FAIR
Finnish AI Region | EDIH

Co-funded by the European Union

PIENI KYBER-TURVAL-LISUUS-OPAS

PK-YRITYKSILLE

2/2025

Kaikki, mitä tarvitset, on kättesi ulottuvilla

Sinua varten

FAIR
Finnish AI Region | EDIH

Tekstit: Martti Asikainen, Solja Sulkunen,
Jussi Rantsi ja Jenni Selosmaa
Toimitus ja taitto: Martti Asikainen
Kuvat: Adobe Stock Photos
https://www.fairedih.fi

sisältö

JOHDANTO

Tämä opas on suunnattu erityisesti pienille ja keskisuurille yrityksille sekä organisaatioille, joilla on rajallinen IT-osaaminen, mutta jotka haluavat hyödyntää tekoälyä liiketoiminnassaan turvallisesti ja vastuullisesti. Tekoälyn käyttöönotto tarjoaa merkittäviä mahdollisuuksia prosessien tehostamiseen, asiakaskokemuksen parantamiseen ja kilpailukyvyn vahvistamiseen. Samalla se tuo mukanaan uudenlaisia riskejä erityisesti tietoturvaan ja yksityisyyden suojaan liittyen.

Kyberturvallisuudella tarkoitamme tässä yhteydessä kaikkia niitä toimenpiteitä ja käytäntöjä, joilla pyritään suojaamaan yrityksen tai järjestön käyttämät tiedot, järjestelmät ja toiminnot luvattomalta pääsyltä, väärinkäytöltä, häirinnältä tai tuhoutumiselta. Tekoälyratkaisujen osalta tämä tarkoittaa esimerkiksi mallien ja datan suojaamista, käyttäjien tunnistamista sekä toimintojen läpinäkyvyyden ja jäljitettävyyden varmistamista eri mekanismein ja toiminnoin.

Koska tekoälyratkaisut kytkeytyvät usein laajoihin tietojärjestelmiin, ja hyödyntävät siten suuria määriä dataa, niiden turvallinen käyttöönotto edellyttää kokonaisvaltaista lähestymistapaa. Tämä ei suinkaan tarkoita pelkästään teknisiä ratkaisuja, vaan myös johdon sitoutumista, henkilöstön koulutusta ja selkeiden käytäntöjen ja pelisääntöjen luomista jokaiselle työyhteisön jäsenelle.

Pienen kyberturvaoppaamme tarkoituksena on tarjota sinulle selkeä ja käytännönläheinen lähestymistapa tekoälyn turvalliseen käyttöönottoon sekä tieto- ja kyberturvaosaamisen kehittämiseen yrityksessäsi. Mikäli käyttämämme termit eivät ole sinulle entuudestaan tuttuja, niin olemme lisänneet oppaamme loppuun pienen sanakirjan, joka helpottaa tekstin seuraamista.

NOPEA KATSAUS TOIMENPITEISIIN

Tekoälyn turvallinen käyttöönotto edellyttää useiden toisiaan tukevien tieto- ja kyberturvallisuustoimien yhdistämistä. Syötteiden huolellinen tarkistus ja puhdistus estävät haitallisten komentojen suorittamisen, kun taas vahva pääsynhallinta, salaus ja tietojen luokittelu suojaavat järjestelmän kriittisiä osia ja arkaluontoista dataa. Injektiohyökkäysten torjuminen, uhkien aktiivinen seuranta sekä säännölliset testaukset, kuten penetraatiotestit ja haavoittuvuusarvioinnit, parantavat järjestelmän resilienssiä. Koko henkilöstön kouluttaminen ja harjoittelu sekä selkeät toimintasuunnitelmat häiriötilanteiden varalta vahvistavat organisaation kykyä reagoida uhkiin nopeasti ja tehokkaasti. Tekoäly itsessään voi toimia sekä suojana että riskinä – siksi sen turvallinen hyödyntäminen edellyttää tietoturvan sisällyttämistä koko kehitysprosessin ja käytön ajaksi alusta alkaen. Tässä luvussa käymme lyhyesti läpi toimenpiteitä, joita voi tehdä välittömästi.

1. **Vahvojen pääsynhallintamekanismien käyttöönotto** on keskeistä tekoälyprojektien tietoturvan kannalta. Tehokas käyttöoikeuksien hallinta perustuu **vähimpien oikeuksien periaatteeseen**: kaikille käyttäjille ja järjestelmille tulisi myöntää vain ne oikeudet, jotka ovat välttämättömiä heidän työtehtäviensä suorittamiseen. Samalla tekoälyjärjestelmiin pääsy tulisi rajata vain niille henkilöille, jotka sitä todella tarvitsevat. Käyttöoikeudet tulee määritellä tarkasti sekä datan käytölle että toiminnallisille oikeuksille. Kriittisiin järjestelmiin on suositeltavaa ottaa käyttöön monivaiheinen tunnistautuminen, joka tuo merkittävän lisäkerroksen tietoturvaan. Käyttöoikeuksien säännöllinen tarkistaminen ja päivittäminen on myös tärkeä osa jatkuvaa tietoturvatyötä, sillä entiset käyttäjät ovat yhtä suuri tietoturvariski kuin nykyisetkin.

2. **Arkaluontoisten tietojen suojaaminen koko niiden elinkaaren ajan** on olennainen osa tekoälyprojektien tietoturvaa. Vahvan salauksen käyttö sekä tietojen säilytyksen että siirron aikana on ensiarvoisen tärkeää. Salausprotokollia tulee päivittää säännöllisesti vastaamaan uusimpia turvallisuusstandardeja, sillä kryptografian menetelmät kehittyvät jatkuvasti. On myös tärkeää tunnistaa ja luokitella yrityksesi tiedot niiden arkaluontoisuuden mukaan, jotta voidaan kohdistaa asianmukaiset suojaustoimenpiteet eri tietoluokkiin. Tekoälyjärjestelmät käsittelevät usein suuria määriä dataa, mikä tekee asianmukaisesta tietojen suojauksesta entistäkin tärkeämpää.

