KYBERTURVALLINEN LIIKETOIMINTA

Sisällys

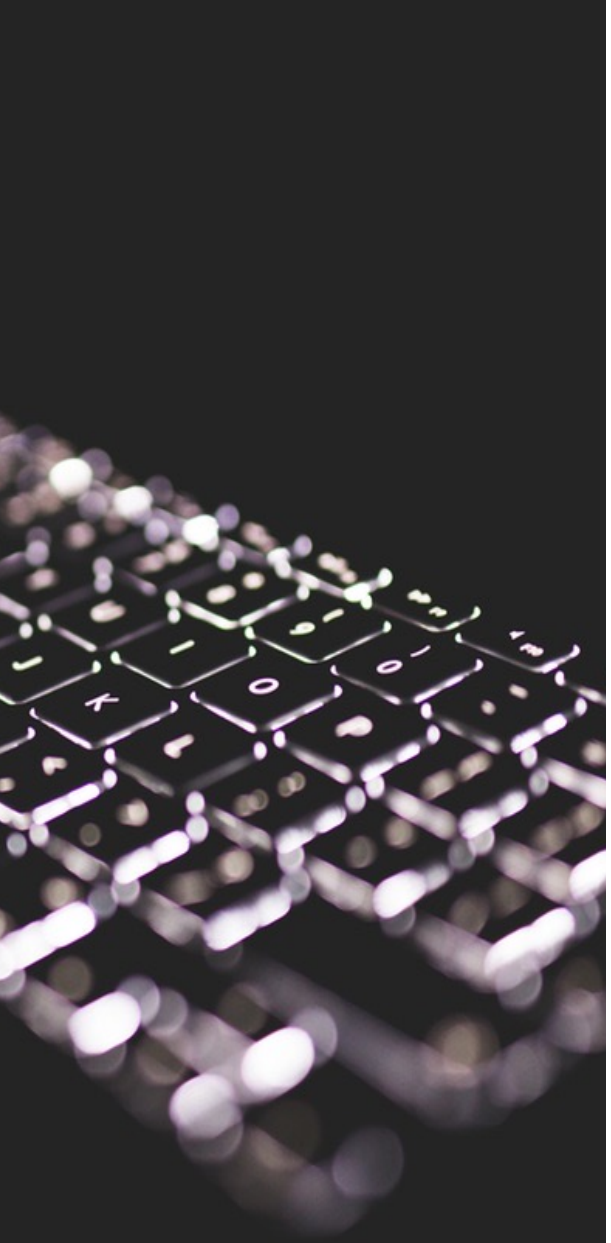
Lukijalle

Aiemmin suuri osa yritysten tietoturvarikkeistä tapahtui organisaation sisällä henkilöstön toimesta, mutta yritysten välisen kaupankäynnin ja tietojen vaihtamisen lisääntyessä on kiinnitettävä entistä tarkempaa huomiota verkkoliikenteen turvallisuuteen. Sähköinen kaupankäynti ja asiointi ovat jatkaneet kasvuaan 2000 luvun alusta ennennäkemättömän nopeasti, ja sitä mukaa myös kyberturvallisuuden merkitys on kasvanut ja jatkaa kasvamistaan huimalla vauhdilla. Tekoäly on tullut osaksi elämäämme, eikä yksikään organisaatio voi sulkea itseään ulkopuolelle tästä kehityksestä. Nykyisin saamme lukea päivittäin uusista tietoturva- ja tietosuojauhkista, joten on tärkeää ennakoida sekä varautua uhkiin ja riskeihin jo etukäteen..

Tämä opas on suunnattu niille, jotka pohtivat kyberturvallisuuteen liittyviä kysymyksiä ja kaipaavat lisätietoa kyberturvallisen liiketoiminnan edistämisestä. Oppaan tarkoituksena on tarjota näkökulmia kyberturvallisen liiketoiminnan edellytyksiin sekä antaa vinkkejä kyberturvallisuuden edistämiseen omassa organisaatiossasi. Toivottavasti materiaali vastaa myös sinun kysymyksiisi.

Antoisia lukuhetkiä toivottaa,

Xcure Oy



Mitä kyberturvallisuudella tarkoitetaan?

