YRITYSJOHDON OPAS

kyberturvallisuuden johtamiseen - tietoturvaosaamisella kilpailuetua.

Yritysjohtaja, onko yrityksesi verkot ja tietoturva valmiina digitalisoitumaan?

elisa

Johdanto

Digitaalisessa maailmassa yrityksen kriittisten toimintojen jatkuvuuden turvaaminen ja yrityksen salassa pidettävän tiedon suojaaminen on välttämätöntä. Yritysten liiketoimintaa vaarantavat uudenlaiset, yhä vaikeammin havaittaviksi muuttuvat kyberuhat, joihin varautumisen tulee olla linjattuna jokaisen yrityksen strategiassa.

Tämä opas auttaa sinua, yritysjohtaja, tunnistamaan, ymmärtämään ja hallitsemaan kyberturvallisuuden eri osa-alueita ja niiden vaikutuksia yrityksenne liiketoimintaan.

Oppaan avulla:

1. Kasvatat liiketoimintajohdon tietoisuutta kyberturvallisuuden merkityksestä
2. Tunnistat yrityksenne olemassa olevat kyvykkyydet sekä kriittisimmät kehittämiskohteet
3. Opit hyödyntämään kyberturvallisuuden tarjoamia mahdollisuuksia omassa liiketoiminnassa
4. Varmistat, että yrityksesi palvelu-arkkitehtuuri, tietoverkot- ja turvallisuus ovat valmiita digitalisoitumaan

Maailma digitalisoituu ja sen myötä eri teknologiat yhdistyvät jatkossa kaikkeen tekemiseen entistä vahvemmin. Asiakaskokemus on liiketoiminnan keskiössä ja sähköisten tietotyön- ja johtamisen välineiden hyödyntämisestä on tullut yrityksissä itsestäänselvyys. Elämme ajassa, jossa yrityksenä tavoittelemme entistä parempaa tasapainoa uusien palvelumallien, uudenlaisen työteon tapojen ja oikeantasoisen suojautumisen välillä.

Digitalisaatiolla ei tarkoiteta vain yhden asian muuttamista sähköisesti järjestettäväksi. Sillä tarkoitetaan kokonaisuutta, joka tehdään eri tavalla kuin ennen. Tulevaisuudessa menestyjäyritykset pääsevät digitalisaatiota hyödyntämällä lähemmäksi asiakkaiden liiketoiminnan arvoketjua ja tuottamaan siihen lisäarvoa. Ansaintalogiikat muuttuvat ja digitaalisuus on yhä suoremmin kiinni sekä asiakkaan että toimittajan välisessä liiketoiminnassa. Samaan muutostahtiin kehittyvät myös erilaiset tietoturvallisuusuhat, jotka pahimmassa tapauksessa vaarantavat perusteellisesti koko yrityksen toimintaa. Pelkästään jo kuluneen vuoden aikana on maailmassa havaittu 38 % enemmän tietoturvallisuusrikoksia edelliseen vuoteen verrattuna. Siinä missä digitalisaatio tuo yrityksille valtavia mahdollisuuksia rakentaa uutta liiketoimintaa, se samalla tuo ennennäkemättömän suurta vastuuta: tieto, sen turvallinen käsittely ja sitä hyödyntävien tahojen identiteetti on turvattava yhtä lailla niin yrityksen työntekijöille kuin sen asiakkaillekin. **Ilman turvallisuusnäkökulmien huomiointia digitalisaatiota ei voi viedä eteenpäin.**

Tietoturvallisuusrikokset ovat kasvaneet kuluneen vuoden aikana

38%

Digitalisoituminen edellyttää tietoverkkojen laajentuessa entistä enemmän huomioarvoa tietoturvaan

Keskeisimpiä kyberturvallisuushaasteita, joita nykypäivänorganisaatiot kohtaavat:

Hyvien kyberturvallisuusosaajien vähäisyys

Turvallisuusuhkien kasvava monimutkaisuus

Kyberturvallisuuteen sijoitettavissa olevien investointien niukkuus

Puutteellinen kyberturvallisuuden tilannetietoisuus

Tietojohtamisen kehittäminen

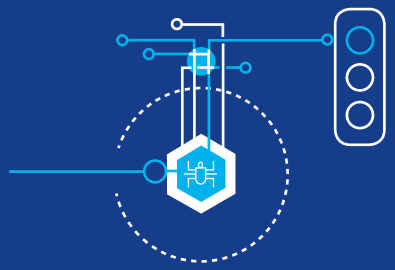
Mistä Kyber-turvallisuudessa on kyse?

Kyberturvallisuus on eittämättä yksi keskeisimmistä yritysten kokonaisturvallisuuteen liittyvistä tekijöistä. Kyberturvallisuudesta puhutaan paljon, mutta yritysten arjessa sitä ymmärretään vielä verrattain vähän, siitäkin huolimatta, että 86 % yrityksistä kertoo edes jollakin tasolla kehittävänsä yrityksen prosesseihin liittyvää tietoturvallisuutta. PWC`n Global Economic Survey (2014) kertoo, että **yhden vuoden aikana yritykset menettivät erilaisten kyberhaittojen vuoksi globaalilla tasolla yhteensä yli 400 miljardia euroa, kun samana vuonna kyberturvallisuuden varmistamiseksi yrityksissä investoitiin vain n. 75 miljoonaa euroa.**

Mistä tämä epäkohta lukemien välillä sitten kertoo?

1. Kyberturvallisuutta ei mielletä osaksi digitalisoituvaa liiketoimintaa
2. Tietoturvaan liittyviä uhkia ei koeta liiketoiminnalle merkittäviksi
3. Tietosuojakäytännöt ovat puutteelliset
4. Tietoturvasta ei tiedetä tarpeeksi organisaation sisällä
5. Kyberturvallisuuden varmistaminen mielletään liian kalliiksi
6. Kyberturvallisuus ei ole johdon strateginen painopiste

Mitä eroa on tietoturvalla ja kyberturvallisuudella.