3. **Tekoälyjärjestelmät voivat olla erityisen alttiita erilaisille injektiohyökkäyksille**, joissa haitallista koodia syötetään järjestelmään. **SQL-injektiot** ovat yleisiä tietokantahyökkäyksiä, joissa hyökkääjä pyrkii manipuloimaan tietokantakyselyjä saadakseen luvattoman pääsyn tietoihin. Komentoinjektiot puolestaan yrittävät saada järjestelmän suorittamaan haitallisia komentoja. **XSS-hyökkäyksissä** (Cross-Site Scripting) hyökkääjät pyrkivät syöttämään haitallista skriptikoodia verkkosovelluksiin, joka sitten suoritetaan muiden käyttäjien selaimissa. Näiden hyökkäysten torjumiseksi on tärkeää käyttää turvallisia ohjelmointikäytäntöjä ja varmistaa, että kaikki syötteet tarkistetaan ja validoidaan huolellisesti.

4. **Tunkeutumisen havainnointi- ja estojärjestelmien käyttöönotto** on tärkeä osa ennakoivaa turvallisuutta. Näiden järjestelmien avulla voidaan aktiivisesti monitoroida verkon liikennettä ja tunnistaa epätavallisia toimintoja, jotka saattavat viitata tietoturvauhkaan. Automaattiset hälytykset epäilyttävästä toiminnasta mahdollistavat nopean reagoinnin mahdollisiin uhkiin. Jatkuva ja reaaliaikainen valvonta on välttämätöntä, sillä kyberuhkat kehittyvät jatkuvasti. Tekoälypohjaiset uhkien havaitsemisjärjestelmät voivat tunnistaa poikkeamia normaalista verkkoliikenteestä ja tunnistaa myös aiemmin tuntemattomia uhkia oppimalla verkkoympäristön tavallisista toimintamalleista.

5. **Säännöllisten turvallisuustestien toteuttaminen** on keskeistä järjestelmien haavoittuvuuksien tunnistamisessa ennen kuin hyökkääjät pääsevät hyödyntämään niitä. Penetraatiotestaus simuloi hyökkääjän toimintaa järjestelmää vastaan, mikä auttaa tunnistamaan ja korjaamaan tietoturva-aukkoja. Haavoittuvuusarvioinnit tarjoavat systemaattisen lähestymistavan heikkouksien tunnistamiseen eri järjestelmissä ja sovelluksissa. Koodin tarkastukset varmistavat, että tekoälyjärjestelmä noudattaa parhaita turvallisuuskäytäntöjä ja standardeja. Nämä testit tulisi toteuttaa säännöllisesti, sillä uusia haavoittuvuuksia löydetään jatkuvasti ja järjestelmät muuttuvat päivitysten myötä.

ENNAKOINNISTA HÄIRIÖTILANTEISIIN

Selkeät ja dokumentoidut toimintaohjeet eri kyberuhkien varalle ovat olennainen osa vahvaa kyberturvallisuusstrategiaa. Yritysten on varauduttava muun muassa palvelunestohyökkäyksiin (DoS, DDoS), tietomurtoihin, haittaohjelmatartuntoihin ja lunnashaittaohjelmiin, jotka voivat vaarantaa järjestelmän toiminnan tai johtaa arkaluontoisten tietojen katoamiseen tai väärinkäyttöön. Nopean ja tehokkaan reagoinnin edellytyksenä on, että ohjeistus on helposti saatavilla ja henkilöstön tiedossa. Harjoitusten ja simuloitujen häiriötilanteiden avulla työntekijät voivat oppia tunnistamaan roolinsa ja vastuunsa kriisitilanteessa.

On tärkeää muistaa, että usein **kyberturvallisuuden heikoin lenkki on ihminen**. Siksi säännöllinen koulutus koko henkilöstölle on keskeinen keino vähentää riskejä ja lisätä tietoturvatietoisuutta. Simuloidut tietojenkalastelukampanjat, selkeät toimintakäytännöt ja tekoälyn turvallisuuteen liittyvä koulutus auttavat luomaan organisaatiokulttuurin, jossa tietoturva otetaan vakavasti ja jokainen ymmärtää oman vastuunsa. Kyberturvallisuus ei ole yksittäinen projekti vaan jatkuva prosessi, joka vaatii pitkäjänteistä työtä, seurantaa ja resurssien kohdentamista.

Teknologian ja uhkaympäristön kehittyessä myös tarkistuslistoja, protokollia ja suojaustoimia on päivitettävä säännöllisesti. Turvallisten ohjelmointikäytäntöjen noudattaminen, alakohtaisten tietoturvakehysten hyödyntäminen ja erikoistuneiden tietoturvaohjelmistojen käyttö vahvistavat järjestelmän suojausta ja auttavat tunnistamaan haavoittuvuudet ennen kuin niitä ehditään käyttää hyväksi. Tekoälyllä on kaksoisrooli kyberturvallisuudessa: se voi sekä parantaa että heikentää turvallisuutta. Tekoälypohjaiset ratkaisut kykenevät analysoimaan suuria tietomääriä, tunnistamaan poikkeavuuksia ja automatisoimaan turvallisuustehtäviä, mutta samaan aikaan rikolliset voivat hyödyntää tekoälyä yhä kehittyneempiin hyökkäyksiin.

Tekoälyä käytetään esimerkiksi uskottavien huijausten laatimiseen ja järjestelmien heikkouksien automatisoituun etsimiseen. Näihin uhkiin varautuminen vaatii ajankohtaista osaamista ja jatkuvaa valppautta.

Turvallisuussuunnittelun tulisi alkaa jo tekoälyjärjestelmien kehityksen alkuvaiheessa. Kun tietoturva rakennetaan järjestelmän arkkitehtuuriin alusta alkaen, säästytään myöhemmiltä korjaustoimilta, jotka ovat usein sekä tehottomia että kalliita. Tämä ennakoiva lähestymistapa, eli "**security by design**", mahdollistaa tietoturvan saumattoman integroinnin osaksi järjestelmän toimintaa.