Yksi kyberturvallisuuteen liittyvistä haasteista on aiheen terminologia. Termille ”kyberturvallisuus” on yhtä monta tulkintaa kuin on aiheen asiantuntijaakin. Kyberturvallisuudella voidaan tarkoittaa lähes mitä tahansa puhtaan teknisestä tietoturvasta verkossa liikkuviin uhkiin, aina henkilöiden tietosuojaan asti, josta organisaatiot ovat yhtäläisesti vastuussa käsitellessään henkilöiden tietoja. Tarkkaa määritelmää kyberturvallisuudelle, kyberturvalle tai kyberuhille on siis suoranaisesti vaikea antaa.

Kuitenkin, se miten me Xcurella kyberturvallisuuden käsitämme, linkittyy pitkälti ajatukseen tahallisesta ja vahingoittavasta toiminnasta. Kyberturvallisuus, ja samalla kyberuhat, liittyvät toiselle osapuolelle tahallisesti aiheutettuihin tuhoihin tai haittoihin verkossa tapahtuvien hyökkäystoimenpiteiden kautta.

Kyberturvallisuus linkittyy siis verkkoon ja vahingoittavaan toimintaan. Kyberhyökkäyksessä hyökkääjä pyrkii teknologian avulla vaikuttamaan fyysiseen maailmaan. Esimerkiksi hakkerit voivat kotisohvaltaan kaataa kokonaisen sähköverkon ja siten aiheuttaa merkittävää vahinkoa paitsi itse sähköyhtiölle, myös sähköverkon asiakkaille.

Verrattuna perinteisempiin tietojen kalasteluun tai tietomurtoihin, kyberturvaan liittyvät uhat ovat siitä uudenlaisia uhkia, että hyökkäys voi tapahtua mistä päin maailmaa tahansa ja kohdistua käytännössä keneen tahansa. Kuka tahansa voi toiselta puolelta maailmaa hyökätä yrityksen toimintaa vastaan pelkän internet-yhteyden avulla ja saada aikaan merkittävääkin vahinkoa.

Tiesitkö?

IoT eli Internet of Things, asioiden internet, yhdistää yhä useampia laitteita verkkoon sekä kotona, että työpaikoilla. Vaikka kodinkoneiden ja laitteiden kytkeminen verkkoon helpottaa elämää, on tällaisella toiminnalla myös täysin omanlaisensa uhat, joita ei vielä tunnisteta riittävästi.

Tiesitkö, että kaikkia verkkoon kytkettyjä laitteita voidaan käyttää palvelunestohyökkäyksen välineinä ja halvaannuttaa esimerkiksi pankin verkon toimivuus täysin? Mitä enemmän laitteita on mukana hyökkäyksessä, sitä laajempaa tuhoa saadaan aikaiseksi.

Tällaisista hyökkäyksistä on paljon esimerkkitapauksia, mutta valitettavasti ihmiset eivät vielä ota tätä uhkaa riittävän vakavasti. Keinot suojautua tällaiselta toiminnalta ovat esimerkiksi laitteiden säännöllinen päivittäminen ja verkon salasanan vaihtaminen säännöllisesti.

XCURE

Millaisia kyberuhkia on olemassa?

Erilaisia kyberuhkien muotoja on olemassa tuhansia, eikä kaikkia pystytä tunnistamaan ajoissa. Erilaisten uhkien kehittäjät ovat käytännössä aina pienen askeleen edellä, ja voimme tehdä vain parhaamme suojautuaksemme uhilta. Tekoälyn nopea kehittyminen lisää uhkien kirjoa merkittävästi. Tämä asettaa melkoisen haasteen teknisille ratkaisuille, sekä myös henkilöille tiedon käsittelijöinä.