Tietoturva suojaa tietojärjestelmässä käsiteltäviä tietoja. Jos tietoturva pettää, seurauksena voi olla, että kyberympäristö toimii toisin, kuin on tarkoitus.

Tietoturva:

- Tietojärjestelmässä olevat tiedot on suojattu
- Tiedot ovat silloin saatavilla, kun niitä tarvitaan
- Tietoja käsittelevät vain sellaiset henkilöt, joilla on siihen oikeus
- Tieto ei ole vahingon seurauksena muuttunut

Kyberturvallisuuden tavoitteena on varmistaa, että kyberympäristöstä ei aiheudu haittaa, vaaraa tai häiriötä kyberympäristöstä riippuvalle toiminnalle.

Kyberuhka:

- Kyberympäristöön vaikuttava teko tai tapahtuma, joka toteutuessaan vaarantaa kyberympäristöstä riippuvaiset toiminnot

Tietoturva-uhka

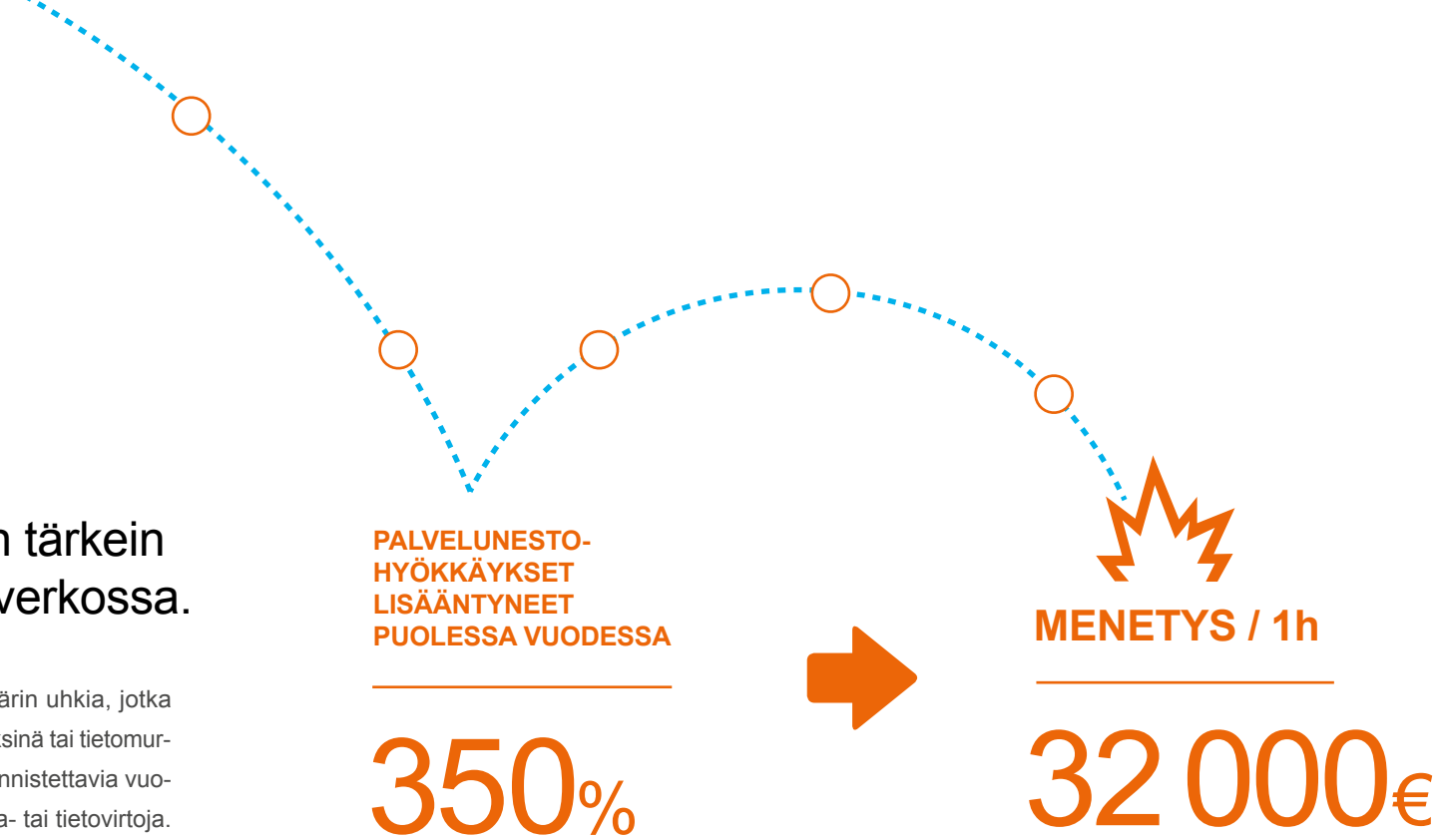
- Tietojärjestelmään vaikuttava teko tai tapahtuma, joka toteutuessaan vaarantaa tietojärjestelmän toiminnan.

Yritysten kyberturvallisuudessa on kyse laajemmasta ulottuvuudesta kuin tietoverkon ja yrityksen it-ympäristön turvallisuudesta sekä niitä uhkaavista hyökkäyksistä. Kyberturvallisuuteen liittyy olennaisesti myös fyysinen turvallisuus, joka sisältää toimitilojen lisäksi valvontalaitteiston sekä prosessit, toimintatavat ja ihmisen toiminnan sekä kyvyn tehdä havaintoja.