Pk-yrityksissä tekoälyn turvallinen käyttöönotto edellyttää kokonaisvaltaista otetta kyberturvallisuuteen. Syötteiden suojaaminen, käyttöoikeuksien hallinta, datan salaus ja injektiohyökkäysten estäminen muodostavat perustan turvalliselle tekoälyratkaisulle. Näiden rinnalla tulee kehittää toimintatapoja uhkien havaitsemiseksi, säännöllistä testausta ja jatkuvaa varautumista erilaisiin häiriötilanteisiin. Samalla on tärkeää tunnistaa inhimillinen tekijä ja varmistaa henkilöstön sitoutuminen tietoturvakulttuuriin.

Kyberturvallisuus ei ole tila, joka saavutetaan ja unohdetaan, vaan jatkuva prosessi, joka vaatii huomiota, osaamista ja kehittämistä. Tekoäly voi olla tehokas työkalu turvallisuuden vahvistamisessa, mutta se voi myös avata uusia hyökkäysreittejä. Siksi tarvitset yrityksessäsi myös jatkuvaa arviointia, koulutusta ja ennakoivia toimenpiteitä.

Oppaamme lopussa tarjoamme linkkejä hyödyllisiin materiaaleihin, koulutuksiin ja palveluihin, jotka tukevat yritystäsi matkallasi. Muistathan, että **kyberturvallisuus ei ole määränpää** – vaan se on jatkuvan sopeutumisen ja oppimisen prosessi.

KYBERTURVALLISUUS KÄYTÄNNÖSSÄ

Selkeät toimintaohjeet
Dokumentoidut toimintamallit auttavat reagoimaan palvelunestohyökkäyksiin, tietomurtoihin ja haittaohjelmiin tehokkaasti ja nopeasti.

Säännöllinen koulutus
Koko henkilöstön kouluttaminen vahvistaa tietoturvatietoisuutta kokonaisvaltaisesti ja ehkäisee samalla inhimillisiä virheitä.

Jatkuva prosessi
Kyberturvallisuus vaatii jatkuvaa seurantaa, testausta ja suojaustoimien päivittämistä.

Tekoälyn kaksoisrooli
Tekoäly voi parantaa turvallisuutta, mutta sitä voidaan käyttää myös kehittyneisiin hyökkäyksiin

Turvallisuussuunnittelu alusta alkaen
Security by design -periaate tarkoittaa sitä, että suojaus rakennetaan osaksi järjestelmän arkkitehtuuria jo kehitysvaiheessa.

Kokonaisvaltainen lähestymistapa
Turvallinen tekoälyn käyttöönotto edellyttää teknisten, organisatoristen ja inhimillisten tekijöiden huomioimista.

MITÄ EROA ON TIETOTURVALLA JA KYBERTURVALLA?

Tietoturva ja kyberturvallisuus, vaikka niitä usein käytetään ammattikielessä vaihtoehtoisina termeinä, edustavat erillisiä lähestymistapoja organisaation voimavarojen suojaamiseen. Vaikka aloilla on huomattavaa päällekkäisyyttä, niiden erojen vivahteellinen ymmärtäminen on olennaista organisaatioille, jotka kehittävät vahvoja turvallisuuskehyksiä. Tietoturva käsittää tietovarojen suojaamisen niiden muodosta riippumatta – olivatpa ne digitaalisia, fyysisiä tai älyllisiä. Tämä tieteenala noudattaa CIA:n turvallisuuskolmion perusperiaatteita: tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Tietoturvan laajuus ulottuu kaikkiin tietomuotoihin, mukaan lukien fyysiset asiakirjat, suulliset tiedonvaihdot ja henkilöstön hallussa oleva institutionaalinen tieto.

Kyberturvallisuus sitä vastoin käsittelee erityisesti digitaalisten omaisuuserien suojaamista kyberalueelta tulevilta uhkilta. Sen ensisijainen painopiste on järjestelmien, verkkojen ja digitaalisen infrastruktuurin puolustaminen virtuaaliympäristöissä tapahtuvalta haitalliselta toiminnalta. Vaikka tietoturva on ollut olemassa siitä lähtien, kun organisaatiot ensimmäisen kerran tunnistivat tarpeen suojata arkaluonteisia tietoja, kyberturvallisuus syntyi samanaikaisesti tietokoneverkkojen ja digitaalisten teknologioiden leviämisen kanssa.

> “
> **TIETOTURVAN JA KYBERTURVALLISUUDEN KESKEINEN ERO NÄKYY NIIDEN LAAJUUDESSA SEKÄ TOIMINTAPERIAATTEISSA.**
> “

Perustavanlaatuinen ero on laajuudessa: tietoturva toteuttaa kattavia käytäntöjä kaikkien tietomuotojen suojaamiseksi, kun taas kyberturvallisuus keskittyy erityisesti teknologisiin puolustuksiin digitaalisia uhkia vastaan. Tietoturvaprotokollat voivat sisältää fyysisiä suojatoimenpiteitä, kuten asiakirjojen turvallisen hävittämisen menetelmiä tai työtilojen turvallisuuskäytäntöjä, kun taas kyberturvallisuus hyödyntää teknisiä toimenpiteitä, kuten verkon palomuureja, tunkeutumisen havainnointijärjestelmiä ja haavoittuvuuksien hallintakehyksiä.

Tällä erolla on merkitystä, koska tehokas turvallisuusarkkitehtuuri edellyttää molempien lähestymistapojen integrointia. Organisaatiot, jotka keskittyvät yksinomaan kyberturvallisuuteen, ovat vaarassa laiminlyödä fyysiset tietovaransa tai sisäisten uhkien vektorit, kun taas ne, jotka painottavat perinteistä tietoturvaa, saattavat kärsiä riittämättömistä teknisistä puolustuskeinoista kehittyneitä kyberhyökkäyksiä vastaan. On tärkeää huomata, että kyberturvallisuushyökkäykset sisältävät myös kaikenlaiset pahantahtoiset vaikuttamisoperaatiot. Kyberrikoksia motivoivat usein taloudelliset motiivit, joskus poliittiset ohjelmat, mutta joskus niitä voidaan toteuttaa yksinkertaisesti “huvin vuoksi” – vain koska joku pystyy siihen.