Kyberuhat voidaan karkeasti jaotella seuraavasti:

- Haittaohjelmahyökkäykset/kalasteluohjelmat, mukaan lukien ransomware eli kiristyshaittaohjelmat
- Tietomurrot/tunkeutumiset
- Palvelunestohyökkäykset
- Sisäiset ja ulkoiset uhat (esim. prosessit, henkilöstö, toimitusketju)

Suurin osa uhista pystytään oikeanlaisilla toimenpiteillä tunnistamaan ja huolellisella suunnittelulla niiden mahdollisiin vaikutuksiin voidaan myös varautua. Organisaatioiden tulisi tarkastaa ja auditoida teknisiä ympäristöjään, prosessejaan, sekä kouluttaa henkilökuntaa toistuvasti. Kun pohjatyöt on tehty hyvin, uhkien tunnistaminen helpottuu ja niiden mahdolliset seuraukset saadaan minimoitua.

Miksi kyberturvallisuudesta tulisi kiinnostua?

Jokainen yritys on nykypäivänä mahdollinen kohde kyberhyökkäyksille tai ylipäätään tietoturvan haavoittumisille, oli organisaatiossa sijaitseva tieto hyökkääjiä kiinnostavaa tai ei. Yleisimmin yrityksiä vastaan tehdään kyberhyökkäyksiä mm. seuraavista syistä:

- Kiinnostava yritystieto, esimerkiksi tuotekehitystiedot
- Kiinnostava yhteistyökumppaneihin liittyvä tieto, esimerkiksi asiakastiedot (mm. luottokortit, henkilötiedot)
- Verkon teknisen suojauksen puutteet
- Verkon tarjoamat mahdollisuudet, eli ihan vain "huvin vuoksi"

Edellä esitetyt esimerkit ovat todellakin vain esimerkkejä, sillä hyökkäyksen takana olevia motiiveja on yhtä monta kuin hyökkääjiäkin.

Tärkeintä onkin tunnistaa, että yrityksellä ei edes tarvitse olla omasta mielestään muita kiinnostavaa tietoa tai syytä olla kyberhyökkäyksen kohteena, sillä hyökkäyksiä tehdään myös ihan vain "huvin vuoksi".

Verkosta on helposti saatavilla palveluna ostettavaa kyberrikollisuutta ns. CaaS-palvelua (Crime-as-a-Service). Tämä tarkoittaa käytännössä sitä, että hyökkääjä voi erilaisilla automatisoiduilla ohjelmistoilla etsiä haavoittuneita tai suojaamattomia verkkoja ja ostaa kohdistettuja hyökkäyksiä yrityksiä kohtaan. Hyökkääjän ei tarvitse edes etsiä mitään erityistä tietoa kiinnostuakseen yrityksen tiedoista ja hyödyntääkseen löydettyä tietoturva-aukkoa. Tämä kaikki onnistuu hyökkääjältä ilman sen erityisempää tietoteknistä osaamista.

Miksikö siis kyberturvallisuudesta tulisi kiinnostua? Yksinkertaisin vastaus on, että kellään ei ole enää varaa olla kiinnostumatta.

Yleisimmät kyberturvallisuuden sudenkuopat

”Eihän meillä ole mitään kiinnostavaa tietoa” –ajattelu. Yllättävänkin monet yritykset kuvittelevat, ettei heillä ole olemassa mitään kovinkaan kiinnostavaa informaatiota, jota joku voisi haluta käsiinsä. Tämä ei kuitenkaan pidä paikkaansa - kaikilla yrityksillä on oletettavasti jotain tietoa, jota esimerkiksi kilpailijoilta halutaan varjella. Lisäksi, vaikka kiinnostavaa tietoa ei olisikaan, se ei tarkoita, etteikö yritys voisi joutua esimerkiksi edellä mainitun ”huvin vuoksi” -hyökkäyksen kohteeksi ja päätyä lopulta asiakkaiden mustalle listalle tietomurtojen vuoksi.

Kaikkia kyberuhkien muotoja ei tunnisteta. Monesti tietoturvaan tai kyberturvaan liittyviä uhkia ajatellaan aina ulkopuolelta tulevina uhkina. Mitäpä jos uhka tuleekin yrityksen sisältä? Yrityksen henkilöstö on yhtälailla kyberuhka kuin mikä tahansa muukin. Henkilöstö voi toimia uhkana sekä tahallisesti, että tahattomasti.

