inevitably Ask, Gandner 12.6.2020a, varsinainen raportti Sam Olyaei ja Jeffrey Wheatman, 19.7.2019, https://www.gartner.com/smarterwithgartner/5-security-questions-board-will-definitely-ask/

Kasey Panetta, The 15-Minute, 7-Slide Security Presentation for Your Board of Directors, Gardner 18.6.2020b, https://www.gartner.com/smarterwithgartner/the-15-minute-7-slide-security-presentation-for-your-board-of-directors

Posthumus, S., von Solms, R. (2004). A framework for the governance of information security. Computers & Security, Volume 23, Issue 8, 2004, 638-646.

SFS (2021) ISO/IEC 27000 Tietoturvallisuuden standardisarja, https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

von Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, Volume 20, Issue 3, 2001, 215-218.

von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Jussi Tammelin, Tietoturvastrategia ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa, Jyväskylän yliopisto, 2021, pro gradu.

TietoEVRY, An Introduction to Cybersecurity, https://www.tietoevry.com/en/services/Cybersecurity/cybersecurity-guidebook

Jiri Vidgren, Kyberturvallisuus yritysstrategiassa, 2019, Jyväskylän yliopisto, Tietojärjestelmätiede, kandidaatintutkielma.

Haastattelut

Oyj Ahola Transport Abp	
	Vesa Ulvi, It-manager
Elisa Oyj	Jaakko Wallenius, turvallisuusjohtaja
Kuopion Energia Oy	Esa Lindholm, toimitusjohtaja
	Jami Miettinen, digijohtaja
Porasto Oy	Petri Suhonen, tietohallintojohtaja, toimitusjohtajan sijainen
Steveco Oy	Jukka Soininen, tietohallintopäällikkö
	Miikka Purhonen, tietoturvapäällikkö
Vaasan Opiskelija-asuntosäätiö	
	Marko Ylimäki, toimitusjohtaja
Wärtsilä Oyj	Teemu Eronen, kyberturvallisuusjohtaja
Anonyymi	1

Liitteet

Liite 1: Nettikyselyn kysymykset

Taustatiedot

1. Yrityksen nimi (vapaaehtoinen)

2. Yrityksen Y-tunnus (vapaaehtoinen)

3. Kyselyn yhteyshenkilö (sähköpostiosoite) (vapaaehtoinen)

4. Yrityksen toimiala (pakollinen)

   Elintarvikeala
   Energia-ala
   Finanssiala
   ICT- ja ohjelmistoala
   Kaupan- ja jakelun ala
   Logistiikka-ala
   Media-ala
   Satama- ja merenkulkualat
   Teleliikenneala
   Teollisuusala
   Terveydenhuoltoala
   Vesihuoltoala

5. Mikä on yrityksen koko henkilöstön ja/tai liikevaihdon määrän mukaisesti? (pakollinen)
   > 2000 konserni (>400 M€/v)
   > 250 suuryritys (> 50 M€/v)
   < 250 PK-yritys (< 50 M€/v)
   < 50 pienyritys (< 10 M€/v)
   < 10 mikroyritys (< 2 M€/v)

6. Kuinka paljon ovat olleet digitaalisen turvallisuuden kehittämis- ja ylläpitokustannukset vuonna 2020, arvio-tarkkuus riittää?
   0 euroa
   < 1000 euroa
   < 10 000 euroa
   < 100 000 euroa
   < 1 000 000 euroa
   > miljoona euroa

7. Mikä on yrityksen käyttämä henkilötyövuosimäärä (htv) omien ja ulkoisten henkilöiden digiturvatehtäviin vuonna 2020 (riskienhallinta, jatkuvuus ja valmius, tietoturva, kyberturva, tietosuoja), arviotarkkuus riittää?
   ___ 0-1

___ 1-2
___ 3-5
___ 5-10
___ yli 10

8. Onko yrityksessä vähintään yksi päätoiminen/oto henkilö seuraavilla digiturvallisuuden osa-alueilla? (valitse kaikki sopivat vaihtoehdot)

   päätoiminen/oto

   __ / __ riskienhallinta
   __ / __ jatkuvuus ja varautuminen
   __ / __ tietoturvallisuus
   __ / __ tietosuoja
   __ / __ kyberturvallisuus

9. Kuinka monta tuntia digitaalisen turvallisuuden koulutusta yrityksen henkilöstö on keskimäärin saanut vuonna 2020 (tuntia/henkilö), arviotarkkuus riittää?