Suomalainen kyberturvallisuuden professori **Jarno Limnell** kuvaa kyberturvallisuutta seuraavasti: ”Kaiken perustana on kyberturvallisuuden ymmärtäminen kananmunana, joka tulee vatkata kaikkeen toimintaan sisälle, eikä vain kuorruttaa tehtyjen ratkaisujen päälle.” Liiketoiminnan näkökulmasta onkin tärkeää, että kybertoimintaympäristö osataan mieltää erityiseksi ekosysteemiksi, jossa fyysinen ja bittien maailma ovat vahvemmin yhteen kietoutuneita.

Kybermaailma on kaikkialla läsnä. Yksiselitteistä jakoa fyysiseen ja bittien maailmaan ei voi tehdä, koska kyberulottuvuuden tapahtumilla on selkeitä fyysisiä seurauksia. Menestyvän liiketoiminnan rakentaminen on riippuvainen bittien maailmasta.

Kyberturvallisuus toteutuu:



Tänä päivänä yritysten tärkein ydin sijaitsee kiistatta verkossa.

Tietoverkkoihin kohdistuu kasvavassa määrin uhkia, jotka voivat realisoitua esimerkiksi verkkohyökkäyksinä tai tietomurtoina. Ne voivat olla yrityksessä vaikeasti tunnistettavia vuotoja, joilla kerätään esimerkiksi jatkuvia raha- tai tietovirtoja. Hewlett Packardin yhdessä amerikkalaisen Ponemon Institute of Cyber Crimen tekemän tutkimuksen (2015) mukaan kyberrikollisuuden on tutkittu maksavan yhdelle Pohjois-Amerikkalaisille yritykselle keskimäärin noin 15 miljoonaa dollaria vuodessa.

Kyberturvallisuuden merkittävistä liiketoimintariskeistä yrityksille raportoi myös Incapsulan tekemä selvitys, joka kertoo että palvelunestohyökkäysten kohteeksi joutuneille keskisuurille yrityksille koitui vuonna 2014 Pohjois-Amerikassa keskimäärin yli 32 000 euron tappiot tunnissa. Samaisen tutkimuksen mukaan myös palvelunestohyökkäykset kasvoivat pelkästään vuoden 2014 alkupuolella jopa 350 %.

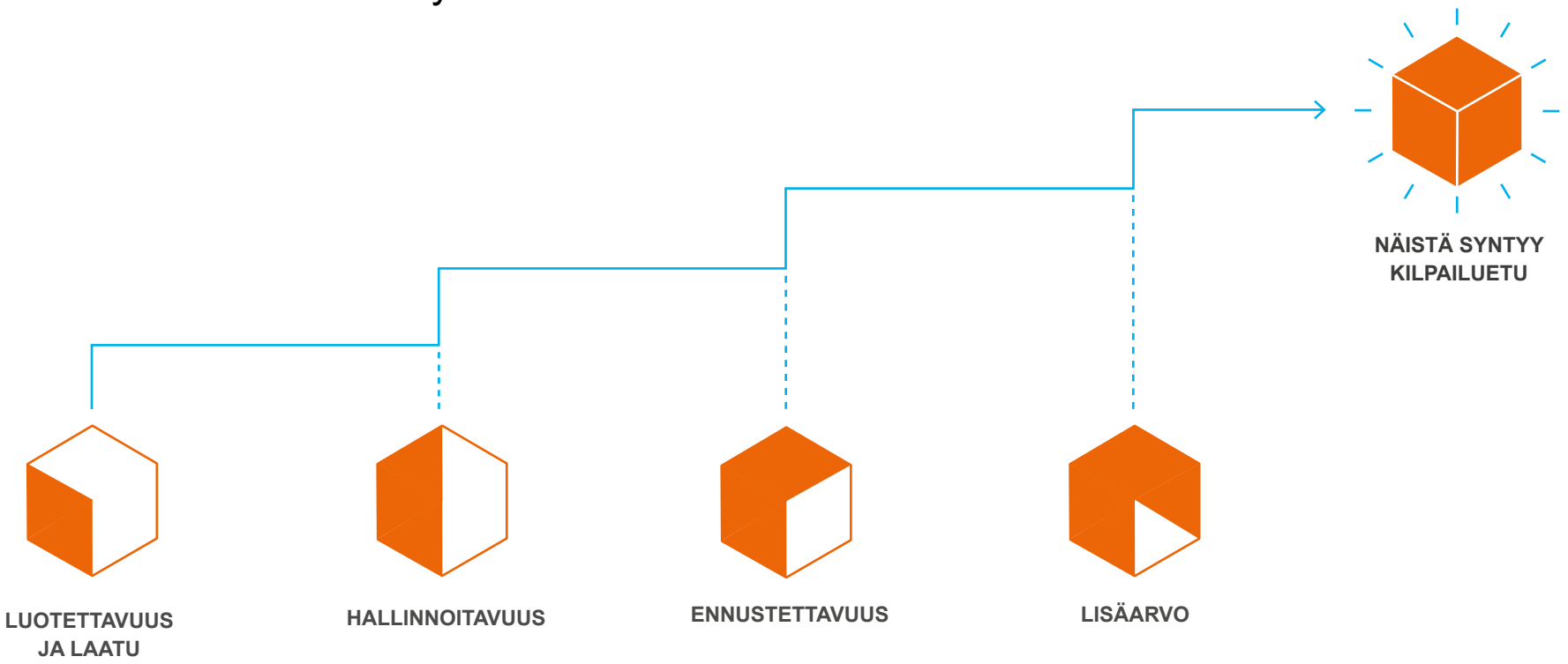
Yksinkertaisimmillaan liiketoimintaa koskettavat tietoturvauhat voivat olla esimerkiksi palvelunestohyökkäyksiä, joilla estetään jonkin verkossa tapahtuvan palvelun käyttäminen, esimerkkinä vaikkapa asiointi verkkopankissa. Toisenlaisen uhan muodostavat erilaiset tunkeutumiset tietojärjestelmiin, koneisiin ja laitteisiin sekä erilaiset haittaohjelmat, jotka voivat levitä esimerkiksi yritysten s-postien tai niiden mukana tulleiden liitteiden kautta.