Esimerkiksi työntekijä voi tiedostamattaan avata sähköpostin mukana tulleen haittaohjelman tai syöttää yrityksen tietojärjestelmien tunnuksia tietojenkalastelijoiden sivustoille, mahdollistaen kyberrikolliselle pääsyn yrityksen tietoihin. Joku saattaa kopioida tietoja omaan henkilökohtaiseen pilvipalveluunsa tai hoitaa työtehtäviä henkilökohtaisella laitteellaan. Toinen taas ottaa työnantajan tietokoneen mukaansa ulkomaan lomamatkoille. Nämä kaikki aiheuttavat kyberuhkia ja saattavat aiheuttaa yritykselle seuraamuksia myös tietosuoja-asetuksen näkökulmasta. Ihminen usein on tietoturvallisuuden heikoin lenkki ja siksi henkilökunnan tietoturvan kouluttamiseen tulisi panostaa. Onko teillä tehty arviota myös tällaisista riskeistä ja koulutettu tietoturvaa henkilöstölle?

Henkilöstö ei tiedä, mitä yrityksen kyberturvallisuus tarkoittaa. Onko henkilöstö 100 % varmasti tietoinen siitä, mitä yrityksen tietoturvapolitiikka käsittää, ja kuinka säännökset koskevat heitä? Onko tietoturvapolitiikkaa tai –ohjeistusta edes tehty ja/tai jaettu henkilöstölle? Valitettavan usein henkilöstö on autuaan tietämätön siitä, mitä tietoturva tarkoittaa työnantajalle ja miten se vaikuttaa hänen työntekoonsa. Toisaalta, haasteita on usein myös esimerkiksi järjestelmien hankintaan liittyen. Tietääkö hankinnasta vastaava henkilökunta, millaisia tietoturvavaatimuksia hankittaville järjestelmille on asetettava?

Tiesitkö?

Monesti kuulee kysymyksen ”Mitä laki vaatii tietoturvalta?” tai ”Mitä meidän on pakko tehdä?”. Tämä on lähtökohtaisestikin väärä ajattelutapa, sillä jokainen yritys on vastuussa oman toimintansa tietoturvallisuudesta ja sen toteuttamisesta ilman, että laki puuttuu asiaan. Tietoturvan vaarantuminen voi aiheuttaa yritykselle merkittävää taloudellista- ja mainehaittaa jo ilman lainsäädäntöäkin.

Vuonna 2018 voimaan astunut EU:n tietosuoja-asetus toi mukanaan uudenlaisen kaikkia koskevan näkökannan tähän asiaan. Organisaatioita velvoitetaan tekemään töitä tietoturvan ja -suojan parantamiseksi ja myös osoittamaan, miten sen osalta toimitaan. Kuitenkin, olipa lakia tai ei, yrityksen olisi tärkeää tunnistaa yrityksen toiminnan jatkuvuutta uhkaavat riskit ja pyrkiä varautumaan parhaansa mukaan niihin.

Kuinka suojautua kyberuhilta?

XCURE

Kyberuhilta suojautuminen lähtee liikkeelle suunnittelusta ja uhkien tunnistamisesta. On olemassa erilaisia standardeja ja kriteeristöjä (kuten ISO 27001 tai KATAKRI), joiden pohjalta voidaan luoda tarkastuslistoja kyberturvallisuuden edistämiseksi. Ohjeistuksia ja standardeja hyödyntämällä yritys voi kehittää suojautumistasoaan itsekin, mikäli organisaatiosta löytyy osaamista ja asiantuntemusta standardien sisällön tulkintaan ja käytäntöihin.

On kuitenkin syytä myös muistaa, että tietoturva-ala muuttuu jatkuvasti ja uusia uhkia syntyy päivittäin. Mikäli organisaatiossa ei ole suunnitelmallista ja järjestelmällistä toimintamallia kyberturvallisuuden raportointiin, seurantaan ja päivittämiseen, pelkkä ohjeistuksien seuraaminen ei riitä. Jos kyberturvallisuutta halutaan itse edistää organisaatiossa ilman ulkopuolisen toimijan avustusta, on sille oltava selkeä suunnitelma ja toimintamalli. Asiantuntemusta täytyy löytyä kaikille kyberturvan eri osa-alueille, kuten dokumentointiin, seurantaan, raportointiin ja ennen kaikkea myös tietoturvan tekniseen puoleen. Jos jokin näistä osa-alueista ontuu, on syytä kääntyä asiantuntijan puoleen oikeiden toimintatapojen varmistamiseksi.