   ___ 0
   ___ 1-2
   ___ 3-5
   ___ 5-10
   ___ yli 10

Seuraavien osioiden vastausvaihtoehdot: ei koske meitä, ei toteutettu, osittain toteutettu, täysin toteutettu (ellei toisin mainita)

Yrityksen strategiantyön lähtökohdat (painopiste)

1. Yrityksen arvot sisältävät digitaalisen turvallisuuden tekijät (Digitaalinen turvallisuus käsittää viisi osa-aluetta: riskienhallinnan, toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden, kyberturvallisuuden sekä tietosuojan.).

2. Yrityksen tuotanto- ja palvelutoiminnalle on asetettu tehokkuustavoitteet.

3. Yrityksen tuottamille tuotteille ja palveluille on asetettu digiturvallisuustavoitteet. (Digitaalisen turvallisuuden tavoitteena on suojata yrityksen toiminta niiltä riskeiltä ja uhkilta, jotka voivat kohdistua yrityksen henkilötietoihin ja tuotteisiin sekä prosesseihin, palveluihin ja tietoaineistoihin digitalisoituneessa toimintaympäristössä.)

4. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät mahdollisuudet.

5. Digiturvallisuudelle on asetettu taloudelliset tavoitteet.

6. Yrityksellä on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.

7. Yritys käyttää standardoitua tai muuta vastaavaa menettelyä strategiatyön lähtökohtana.

8. Yrityksellä on kyky arvioida riittävä resurssointi ja budjetti digi- ja kyberturvallisuuteen.

9. Yrityksellä on riittävästi osaavaa henkilöstöä kyberturvallisuuden eri osa-alueilla.

10. Yrityksellä on riittävät resurssit ja osaaminen digitaalisen turvallisuuden ylläpitoon ja kehittämiseen osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).

11. Yrityksen on tunnistanut sen liiketoiminnan kannalta kriittiset toiminnot, palvelut, tiedot, tietovarannot ja tietojärjestelmät.

    a. Jos kyllä, niin miten ne ovat vaikuttaneet esimerkiksi alihankintaketjuihin? <vapaa laatikko>

12. Kyberturvallisuudelle on määritetty tehokkuusvaatimukset (kustannus-vaikuttavuus).

    a. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki <vapaa laatikko>

13. Kuinka suuri osa yrityksen liiketoiminnasta on riippuvainen järjestelmien ja datan toimivuudesta ja digitaalisen tiedon eheydestä?

    ___ <20 %
    ___ 20-40 %
    ___ 40-60 %
    ___ 60-80 %
    ___ > 80 %

14. Yritys hyödyntää kyberturvallisuuskatsauksia (tilannekuva) strategisessa suunnittelussa.

15. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa?
    (avoin vastaustila)

Yrityksen strategiatyö

1. Yrityksellä on säännöllinen ja toimiva strategiaprosessi tai toimintamalli yrityksen strategian (tai vastaavan tason ohjauksen) laatimiseen.