Yhdeksi yleisimmäksi kyberhyökkäyksen reitiksi on tunnistettu Flash-ohjelma, samoin erilaisten verkkosivustojen suojaamattomat alustat ja esimerkiksi tietokoneen päivittämätön Java-ohjelmisto. Lisäksi nykyisin suuressa suosiossa olevat blogit ja niissä käytetyt verkkoalustat on tunnistettu haavoittuvaisiksi erilaisille tietoturvahyökkäyksille, erityisesti päivittämättöminä. Yrityksiin kohdistuneiden hyökkäysten taustalla ovat pääosin järjestelmällisesti operoivat tahot, joiden tärkeimpänä motiivina on raha. Taloudellista hyötyä tavoitellaan arvokkaalla tiedolla, jota ovat mm. yrityksen osaamispääoma, salaisten yritystiedot, tiedot tuotekehityksestä ja innovaatioista sekä asiakkaisiin liittyvä tieto.

Liian usein tietoturvasta ja kyberturvallisuudesta keskusteltaessa keskitytään pelkkiin uhkiin ja niiden kohtaamisen, mikä toki on tärkeää. **Digitalisaatio ja verkottuminen tarjoavat kuitenkin yrityksille jatkuvasti myös lisää mahdollisuuksia toiminnan laajentamiseen ja tehostamiseen, uusien palveluiden kehittämiseen ja kustannusten alentamiseen.**

”Kyberturvallisuuden korkea hinta, johtuu monesti siitä, että tietoturvaa ryhdytään käsittelemään projekteissa liian myöhään. Tietoturvatoimien vaikutukset vaikkapa aikatauluun voivat silloin olla merkittäviä”

Kyberturvallisuus on mahdollisuus

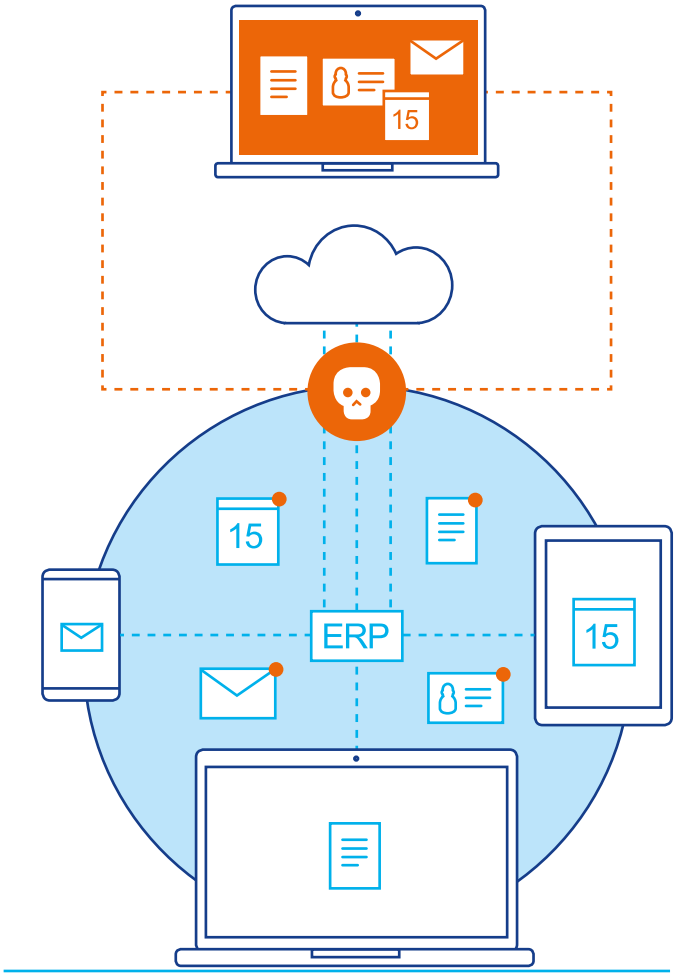


Miksi kyberturvallisuuden varmistaminen on strategisesti tärkeää?

Erityisesti pk-yrityksissä voi liiketoimintajohdon olla verrattain helppo tuudittautua siihen ajatukseen, että tietoturvallisuus ”ei koske meitä, emmehän me käsittele mitään valtion salaisuuksia.” Mutta hetken asiaa mietittyäsi huomaat varmasti, kuinka usein ja kuinka paljon sensitiivistä, korkean profiilin osaamispääomaa ja liiketoiminnallesi kriittistä tietoa yrityksesi eri tietojärjestelmissä todella päivittäin liikkuu.

Pysähdy hetkeksi seuraavien kysymysten pariin:

- Onko yrityksellänne käytössä henkilöstön tabletteja, älypuhelimia ja etäyhteyksiä?
- Onko henkilöstöllänne pääsy s-postiin mobiililaitteella?
- Käyttääkö henkilöstönne työpaikan sähköpostia omilla henkilökohtaisilla päätelaitteilla?
- Onko yrityksessänne käytössä sähköisiä kalentereita tai pidättekö verkon kautta etätapaamisia asiakkaidenne kanssa?
- Onko yrityksenne aktiivinen sosiaalisessa mediassa?
- Onko yrityksellänne verkkokauppa tai sähköinen kassajärjestelmä?
- Onko yrityksenne dataa tallennettuna pilvipalveluihin?
- Onko yrityksellänne käytössä yksi tai useampi toiminnanohjausjärjestelmä?