Oletko kuullut ns. tietoturvakävelystä? Tietoturvakävelyllä kuljette tietoturva-asiantuntijan kanssa yhdessä läpi organisaationne tietoturvahaasteita aina ihan konkreettiselle toimitilan kattavalle kävelylle. Voitte yllättyä mitä asioita tietoturvakävelyillä nouseekaan vastaan!

5 askelta kyberturvalliseen liiketoimintaan

XCURE

1. Tiedon luokittelu ja riskilähtöinen ajattelu

Jotta liiketoiminnasta saataisiin kyberturvallisempaa, kaikkein tärkeintä on lähteä liikkeelle yritykselle tärkeimpien tietojen kartoittamisesta, määrittelystä ja luokittelusta. Mitä on yritykselle kriittisin ja tärkein tieto? Missä tämä tieto sijaitsee? Kuinka tätä tietoa käsitellään, siirretään, suojataan?

Mikään tietoturvan kehityksessä ei voi onnistua, jos tietoja ei ole ensin kartoitettu ja luokiteltu. Tällöin on aivan mahdotonta tietää, mitä tietoa täytyy ylipäätään suojata. Tiedon luokittelu ja sen elinkaaren pohdinta sekä mahdollisten riskien hallinta on kaiken pohja kyberturvallisuuden edistämiseksi.

2. Tiedon sijoituspaikkojen turvallisuus

Kun tiedetään, missä kriittisin tieto sijaitsee, arvioidaan näitä sijainteja ja niiden turvallisuutta. Tämä voi käsittää järjestelmiä, kassakaappeja, toimistoja tai vaikkapa pöytälaatikoita. Sijoituspaikkojen turvallisuutta arvioidaan tiedon elinkaaren mukaisesti ja pohditaan kohta kohdalta, onko tieto varmasti jokaisessa vaiheessa suojattua.

Millainen tiedon elinkaari on, missä tieto syntyy, tulostellaanko sitä mappeihin, missä mapit sijaitsevat, kuka tietoa käsittelee, miten ja mihin tieto tallennetaan? Missä vaiheissa joku voi päästä tietoon käsiksi? Mitkä tiedon käsittelyn vaiheet ovat haavoittuvaisimpia?

3. Henkilöstön koulutus

Kun tieto on luokiteltu, kriittisin ja tärkein tieto tunnistettu ja sen suojaus on varmistettu, varmistetaan myös henkilöstön tiedottaminen. Kuten jo aiemmin on todettu, ihminen on tietoturvan heikoin lenkki. Vahinkoja sattuu, mutta työntekijä voi toimia myös tahallisesti. Kaikki henkilöstöön liittyvät riskit on arvioitava ja koko henkilöstön tulee olla tietoinen organisaation tietoturvan periaatteista ja ohjeistuksista. Monissa tapauksissa yritykseen on luotu laajat tietoturvapolitiikat ja –dokumentit, mutta työntekijät ovat autuaan tietämättömiä tietoturvaan liittyvistä käytänteistä.

4. Kriisitilanteisiin varautuminen

On tärkeää määrittää ja suunnitella, kuinka esimerkiksi havaitsemme, mikäli järjestelmissämme tapahtuu jotain poikkeavaa tai jos tietoa on vaikkapa varastettu. Havaitsemmeko tällaista tilannetta varmasti? Jos näin, niin mitä tapahtuu sen jälkeen? Kyberturvallinen liiketoiminta ei tarkoita 100-prosenttista tietoturvallisuutta, vaan uhkien todellisen luonteen tunnistamista.