Organisaatioympäristöjen digitalisoituessa entistäkin enemmän myös näiden tieteenalojen välinen raja jatkaa kaventumistaan. Tehokkaimmat turvallisuusohjelmat sisältävät molemmat näkökulmat ja tunnustavat, että kattava tietosuoja edellyttää sekä digitaalisen että fyysisen tiedon sijainnin suojaamista.

KESKEISET VINKKIMME PK-YRITYKSILLE

Pienet ja keskisuuret yritykset (pk-yritykset) kohtaavat yhä monimutkaisempia haasteita digitaalisessa toimintaympäristössä. Niiltä odotetaan samanlaista tietosuojaa kuin suurilta organisaatioilta, mutta käytettävissä olevat resurssit ovat usein rajalliset. Tässä tilanteessa on tärkeää ymmärtää ero tietoturvan ja kyberturvallisuuden välillä, jotta niukat resurssit voidaan kohdentaa mahdollisimman tehokkaasti.

Tietoturva kattaa kaiken yrityksen tiedon suojelun riippumatta siitä, onko tieto digitaalisessa, fyysisessä tai inhimillisessä muodossa. Tämä sisältää esimerkiksi asiakasrekisterit, taloustiedot, liiketoimintaprosessit ja työntekijöiden hiljaisen tiedon. Kyberturvallisuus taas keskittyy digitaalisiin uhilta suojautumisen keinoihin, kuten palomuureihin, haittaohjelmien torjuntaan ja verkkoinfrastruktuurin turvaamiseen. Vaikka pk-yrityksillä ei ole usein mahdollisuutta ylläpitää omaa tietoturvatiimiä, ne voivat silti saavuttaa korkean turvallisuustason strategisella lähestymistavalla. Suosittelemme pk-yrityksille strategiaa, joka käsittelee molempia toimialueita seuraavien toimenpiteiden avulla:

- Tietoturvan osalta pk-yritysten tulisi luoda selkeät käytännöt tiedon käsittelyyn, luokitella arkaluontoiset tiedot, ottaa käyttöön perusmuotoiset fyysiset suojatoimet ja tarjota koko henkilöstölle säännöllistä tietoisuuskoulutusta. Nämä toimet eivät vaadi suuria investointeja, mutta voivat merkittävästi vähentää altistumista yleisille uhille.

- Kyberturvallisuuden osalta valikoiva ulkoistaminen hallituille tietoturvapalveluille (MSSP) voi osoittautua kustannustehokkaimmaksi vaihtoehdoksi. Ulkopuoliset asiantuntijat voivat tarjota yritystason suojaa, jatkuvaa valvontaa ja nopeaa reagointia uhkatilanteissa murto-osalla sisäisen tiimin kustannuksista. Pk-yritysten kannattaa valita palveluntarjoajia, jotka hallitsevat toimialakohtaiset vaatimukset ja pystyvät tukemaan vaatimustenmukaisuutta.

- Pilvipohjaiset tietoturvaratkaisut tarjoavat kustannustehokkaan keinon parantaa suojausta. Tilausperusteiset mallit mahdollistavat pääsyn kehittyneisiin teknologioihin ilman merkittäviä alkuinvestointeja. Lisäksi yhteistyö turvallisuuskonsulttien kanssa voi tuoda arvokasta näkemystä ja varmistaa säännöllisen arvioinnin. Esimerkiksi neljännesvuosittaiset tai puolivuosittaiset tarkastukset voivat tarjota jatkuvaa valvontaa ilman pysyviä henkilöstökustannuksia.

- Kyberturvallisuusvakuutukset täydentävät teknisiä ja organisatorisia toimenpiteitä tarjoamalla taloudellista suojaa vahinkojen varalta. Pk-yritysten on kuitenkin tärkeää varmistaa, että vakuutus kattaa niiden erityiset riskit ja toimintaympäristön.

Kuten toimenpiteet osoittavat, niin tehokas tieto- ja kyberturvallisuus ei välttämättä vaadi huomattavia taloudellisia resursseja. Sen sijaan se vaatii saatavilla olevien resurssien harkittua kohdentamista, joka perustuu selkeään ymmärrykseen organisaation riskeistä.

Erottamalla tietoturva- ja kyberturvallisuusvaatimukset toisistaan pk-yritykset voivat kehittää kontrolliaan oikeassa suhteessa, joka suojaa liiketoimintaa ilman huomattavia kustannuksia. Paras lähestymistapa yhdistää valikoiva ulkoistaminen ja sisäisen osaamisen kehittäminen. Kouluttamalla olemassa olevaa henkilöstöä turvallisuuden perusteisiin voidaan rakentaa kestävää asiantuntemusta, joka vahvistaa organisaation kykyä toimia itsenäisesti ja arvioida ulkoisten kumppaneiden työtä kriittisesti.

HAAVOITTUVUUKSIEN HALLINTAKEHYKSET

Haavoittuvuuksien hallintakehykset ovat jäsenneltyjä toimintamalleja, joiden avulla pk-yritykset voivat tunnistaa, arvioida ja korjata tietoturvaheikkouksia järjestelmissään ja ohjelmistoissaan. Nämä kehykset luovat johdonmukaiset prosessit turvallisuusriskien hallintaan.

Haavoittuvuuksien hallintakehysten avulla pk-yritys kykenee muun muassa:

- löytämään haavoittuvuuksia säännöllisten skannausten, testausten ja valvonnan avulla
- arvioimaan kunkin haavoittuvuuden vakavuuden ja mahdollisen vaikutuksen liiketoimintaan
- priorisoimaan riskit suuruuden, hyödynnettävyyden ja liiketoimintavaikutusten perusteella
- tukemaan korjausprosessin seurantaa
- varmistamaan, että haavoittuvuudet käsitellään asianmukaisesti
- mahdollistamaan selkeän raportoinnin haavoittuvuuksien tilasta koko pk-yrityksessä

Tunnetuimpia haavoittuvuuksien hallintakehyksiä ovat NIST-kehys (erityisesti SP 800-40), CIS Controls, ISO 27001/2 standardit sekä OWASP-standardit verkkosovelluksille. Nämä tarjoavat testatut menetelmät organisaation hyökkäyspinnan pienentämiseksi ja vahvan turvallisuusaseman ylläpitämiseksi myös uusien uhkien ilmaantuessa. PK-yrityksille, joilla on rajalliset resurssit, nämä kehykset voidaan soveltaa kevyemmin keskittyen kriittisimpiin järjestelmiin. Näinkin toteutettuna ne tarjoavat järjestelmällisen suojan kehittyviä kyberuhkia vastaan.