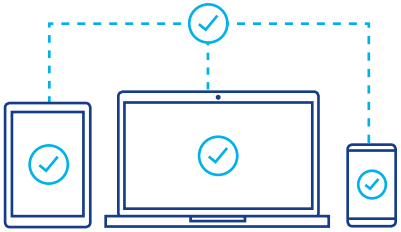
Tiedätkö, kuinka hyvin yrityksenne työasemat ja tietoverkot ovat suojattu?

Suomalaisyritysten työasemaympäristöt on suojattu pääosin virustorjuntaohjelmistoilla ja palomuureilla. Moni luulee toimivansa suojatussa ja turvallisessa ympäristössä, mutta suljettuja ympäristöjä ei enää ole. Verkkoympäristöjä pitää reaaliaikaisesti valvoa, jotta siellä eivät pääse operoimaan väärät tahot. Harvalla yrityksellä on hallussa verkon reaaliaikainen tilannekuva, eikä lokitietoja hallita tehokkaasti. Yrityksissä ei usein varmuudella edes tiedetä, mitä kaikkea omaan verkkoympäristöön voidaan liittää ilman virallista prosessia tai valtuuksia.

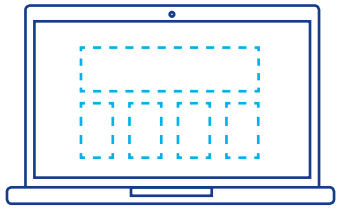
Moni luulee toimivansa suojatussa ja turvallisessa ympäristössä, mutta suljettuja ympäristöjä ei enää ole.

Verkkojen turvallisuus

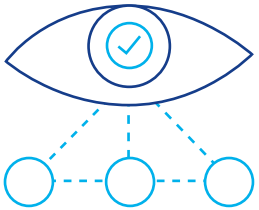
Suojaa sisäinen verkkonne sekä käyttämänne pilvipalvelut.
Yrityksenne tietoliikenneverkkojen turvaaminen luvattomia tunkeutumisia, väärinkäyttöä ja palvelunestoa vastaan vaatii:



1. Kaikkien verkon laitteiden ja yhteyksien tunnistamista



2. Selkeiden rajapintojen luomista yrityksenne järjestelmien ja muun verkkomaailman välille



3. Valvonnan toteuttamista.

Tiedon vuotaminen kilpailijalle voi haitata yrityksen kilpailukykyä merkittävästi. Esimerkiksi työsuhteita koskevien tietojen vuotaminen taas voi vahingoittaa yrityksen sisäistä luottamusta. Vuotojen selvittely ja vahinkojen rajaaminen sitoo usein henkilöitä organisaation kaikilla tasoilla. Tietokoneille pesiytyneet haittaohjelmat voivat hidastaa ja jumiuttaa tietokoneita, ja sitä kautta koko yrityksen toimintaa, kun taas niiden poistaminen sitoo henkilötyötä sekä laitteita, ja voi aiheuttaa katkoja normaalissa toiminnassa. Suuren riskin muodostavat myös työntekijöiden liian laajat käyttöoikeudet eri tietojärjestelmiin, jotka voivat johtaa tahallisiin tai tahattomiin väärinkäytöksiin.

Pahimmassa tapauksessa yrityksen tietoturva-aukot voivat johtaa yrityksen koko tuotannon pysähtymiseen, tuotteiden pilaantumiseen ja henkilöstön loukkaantumisiin. Siltikin monesta näkökulmasta yksi **merkittävimmistä uhista liiketoiminnalle on yrityksen maineen menetys asiakkaiden silmissä**. Menetetyt työtunnit ja tuotannon seisakkien aiheuttama menetys voidaan konkreettisesti osoittaa euroissa, mutta mikä on yrityksen maineen hinta? Mitä maksaa se, kun asiakkaiden luottamus menetetään?

Asiakkaan luottamus on yritykselle korvaamattoman tärkeää

Näin varmistat yrityksesi tietoturvan riittävän perustason:

1. Huolehdi että ohjelmistot ovat ajan tasalla – älä luota vain automaattisiin päivityksiin
2. Varmista, että virustorjunta on kunnossa – suurin osa uhista on estettävissä
3. Tarkista, että käyttöoikeudet pysyvät aina varmassa tallessa
4. Varmista, että tietoverkon turvallisuus on ajan tasalla sekä valvonta ja hallinta mahdollisimman reaaliaikaista
5. Huolehdi, että keskeiset palvelimet ja liiketoiminta sovellukset ovat keskitetyn hallinnan piirissä
6. Varmista, työntekijöiden päätelaite turvallisuus on valvottua ja keskitetyn hallinnan piirissä
7. Tarkista, että käyttöoikeudet perustuvat tarpeeseen, ja oikeudet ovat ajan tasalla työrooliin liittyen

Konkreettinen ja verrattain läheltä löytyvä esimerkki tietoturva-uhan realisoitumisesta löytyy nostolaitteita valmistavan Konecranes Oy:n liiketoiminnasta, jonka ulkomainen tytäryhtiö joutui kevään 2015 aikana mittavan verkkopetoksen uhriksi. Yrityksen tietoverkkoihin asennettiin haittaohjelmia, jotka pahimmassa tapauksessa olisivat voineet lamauttaa koko tytäryhtiön liiketoiminnan. Kyseisessä tapauksessa verkkoon murtauduttiin hakkeroimalla sisään suoraan yksittäisen työntekijän sähköpostin kautta. Rikoksen tekijät ovat identiteettivarkaudella ja muilla petollisilla toimilla saaneet Konecranesin tytäryhtiön suorittaman aiheettomia maksuja jopa 17,2 miljoonaa euroa.

Tämän päivän digitaalisessa maailmassa, jossa palvelut siirtyvät verkkoon kiivaalla vauhdilla, tietoturvaan liittyvät liiketoimintariskit ovat todellisia ja koskettavat jokaista yritystä niiden toimialasta ja koosta riippumatta. Erityisen kiinnostuneita kyberrikolliset ovat juuri pk-yrityksistä, jotka ovat usein kovin haavoittuvaisia hyökkäyksille verrattain puutteellisen tietoturvallisuutensa vuoksi.