Kaikkiin uhkiin emme voi varautua eikä niiltä voi suojautua, mutta tärkeää on, että organisaatiossa on luotu selkeä suunnitelma tietoturvapoikkeaman toteutuessa. Kuinka voimme jatkaa toimintaamme mahdollisimman nopeasti, miten reagoimme ja kuinka viestimme tapahtuneesta esimerkiksi viranomaisille, henkilöstölle ja/tai asiakkaille? Pahimpaankin skenaarioon on hyvä olla suunnitelma, vaikkei tilannetta koskaan tulisikaan eteen.

5. Tietoturvan jatkuvuus ja ylläpito

Tietojen ja järjestelmien suojaukseen tulee puuttua jatkuvasti. Ei riitä, että kartoitus ja vaadittavat toimenpiteet toteutetaan kerran tai kaksi ja oletetaan kaiken olevan kunnossa. Kuten todettu, kybermaailma muuttuu jatkuvasti, jokainen päivä tuo mukanaan uudenlaisia, kehittyneempiä uhkia. Tästä syystä tietoturvallisuuden ylläpito on jatkuva prosessi.

Organisaatioon on luotava säännölliset tarkastukset ja toimintamalleja on uudistettava aina vastaamaan sen hetken tilannetta. Tarvittaessa jatkuvuuden ylläpitoon voidaan ottaa myös ulkopuolinen kumppani, jonka kanssa suoritetaan säännöllisiä tarkistuksia – organisaation tarpeen mukaisesti. Tärkeintä on, että ajattelua uudistetaan säännöllisesti ja kybermaailman muutoksista pysytään valppaina jatkuvasti.

Kyberturvallisuuden ammattilaiset palveluksessasi

Xcuren asiantuntijat ovat kyberturvallisuuden ammattilaisia. Meidän tapamme toimia takaa sen, että asiakkaamme saavat aina tarpeisiinsa vastaavat tietoturvaratkaisut kustannustehokkaasti.

Xcuren asiantuntija- ja tekniset tietoturvapalvelut vastaa asiakkaan kyberturvahaasteisiin. Asiantuntijamme käy yhdessä asiakkaan kanssa läpi organisaation tietoturvallisuuden nykyisen tason ja laatii suunnitelman sekä kehitysehdotukset siitä, kuinka tietoturvassa päästään järkevällä tavalla ja kustannustehokkaasti eteenpäin.

Tarjoamme sekä yksittäisiä koulutuksia, että jatkuvampia ylläpito- ja asiantuntijapalveluita sekä kehittämäämme Tietosuojatyökalua organisaation tietosuojan ja tietoturvan hallintaan. Koulutuksemme on täysin räätälöitävissä asiakkaan tarpeen mukaisesti. Olemme järjestäneet koulutuksia yritysjohdolle ja henkilöstölle mm. tietosuojaan, tietoturvan tekniseen puoleen, tietoturvallisuuden johtamisnäkökulmaan, henkilöstön tietosuoja- ja turvaosaamiseen sekä tietoturvapolitiikan jalkauttamiseen liittyen.

Asiantuntijapalvelut on räätälöitävissä tarpeen mukaan, ja toteutettavat toimenpiteet katsotaan aina tapauskohtaisesti asiakkaan kanssa.

Lisätietoa aiheesta

Toivottavasti materiaalimme tarjosi sinulle lisätietoa kyberaiheisiin liittyen ja vastasi sinulla mahdollisesti avoinna olleisiin kysymyksiin. Mikäli jokin jäi vielä askarruttamaan, otathan yhteyttä Xcuren asiantuntijoihin. Autamme mielellämme kaikissa kyberturvallisuutta ja tietosuojaa koskevissa asioissa!

Tutustu myös blogiimme, jossa käsittelemme tietoturvaan, tietosuojaan, kyberturvallisuuteen ja tiedonpalautukseen liittyviä aiheita!

Xcure Oy on tietosuojaan ja tietoturvaan erikoistunut palvelu- ja ohjelmistoyritys. Olemme auttaneet asiakkaitamme tietoturvan ja tietosuojan haasteissa jo vuodesta 2006. Olemme kehittäneet asiakkaidemme pyynnöstä mm. Tietosuojatyökalun, joka auttaa organisaatioita toimimaan lainsäädännön vaatimalla tavalla.

XCURE