YLEISIMMÄT HAAVOITTUVUUDET TOIMITUSKETJUISSA

Kun puhutaan haavoittuvuuksien hallinnasta, niin on selvää, ettei toimitusketjujen haavoittuvuuksia voida sivuuttaa. Kyberturvallisuus on vain niin vahva kuin sen heikoin lenkki – ja ihmisten tavoin myös toimitusketju muodostaa usein kriittisen heikkouden. Kun pk-yritys käyttää ulkoisia toimittajia, alihankkijoita tai ohjelmistokomponentteja, sen hyökkäyspinta laajenee merkittävästi.

Toimitusketjujen haavoittuvuudet voivat liittyä muun muassa seuraaviin riskeihin:

1. **Ohjelmistokomponentit:** Avoimen lähdekoodin kirjastot ja kolmannen osapuolen komponentit voivat sisältää haavoittuvuuksia, jotka periytyvät suoraan lopputuotteeseen.
2. **Toimittajien pääsy järjestelmään:** Ulkoisilla kumppaneilla voi olla pääsy yrityksen kriittisiin järjestelmiin ja tietoihin. Jos heidän omat suojaustoimensa ovat puutteelliset, riskit realisoituvat toisinaan hyvinkin nopeasti.
3. **Laitteistohaavoittuvuudet:** Laitekomponentit tai laiteohjelmistot voivat sisältää tahattomia tai tahallisia haavoittuvuuksia jo valmistusvaiheessa.
4. **Päivitys- ja jakelukanavat:** Hyökkääjät voivat saastuttaa ohjelmistoja hyökkäämällä niiden päivitysmekanismeihin.

Erityisen vaikeasti havaittavia ovat ns. upstream-haavoittuvuudet eli sellaiset tilanteet, joissa esimerkiksi ohjelmistokirjasto käyttää toista kirjastoa, joka puolestaan sisältää haavoittuvuuden. Tämä tekee ongelman jäljittämisestä monimutkaista, ja toisinaan jopa lähes mahdotonta.

> **“ NOLLALUOTTAMUKSEN PERIAATETTA SOVELLETAAN MYÖS YHTEISTYÖ-KUMPPANEIHIN. ”**

Toimitusketjun suojaaminen edellyttää monitasoista lähestymistapaa. Aloita tekemällä säännöllisiä toimittajien turvallisuusarviointeja ja sisällytä auditointivaatimuksia sekä turvallisuusvaatimuksia suoraan sopimuksiin. Osana kehitysprosessia kannattaa toteuttaa koodin tarkastuksia ja haavoittuvuusskannauksia erityisesti silloin, kun otetaan käyttöön kolmannen osapuolen komponentteja.

Samalla on tärkeää soveltaa aikaisemmin mainitsemaamme niin kutsuttua nollaluottamusperiaatetta (eng. zero trust) myös ulkoisiin kumppaneihin. Kaikkien toimijoiden – niin sisäisten kuin ulkoisten – tulisi toimia nollaluottamusperiaatteiden mukaisesti. Myös toimitusketjun kokonaiskuvan ymmärtäminen on ratkaisevaa.

Kartoitus kaikista riippuvuuksista ja toimittajista tuo näkyviin ne riskikohdat, jotka muuten voisivat jäädä piiloon. Kun tähän yhdistetään kyky reagoida nopeasti uusiin haavoittuvuuksiin ja ottaa korjaukset viipymättä käyttöön, yrityksellä on huomattavasti paremmat edellytykset puolustautua yhä kehittyneempiä toimitusketjuhyökkäyksiä vastaan.

MUISTA TÄMÄ TOIMITUSKETJUN HAAVOITTUVUUKSISTA

Toimitusketjut edustavat usein kyberturvallisuuden heikoimpia lenkkejä. Ulkoisten toimittajien käyttöön luottaminen laajentaa merkittävästi mahdollista hyökkäyspintaa.

1. **Ohjelmistokomponentit:** Kolmannen osapuolen komponentit voivat sisältää haavoittuvuuksia, jotka vaarantavat järjestelmän turvallisuuden.
2. **Toimittajien järjestelmäkäyttöoikeudet:** Ulkoiset kumppanit voivat saada luvattoman pääsyn kriittisiin järjestelmiin ja arkaluontoisiin tietoihin.
3. **Laitteistohaavoittuvuudet:** Fyysiset laitteet voivat sisältää tahallisia takaovia tai tahattomia tietoturva-aukkoja.
4. **Päivitys- ja jakelukanavat:** Hyökkääjät voivat vaarantaa ohjelmistopäivitysmekanismit levittääkseen haitallista koodia.

Tehokas suojaaminen vaatii kattavan, monikerroksisen lähestymistavan:

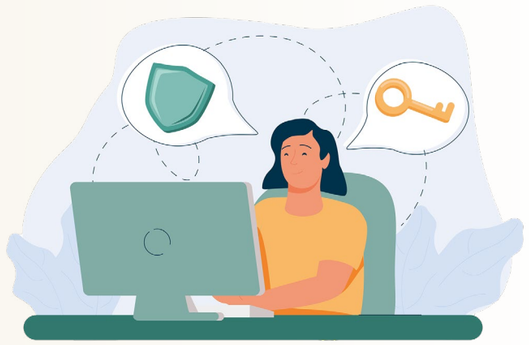
- Kaikkien toimittajien säännöllisten turvallisuusarviointien suorittaminen
- Zero-trust-periaatteiden toteuttaminen kaikissa kumppanuuksissa
- Yksityiskohtaisten riippuvuuksien ja toimittajasuhteiden inventaarion ylläpitäminen

KATTAVAN TIETOTURVARAKENTEEN RAKENTAMINEN TYHJÄSTÄ

Tietoturvan vahvistamiseksi suosittelemme ottamaan käyttöönne **tunkeutumisen havaitsemis- ja estojärjestelmät** (IDS/IPS), jotka valvovat luvattomia pääsyyrityksiä ja reagoivat niihin reaaliajassa. Nämä järjestelmät toimivat digitaalisina vartioina, hälyttäen tietoturvahenkilöstöä epäilyttävästä toiminnasta ja estäen uhkat automaattisesti. Myös vähäisillä IT-resursseilla toimivat organisaatiot voivat hyödyntää perusvalvontaratkaisuja, jotka tarjoavat kriittisen näkyvyyden mahdollisiin tietoturvaongelmiin ja tunkeutumisyrityksiin.