Konecranesin tytäryhtiössä tietoturva-uhka konkretisoitui ja yritys kärsi jopa 17,2 miljoonan euron tappiot

Miten yrityksen kyberturvallisuutta johdetaan?

Kyberturvallisuuden johtamiseksi tarvitaan uudenlaista ajattelua ja toimintamallia, jossa nykyinen kyvykkyys varautumiseen ei enää riitä. Digitaalinen ja fyysinen maailma kietoutuvat yhä tiiviimmin yhteen ja verkottuneessa maailmassa kyberturvallisuuteen tarvitaan reaaliaikaista tietovirtojen valvontaa ja hallintaa.

EU:n tietosuoja-asetus muuttaa yritysten tietosuojakäytäntöjä

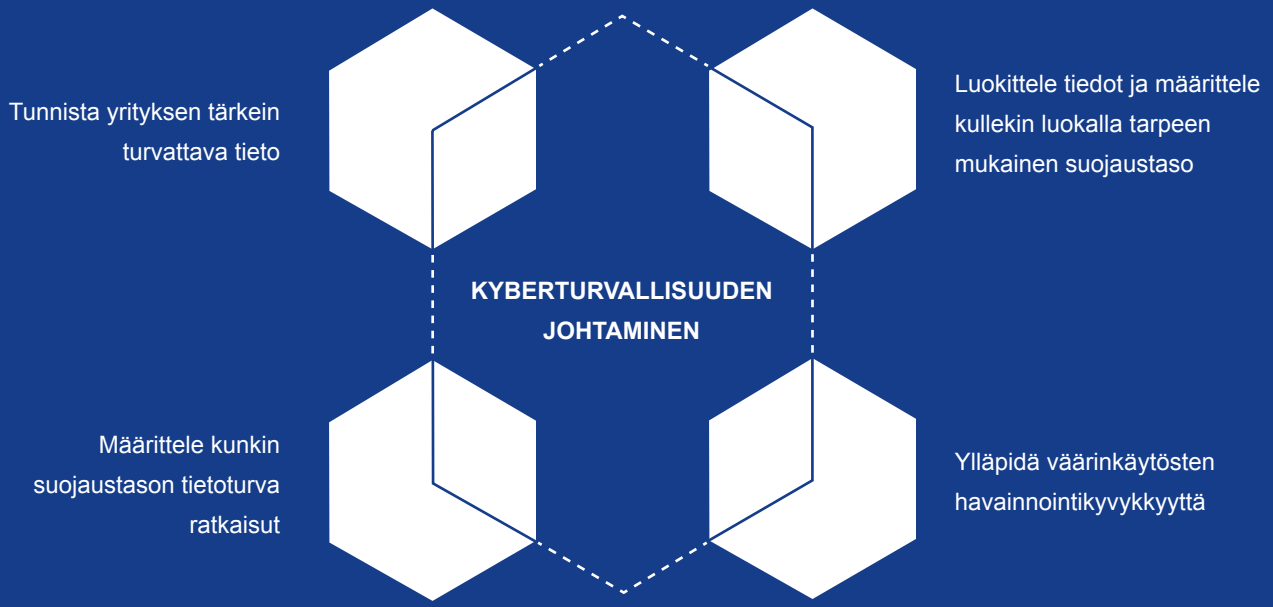
Varmista, että yrityksesi tietosuojakäytännöt ovat ajan tasalla:

EU:n yleinen tietosuoja-asetus tulee lähitulevaisuudessa muuttamaan henkilötietojen käsittelyn sääntelyn perustaa ja tuo mukanaan uusia, nykyistä tiukempia vaatimuksia rekisterinpitäjille. Jatkossa henkilötietojen käsittelyn tulee olla suunnitelmallista, dokumentoitua ja perustua riskianalyysiin. Rekisterinpitäjän tulee jatkossa kyetä tarvittaessa osoittamaan, että on toiminut asetuksen vaatimusten mukaisesti, korotettujen sanktioiden uhalla.

Digitaalisen liiketoiminnan jatkuvuuden ja häiriöttömän käytön kannalta on tärkeää tunnistaa liiketoimintaan kohdistuvat merkittävät uhkatekijät ja keinot niiden torjumiseksi. Yhtä lailla yrityksen tulee pitkäjänteisesti kehittää yrityksen osaamista kyberturvallisuuden kyvykkyyden rakentamiseksi, sekä ennen kaikkea kehittää henkilöstönsä tietoisuutta ja havainnointikykyä tietoturvallisuuteen liittyvissä asioissa. **Ensin tulee siis ymmärtää, minkälaista uhkaa vastaan ollaan todellisuudessa suojautumassa.** Vasta selkeän uhka-analyysin jälkeen kannattaa lähteä miettimään ennaltaehkäisyn puolustautumistoimenpiteitä, joihin kuuluvat yhtä lailla ihmiset, prosessit kuin teknologiakin.