2. Yrityksen strategian (tai vastaavan) laatimisesta vastaa

    a. hallituksen puheenjohtaja / hallitus
    b. toimitusjohtaja / johtoryhmä
    c. strategiapäällikkö (vast)
    d. ei kukaan

3. Strategian (tai mission) perusteella yrityksen digitalisaatio liittyy (valitse tarvittaessa useampi)

    a. alustatalouteen (verkkokauppaan)
    b. hallintopalvelut (taloushallinto, henkilöstöhallinto)
    c. viestintään ja etätyöhön (sosiaalinen media, verkkokokoukset, etäjohtaminen)
    d. pilvipalveluihin (hajautetut järjestelmät)
    e. yrityksen operatiiviseen toimintaan
    f. toimitusketjuihin (liiketoimintamallit)
    g. yrityksen tuotteisiin ja palveluihin

4. Strategiatyössä on asetettu tavoitteet yrityksen

    a. taloudelle
    b. tuotteille ja palveluille
    c. tuotantotoiminnalle
    d. henkilöstön osaamiselle
    e. digitalisaatioasteelle
    f. toiminnan jatkuvuudelle (resilienssi)

    g. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? <vapaa laatikko>

5. Yrityksen strategiassa (tai vastaavassa) on asetettu tavoitteet turvallisuuden osatekijöille:

    a. yleiset vaatimukset
    b. henkilöstöturvallisuus
    c. tilaturvallisuus
    d. työturvallisuus
    e. tietoturvallisuus
    f. kyberturvallisuus

    g. Jos johonkin em kyllä, niin millaisia tavoitteita on asetettu? <vapaa laatikko>

6. Yrityksen liiketoimintastrategiassa on määritetty digitaaliset menestystekijät.

    a. Jos kyllä, niin millaisia menestystekijöitä on määritetty? <vapaa laatikko>

7. Yrityksen johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.

8. Strategiatyössä on menettely, jolla voidaan tunnistaa yrityksen digitalisaatioon liittyvät uhkatekijät.

9. Strategiatyössä on määritelty viestinnän linjaukset ja avoimuusperiaatteet mahdollisen kriisitilanteen varalta.

10. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa? (avoin vastaustila)

Yrityksen strategian toimeenpano ja tulosten mittaaminen

1. Yrityksen digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti hyödyntäen yhtä tai useampaa selkeää prosessia tai hallintamallia.

2. Yrityksellä on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.

3. Yrityksellä on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.

4. Yrityksellä on menettely, jolla se seuraa toimintaympäristössä tapahtuvia ilmiöitä ja arvioi niiden vaikutusta yrityksen toimintaan.

5. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa, (toimitusketjun hallinta).

6. Yrityksellä on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.

7. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti yrityksen johdolle.

8. Yrityksessä viestitään digiturvallisuuden riskitilanteesta ja uusista riskeistä koko yrityksen laajuisesti.

9. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.

10. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta ja henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.

11. Yritys harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.

12. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella.

13. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa? (avoin vastaustila)

Yrityksen digi- ja kyberturvallisuustoimenpiteiden nykytilanne

1. Yrityksen tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.

2. Yrityksellä on strategiaprosessi, joka huomioi kyberympäristön vaikutukset omaan liiketoimintastrategiaan.

    a. Anna toteutuksesta esimerkki <vapaa laatikko>

3. Yritys on huomioinut digitaalisen turvallisuuden osana yrityksen prosesseja, toimintamalleja ja järjestelmiä (kokonaisarkkitehtuuria).

4. Yritys tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt (kyberturvallisuus), toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.

5. Yritys on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.

6. Yritys on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.

7. Yrityksessä on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten yritysten tai yhteiskunnan toimintaan.

8. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.

9. Yrityksessä on määritelty digitaaliseen turvallisuuteen liittyvät mittarit, joiden avulla yritys voi seurata osa-alueiden kehittymistä.