Säännöllinen tietoturvan testaaminen, erityisesti tunkeutumistestaus, auttaa tunnistamaan haavoittuvuudet ennen niiden hyväksikäyttöä. Nämä ennakoivat arvioinnit jäljittelevät todellisia hyökkäysskenaarioita paljastaen järjestelmien ja prosessien kriittiset heikkoudet. Vaikka kattava tunkeutumistestaus vaatii usein ulkopuolista asiantuntemusta, pienemmätkin organisaatiot voivat hyötyä yksinkertaistetuista haavoittuvuusskannauksista ja tekoälysovellusten tietoturvatarkistuslistoista.

Lisäksi on myös suositeltavaa, että yritys laatii selkeän **toimintasuunnitelman** palvelunesto-hyökkäysten, tietoturvamurtojen ja muiden kriittisten insidenttien varalle. Tehokas insidentinhallinta varmistaa nopean ja koordinoidun reagoinnin uhkatilanteissa, mikä puolestaan **minimoi vahingot ja lyhentää palautumisaikaa**. Hyvin dokumentoidut menettelytavat tarjoavat myös arvokasta tukea jopa akuutin kriisin aiheuttamassa stressitilanteessa.



On myös tärkeää ymmärtää, että **suurin kyberturvallisuusriski on ihminen itse**. Maailman talousfoorumin Global Risks Report -raportin (2022) mukaan peräti 95 prosenttia tietoturvaongelmista johtuu inhimillisistä virheistä. Nämä virheet voivat olla moninaisia: työntekijät lankeavat tietojenkalastelupetoksiin, käyttävät heikkoja salasanoja tai jakavat vahingossa arkaluonteista tietoa väärille henkilöille. Tällaiset laiminlyönnit voivat kumota kehittyneimmätkin suojatoimet.

Inhimillisten virheiden ja sosiaalisen manipuloinnin aiheuttamien riskien vuoksi yritysten on investoitava henkilöstön koulutukseen ja tietoisuuden lisäämiseen. **Säännöllinen tietoturvakoulutus** opettaa työntekijöitä tunnistamaan ja torjumaan manipulointiyrityksiä, kuten tietojenkalasteluviestejä ja petollisia yhteydenottoja. Erityisesti teknisesti rajallisemmille organisaatioille inhimillisten tekijöiden huomioiminen tietoturvassa tarjoaa merkittävän suojan kohtuullisilla investoinneilla.

MITÄ PK-YRITYS VOI TEHDÄ TIETOMURRON SATTUESSA?

Etukäteen laadittu incidentinhallintasuunnitelma lyhentää merkittävästi reagointiaikaa ja minimoi tietomurrosta aiheutuvat vahingot. Jopa selkeä perustason dokumentti, jossa määritellään keskeiset vastuut ja toimenpiteet, voi osoittautua elintärkeäksi tietoturvakriisin aikana. Jos pk-yrityksesi joutuu tietomurron kohteeksi, välitön ja järjestelmällinen toiminta on ratkaisevaa.

TÄSSÄ KAHDEKSAN KRIITTISTÄ TOIMENPIDETTÄ HÄTÄTILANTEESEEN:

1. **Eristä uhka välittömästi** – Katkaise vaarantuneiden järjestelmien verkkoyhteydet estääksesi lisävahingot ja tietojen leviämisen.

2. **Selvitä vahingon laajuus** – Tunnista vaarantuneet tiedot, murron toteutustapa ja mahdolliset uhrit. Dokumentoi havainnot huolellisesti.

3. **Täytä ilmoitusvelvollisuus** – GDPR-lainsäädäntö edellyttää merkittävien tietomurtojen ilmoittamista viranomaisille 72 tunnin kuluessa Suomessa ja koko EU:ssa.

4. **Informoi sidosryhmiä läpinäkyvästi** – Ota yhteyttä vaikutuksen kohteisiin: asiakkaisiin, kumppaneihin ja työntekijöihin, joiden henkilötiedot saattavat olla vaarantuneet.

5. **Pidä tarkkaa kirjaa kaikesta** – Dokumentoi jokainen vaihe reagointiprosessissa lakisääteistä raportointia ja mahdollisia vakuutuskorvauksia varten.

6. **Korjaa turva-aukot kiireellisesti** – Paikka haavoittuvuudet, jotka mahdollistivat tietomurron, ja päivitä tietoturvaprotokollat välittömästi.

7. **Turvaudu asiantuntija-apuun** – Vakavien tapausten yhteydessä konsultoi kyberturvallisuus- ja tietoturva-asiantuntijoita, lakimiehiä tai kriisinhallintaeksperttejä.

8. **Ota opikseksi** – Analysoi tapahtunut perusteellisesti ja kehitä tietoturvakäytäntöjäsi tunnistettujen puutteiden perusteella.

Valmistautuminen on paras suojasi. Hyvin suunniteltu ja harjoiteltu toimintamalli mahdollistaa ammattitaitoisen ja harkitun reagoinnin kriisitilanteessa. Kun tiimisi tietää tarkalleen, mitä tehdä, vältytään paniikkipäätöksiltä ja kalliilta virheiltä paineen alla. Säännöllinen suunnitelman läpikäynti ja päivitys varmistavat sen toimivuuden todellisessa hätätilanteessa.