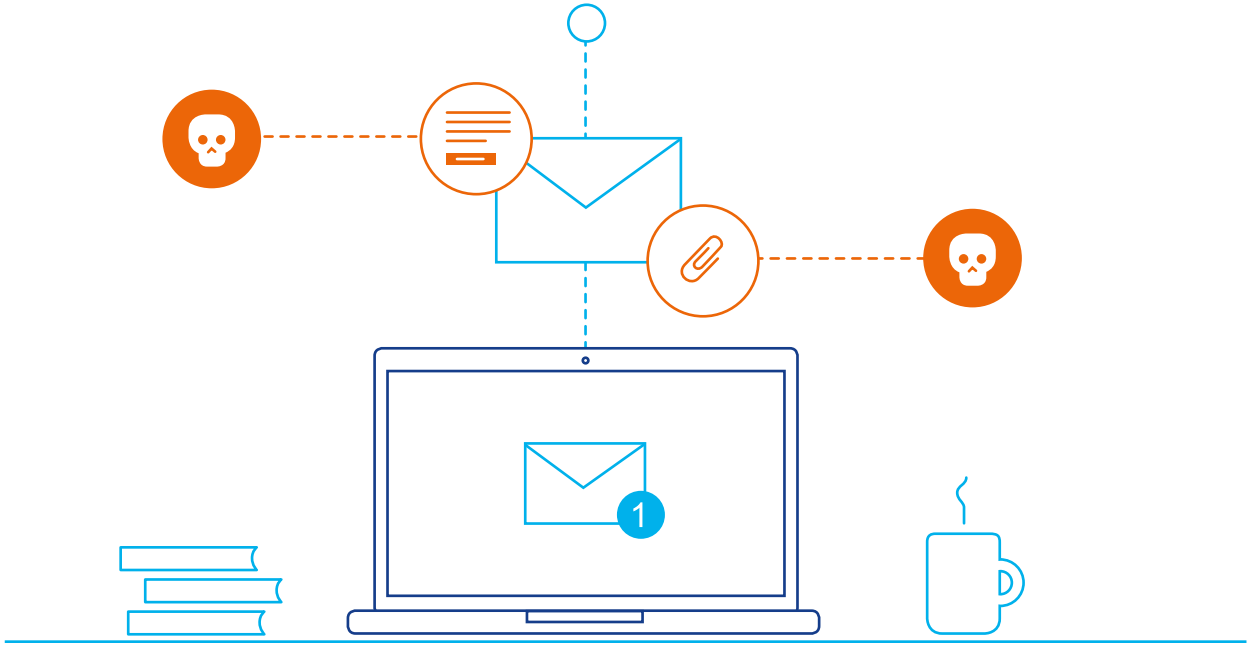
Verkon tilannekuvalla ja valvonnalla, sekä analysoinnilla tunnistetaan piileviä trendejä ja uhkia ajoissa. Valtaosa verkossa olevista laitteista on melko helppo tunnistaa.

Kyberturvallisuuden johtaminen



45%

Tietoturvahyökkäyksistä aiheutuu sähköpostiviestien mukana tulleiden linkkien tai liitteiden avaamisesta



Johtamisen näkökulmasta on lisäksi elintärkeää huomata, että lopulta suurin riski yrityksen tietoturvalle ei suinkaan ole teknologia vaan, yksittäinen ihminen, joka täysin tiedostamattaan altistaa yrityksen uhalle. Vaikka ulkopuoliset ”pahaa tahtovat” tahot tulee aina ottaa huomioon kyberturvallisuudesta puhuttaessa, on monessa tutkimuksessa kuitenkin huomioitu, että **suurin uhka vahingoille tulee sisältä päin**. Usein kyseinen ”pahaa tahtova” taho saa yrityksessä työskentelevän henkilön toimivaan väärin, esimerkiksi lataamaan sähköpostista haitallisen liitteen, juuri niin kuin kävi hieman aiemmin kuvatussa Konecranesin tytäryhtiön tapauksessa. Tutkimukset itse asiassa paljastavat, että jopa 45 % tieturvallisuushyökkäyksistä on aiheutunut yrityksille juuri näin.

Varmasti meistä moni on avannut tiedoston, jonka lähettäjästä, sisällöistä tai liitteistä ei ole ollut varmuutta. Tällöin olemme altistaneet oman organisaatiomme kyberuhalle.

Kyberuhkien kaksi juurisyytä liittyvät molemmat ihmiseen; toinen on ihmisten osaamattomuus ja toinen välinpitämättömyys. Vain toiseen näistä voimme aktiivisesti vaikuttaa.

– Jarno Limnell

Uhkakuvien sijaan turvallisuus tulee nähdä mahdollisuutena laskea kustannuksia pitkällä aikavälillä ja varmistaa liiketoiminnan jatkuvuus.

Tämä kokonaisvaltainen asenteiden, toimintatapojen ja teknisen infrastruktuurin kolmiyhteys voi auttaa kyberturvallisuuden vastuualueiden tunnistamisessa. **Asenteiden ohjaamisen täytyy lähteä ylimmästä johdosta ja teknologian hyödyntämisen ja siihen liittyvien toimintatapojen kehittämiseen tarvitaan viime kädessä aivan koko yrityksen henkilöstöä**.

Oikeanlaisten tietoturvallisuutta koskevien asenteiden edistäminen ei yleensä ole kovin haasteellista. Yrityksistä ei varmastikaan juuri löydy henkilöitä, joiden mielestä tietoturvallisuus olisi lähtökohtaisesti huono asia. Yrityksen ylintä johtoa tarvitaan kuitenkin juuri ohjaamaan henkilöstön asenteita ja auttamaan heitä ymmärtämään tietoturvallisuuden merkitys omalle työlleen ja osana yrityksen tulevaisuutta. Johdon tulee aktiivisesti kommunikoida henkilöstölle heidän näkemyksensä siitä, millainen tapa toimia edistää pitkällä tähtäimellä yrityksen menestystä. Johdon kannattaa myös edistää sellaista ilmapiiriä, jossa kaikki työntekijät ovat motivoituneita osallistumaan tietoturvallisuuden kehittämiseen tuoden aktiivisesta esiin asioita, joilla voi olla vaikutusta yrityksen turvallisuuden tilannekuvaan.