10. Yrityksessä kehitetään riskienhallintaprosessia riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.

11. Yrityksellä on kyky valita toiminnan edellyttämät kyberturvalliset teknologiat.

12. Yrityksen tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.

13. Yrityksellä on toteuttamiskelpoinen varautumisen ja jatkuvuuden hallinnan suunnitelma.

    a. Jos kyllä, niin anna toteutuksesta lyhyt digi- ja kyberturvallisuusesimerkki <vapaa laatikko>

14. Yrityksellä on häiriö- ja kriisitilanteiden viestintäsuunnitelma.

15. Yrityksessä tietoturvasta ja tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi.

16. Kuinka moneen digitaaliseen turvallisuuteen liittyvään harjoitukseen yritys on osallistunut vuoden 2020 aikana?
    ___ 0
    ___ 1–2
    ___ 3-5
    ___ yli 5

17. Kuinka monta digitaaliseen turvallisuuteen liittyvää harjoitusta **yritys on itse järjestänyt** vuoden 2020 aikana?
    ___ 0
    ___ 1-2
    ___ 3-5
    ___ yli 5

18. Kyselyn pohjalta jäikö Teille jokin kysymys tai yrityksen kyberturvallisuuteen liittyvä menestystekijä tai merkittävä puute, josta emme osanneet kysyä tässä osiossa? (avoin vastaustila)

Liite 2: Haastattelukysymykset

Digipoolin STRATEGIA22-projekti: Haastattelukysymykset

Teema 1: Yrityksen strategiset tavoitteet

(asetetut tavoitteet: taloudellisuus, tehokkuus (ulkoinen, sisäinen), kehittäminen)

1. Miten kyberturvallisuus näkyy yrityksen strategisissa tavoitteissa?
2. Onko hallituksella riittävä tietämys ja asiantuntemus, jotta se voi olla vastuussa kyberturvallisuutta koskevista päätöksistä?
3. Miten kyberturvallisuus vaikuttaa hallituksen ja johdon vastuisiin?
4. Kuinka organisaationne varmistaa, että toimenpiteenne ovat tehokkaita?
5. Kuinka organisaationne pysyy ajan tasalla kyberuhkista?
6. Strategisia ohjaimia ovat yleensä liiketoiminta, teknologia ja ympäristö.
    a. Miten kyberturvallisuus voisi tuoda yritykselle kilpailuetua?
    b. Tulisiko kyberturvallisuuden olla yrityksen strateginen ohjain em. lisäksi?
7. Onko teillä jotakin mielessä, jota en osannut kysyä?

Teema 2: Strategioiden toteutumisen turvaaminen

(riskianalyysi, strateginen valvonta, viestintä ja koulutus, operatiivisen johtamisen kytkentä strategiaan, ammattimainen strategiatyöskentely)

1. Miten kyberriskien arviointi on sidottu osaksi liiketoimintariskien arviointia?
2. Onko organisaatiossa viestitty selkeästi organisaation tärkeimmistä tavoitteista ja varmistettu, että nämä prioriteetit ohjaavat myös kyberturvallisuustoimenpiteitä?
3. Vallitseeko organisaatiossanne hyvä turvallisuuskulttuuri?
4. Millä tavoin organisaatio rajoittaa riskejä, jotka liittyvät tietojen, järjestelmien ja yhteyksien jakamiseen muiden organisaatioiden kanssa?
5. Millä tavoin organisaatiomme varmistaa sen, että kyberturvallisuus otetaan huomioon liiketoimintaan liittyvissä päätöksissä?
6. Onko hallituksella tiedossa, kuka johtaa toimintaa tietoturvaloukkauksissa ja kenellä on valtuudet tehdä päätöksiä?
7. Onko teillä jotakin mielessä, jota en osannut kysyä?

Lopuksi: Mikä olisi teidän yrityksenne oppi tai esimerkki, jota voisi kertoa/käyttää esimerkkinä muillekin?

Saako nimeänne/yritystä käyttää lähdeluettelossa?

Liite 3: Kyselyn tulosten kaaviot (erillinen tiedosto: STRATEGIA22 Kyselyn tulokset.pdf)

Huopalahdentie 24 I 00350 HELSINKI I FINLAND I www.cyberwatchfinland.fi