TIETOTURVAN INTEGROINTI OSAKSI YRITYSTÄ

Kaikille yrityksille, jotka operoivat internetissä näkyviä palveluita tai sisäisiä työkaluja – olivatpa ne tekoälypohjaisia tai eivät – kyberturvallisuuden tulee olla jatkuva prioriteetti. Tämä sisältää tyypillisesti yhdistelmän henkilöstökoulutusta, jäsenneltyjä tietoturvatarkistuslistoja, parhaiden koodauskäytäntöjen noudattamista, kyberturvallisuusviitekehysten ja erikoisohjelmistojen käyttöä sekä säännöllisiä auditointeja ja prosessikatselmuksia.

Rajallisin teknisin resurssein toimivat organisaatiot voivat vastata näihin vaatimuksiin tehokkaasti yhdistämällä ulkoistamista, pilvipalvelupohjaisia tietoturvaratkaisuja ja kohdennettuja sisäisiä aloitteita. Tietoturvaviitekehykset, kuten NIST:n kyberturvallisuusviitekehys, tarjoavat jäsenneltyä ohjausta, joka voidaan sovittaa organisaation kokoon ja monimutkaisuuteen. Vastaavasti pilvipalveluntarjoajat tarjoavat yhä kehittyneempiä tietoturvatyökaluja, jotka vaativat minimaalista teknistä asiantuntemusta käyttöönotossa.

Tekoäly itsessään näyttelee kriittistä roolia sekä kyberturvallisuuden vahvistamisessa että uhkaamisessa. Tekoälyyn liittyvien kehitysprojektien tietoturvariskien hallinta tulisi aloittaa varhaisessa vaiheessa kalliiden yllätysten välttämiseksi myöhemmissä käyttöönottovaiheissa. Tämä "*security by design*" -lähestymistapa integroi suojatoimet koko kehityselinkaaren ajaksi sen sijaan, että niitä yritettäisiin lisätä jälkikäteen. Tämä on tyypillisesti paitsi tehokkaampi myös taloudellisempi vaihtoehto.

> **MUTTA EIHÄN MINULLA OLE ARKALUONTOISTA TIETOA?**
>
> Tiesitkö, että yleisen tietosuoja-asetuksen alaisuuteen kuuluu kaikki henkilöihin liittyvä tieto. Jos sinulla on asiakkaita ja/tai työntekijöitä, niin silloin sinulla on myös tietosuoja-asetuksen alaista arkaluontoista tietoa.

Samaan aikaan pahantahtoiset toimijat käyttävät tekoälyä yhä kehittyneempien kyberhyökkäysten luomiseen, kun taas kyberturvallisuustyökalut hyödyntävät tekoälyä uhkien havaitsemisessa ja neutraloimisessa tehokkaammin. Tämä teknologinen kilpavarustelukilpailu tekee jatkuvasta tietoturvatietoisuudesta erityisen tärkeää tekoälyratkaisuja toteuttaville organisaatioille. Sekä tekoälyteknologioiden suojakykyjen että mahdollisten haavoittuvuuksien ymmärtäminen auttaa organisaatioita tekemään tietoisia päätöksiä niiden käyttöönotosta ja suojaamisesta.

MERKITYS KOROSTUU ENTISESTÄÄN TEKOÄLYN MYÖTÄ

Kyberuhkien lisääntyessä integraatioiden tietoturva on noussut yhdeksi keskeiseksi painopisteeksi jokaisessa yrityksessä. API-rajapintojen käyttö arkaluonteisten tietojen käsittelyssä on kasvanut, mikä tekee näiden yhteyksien suojaamisesta kriittistä.

Integraatio-ongelmat tai tietomurrot voivat aiheuttaa merkittäviä operatiivisia häiriöitä. Uudet säädökset, kuten NIS2 ja DORA, lisäävät vaatimustenmukaisuuden painetta. Niiden myötä yritysten odotetaan kiinnittävän yhä enemmän huomiota tietoturvaan suojautuakseen kyberuhkilta ja varmistaakseen säädösten noudattamisen.

KESKEISET KYSYMYKSET

Integraatio- ja tietoturvatiimit joutuvat usein pohtimaan:

- Ovatko integraatiototeutuksemme ja -alustamme turvallisia?
- Noudattavatko kehittäjät turvallisia käytäntöjä?
- Ovatko toimintamallimme vaatimuksenmukaisia?

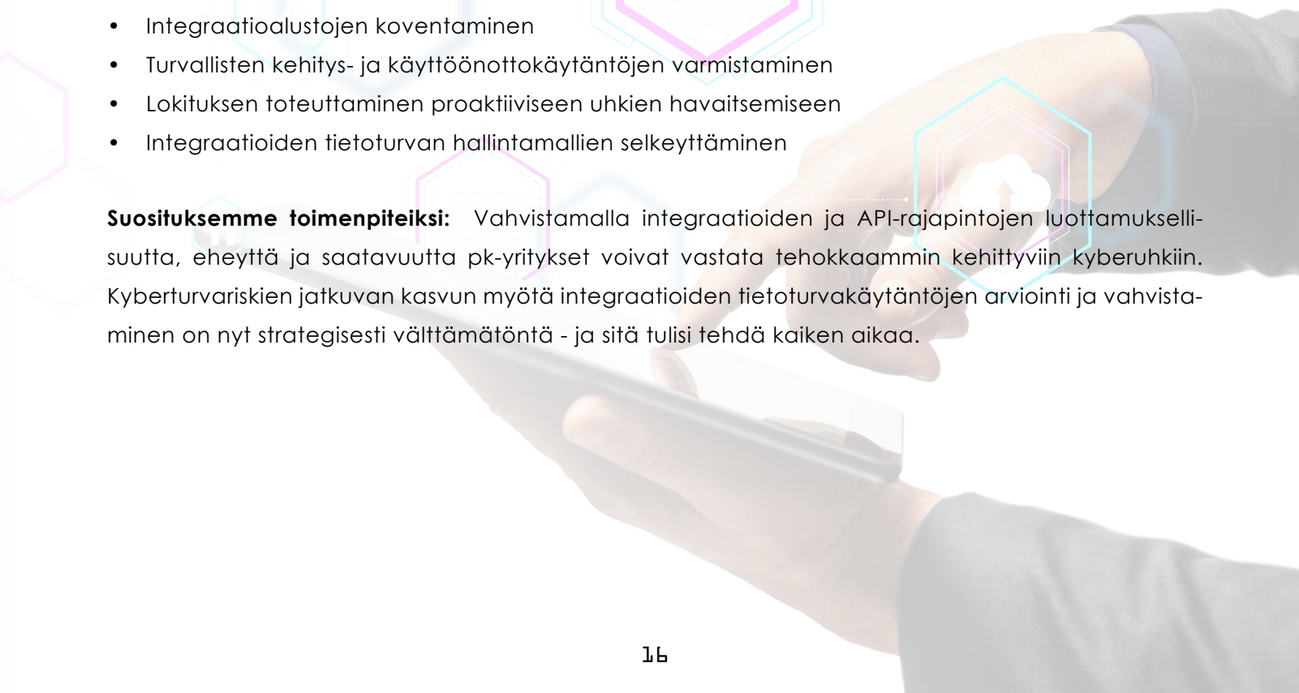
Pohdi hetki, miten yrityksessänne on pyritty vastaamaan edellä mainittuihin kysymyksiin? Ymmärrätkö, mitä ne tarkoittavat? Entä ovatko tietonne vaatimuksista ajankohtaiset?