Yhdeksi kaikkein keskeisimmästä kysymyksistä kyberturvallisuuden johtamisessa nousee ehdottomasti yrityksen resilienssi, eli sietokyvyn kehittäminen. **Resilienssi tarkoittaa yrityksen kykyä selvitä erilaisista normaalitilanteesta poikkeavista häiriötilanteista sekä riskin realisoituessa kykyä palauttaa toiminnat mahdollisimman nopeasti häiriötilannetta edeltäneellä tasolle**. Resilienssiin kuuluu keskeiseltä osaltaan myös koko organisaation henkinen kriisinsietokyky, joka tulevaisuuden menestyvän yrityksen johto lähtee systemaattisesta kehittämään.

Yrityksen kyberturvallisuuden varmistaminen vaatii yritysjohdolta strategista suunnittelua ja toteuttamista käytännön tasolla.

”Johtajan täytyy ymmärtää, mitä organisaatio tai yritys tavoittelee kyberturvallisuuteen panostamalla. Kyse on johtajan kyvystä strategiseen ajatteluun sekä kyvystä sitouttaa koko organisaatio mukaan. Ilman strategista osaamista ja ymmärrystä kyberturvallisuudesta on johdon mahdotonta sitoutua ja ennen kaikkea ohjata kyberturvallisuutta organisaatiossaan. Toisaalta, hyvin johdettu ja tekojen kautta hoidettu kyberturvallisuus voi olla yritykselle hyvin vahva kilpailuetu. Välttämättömyys se on joka tapauksessa.”

Kyberturvallisuus on liiketoimintahaaste, ei pelkästään teknologinen haaste

Yritysjohtaja, näin turvaat liiketoimintanne digitaalisen ympäristön:

1. Ymmärrä liiketoiminne kannalta liiketoimintakriittinen tieto ja suojaa se
2. Tunnista millaisilta uhkia vastaan olette suojautumassa
3. Rakenna yrityksenne prosessi, jolla systemaattisesti hallinnoida riskejä – sitoudu jatkuvaan turvallisuuden ylläpitoon ja kehittämiseen
4. Jos riski huolellisesta varautumisesta huolimatta konkretisoituu, reagoi välittömästi
5. Varmista, että viestinnän ja yksityisyyden suoja-asiat ovat tunnistettu ja huomioitu toiminnassa
6. Kouluta henkilöstösi kyberturvallisuudesta – rakenna ja ylläpidä ohjeistoa hyvistä toimintatavoista
7. Investoi kyberturvallisuuteen ja hyödynnä asiantuntijoita, joiden avulla voit tehostaa omaa liiketoimintaasi

Tiedosta riskit, suojaa toimintasi, toimi turvallisesti!

Suomalaisissa yrityksissä on herätty kyberturvallisuuteen toden teolla vasta viime vuosien aikana. Viimeistään nyt yrityksiin tarvitaan strategia kyberuhkien varalle, jossa arvioidaan laajasti liiketoimintaa ja tietopääomaa uhkaavia riskejä.

“Vapauden hinta on jatkuva valppaus”, sanoi jo Thomas Jeffersonkin. Sama pätee tietoturvaan ja kyberturvallisuuteen. Vaikka aina aika ajoin jokin taistelu voitettaisiin tai hävittäisiin, niin kilpailu voittajista ja häviäjistä jatkuu aina. Riittävin investoinnein tässä kilpailussa pysyy aina voitolla.

Varmista, että olet liikkeellä ajoissa.

Meidän tehtävämme on auttaa sinua.

Lähdetään yhdessä varmistamaan liiketoimintanne turvaamiseen keskittyvää kyberstrategiaa. Tehdään siitä teidän tarpeisiin sopiva.

Tutustu Elisan Tietoturvapalveluihin ja kysy lisää kyberturvallisuuden asiantuntijoiltamme:

Pasi Korhonen
Vice President

Näkemyksellinen liiketoiminnan johtaja, joka vuosikymmenten kokemuksella vastaa erikokoisten, useilla eri toimialoilla toimivien asiakkaiden tietoturvallisuustrategioiden kehittämisestä.

pasi.korhonen@elisa.fi
+ 358 50 506 0804

Petri Vilander
Cyber Security Manager

Tietoturvallisuusyksikön johdossa toimiva kyberasiantuntija, joka opastaa asiakkaita tietoturvallisuuden johtamisessa varmistaen, että tietoverkot ovat suojatut ja valmiit digitalisoitumaan.

petri.vilander@elisa.fi
+ 358 50 1964

Jaakko Wallenius
Chief Security Officer, Vice President

Yli 20 vuoden kokemuksen omaava kyber- ja tietoturvallisuuden johtaja, joka auttaa asiakkaita yhdistämään yrityksen osaamisen, liiketoiminnan kehittämisen ja sen johtamisen osaksi yrityksen kokonaisvaltaista turvallisuusstrategiaa.

jaakko.wallenius@elisa.fi
+ 358 50 525 0138

Johtajan muistilista avuksi kyberturvallisuus-palveluiden asiantuntemuk-sen hankkimiseksi:

1. Kartoita palveluntarjoajan kokonaispalveluosaaminen – varmista että korkealaatuista turvallisuusteknologiaa täydentävät myös sitä tukevat palvelut
2. Tarkastele tarjoajan palveluprosessia ja historiaa - miten tarjoaja hoitaa kriittiset ongelmatilanteet? Millainen on tarjoajan muutos-hallintaprosessi tai resurssien riittävyys?
3. Vertaile millaisia teknologiavaihtoehtoja toimittaja tarjoaa ja missä hankittavat palvelut tuotetaan?
5. Varmista myös toimittajan henkilöstön asiantuntijataso- mitä taustaselvityksiä henkilöstölle on tehty ja millaisia koulutuksia se on saanut?
6. Tunnista pitääkö toimittaja itseään turvallisuuden asiantuntijayrityksenä ja palveluosaajan vai teknologiatoimittajana?

Taitto, graafinen ulkoasu ja kuvat: **pasituomaala.com**