TYYPILLISIMMÄT VAHVISTAMISTA KAIPAAVAT OSA-ALUEET

Vaikka useimmat pk-yritykset tunnistavat jo tänä päivänä riskit, niin monet tarvitsevat yhä apua niiden systemaattiseen käsittelyyn. Tyypillisimmät vahvistamista kaipaavat osa-alueet yrityksissä ovat:

- Integraatioalustojen koventaminen
- Turvallisten kehitys- ja käyttöönottokäytäntöjen varmistaminen
- Lokituksen toteuttaminen proaktiiviseen uhkien havaitsemiseen
- Integraatioiden tietoturvan hallintamallien selkeyttäminen

Suosituksemme toimenpiteiksi: Vahvistamalla integraatioiden ja API-rajapintojen luottamuksellisuutta, eheyttä ja saatavuutta pk-yritykset voivat vastata tehokkaammin kehittyviin kyberuhkiin. Kyberturvariskien jatkuvan kasvun myötä integraatioiden tietoturvakäytäntöjen arviointi ja vahvistaminen on nyt strategisesti välttämätöntä - ja sitä tulisi tehdä kaiken aikaa.



TOP5 PK-YRITYSTEN KYBERTURVALLISUUSSTRATEGIAT BUDJETTIA SILMÄLLÄ PITÄEN

1. RAKENNA IHMISPALOMUURI KOHDENNETUN KOULUTUKSEN AVULLA

Yleisluontoisten tietoturvakoulutusten sijaan kehitä räätälöityä koulutusta, joka pureutuu juuri sinun yrityksesi haavoittuvuuksiin. Rakenna todellisuutta vastaavia harjoitusskenaarioita, jotka mallintavat työntekijöidesi kohtaamia uhkia, kuten tekoälyn avulla luotuja kalasteluviestejä, jotka jäljittelevät yrityksesi viestintätyyliä. Valitse jokaiselta osastolta "tietoturvalähettiläitä", jotka saavat syventävää koulutusta ja toimivat lähitukena tietoturvakysymyksissä. Tämä ihmislähtöinen toimintamalli muuntaa tietoturvan pelkästä IT-asiasta koko henkilöstön yhteiseksi vastuuksi ilman merkittäviä kustannuksia. Todenna kehitys mittaamalla tuloksia simuloiduilla kalastelutesteillä ennen ja jälkeen koulutusten, jolloin voit osoittaa sijoituksen hyödyt ja kehittää toimintamallia edelleen. Pienyrityksillekin on tarjolla maksuttomia työkaluja, joiden avulla tietoturvaa voi parantaa ilman erillistä turvallisuustiimiä.

2. OTA KÄYTTÖÖN VAIHEITTAINEN ZERO TRUST -ARKKITEHTUURI

Unohda perinteiset palomuuriajattelut. Kehitä organisaatiossasi asteittain zero trust -lähestymistapaa—"älä koskaan luota, varmistu aina"—pelkkien ulkokehän puolustusten sijaan. Aloita käytännönläheisillä, kustannustehokkailla toimenpiteillä: jaa verkkosi loogisiin osiin suojataksesi kriittiset järjestelmät, ota käyttöön tarkat käyttöoikeudet selkeiden roolikuvausten pohjalta ja edellytä monivaiheista tunnistautumista arkaluontoisiin tietoihin. Jokainen harkittu parannus vahvistaa tietoturvaasi merkittävästi ilman kalliita yritystason investointeja. Huomioi, että erityyppinen tieto vaatii erilaisen suojaustason. Aloita kaikkein arkaluontoisimmista tiedoista ja järjestelmistä, erityisesti tekoälysovelluksista jotka käsittelevät asiakastietoja. Tämä strategia varmistaa, että jokainen käyttäjä ja laite tunnistetaan ennen pääsyn myöntämistä sijainnista riippumatta. Muista noudattaa tiedon minimoinnin periaatetta—kerää ja säilytä vain toimintasi kannalta välttämätön tieto.

3. HYÖDYNNÄ TEKOÄLYLLÄ VARUSTETTUJA TIETOTURVATYÖKALUJA

Ota tekoäly käyttöön kilpailuetuna hyödyntämällä tietoturvatyökaluja, jotka käyttävät koneoppimista tarjotakseen yritystasoista suojaa PK-yritysten budjettiin sopivalla hinnalla. Useat kyberturvallisuuden tarjoajat ovat kehittäneet nimenomaan pienille ja keskisuurille yrityksille räätälöityjä tekoälyratkaisuja joustavilla hinnoittelumalleilla. Etsi yhdistettyjä tietoturvakokonaisuuksia, jotka sisältävät useita toimintoja samassa paketissa – virustorjunnan, palomuurin ja sähköpostisuojauksen – saadaksesi parhaan vastineen rahoillesi. Nämä mo dernit työkalut tunnistavat automaattisesti epäilyttävät

toimintamallit, havaitsevat haavoittuvuudet ennen kuin niitä ehditään hyödyntää ja sopeutuvat jatkuvasti kehittyviin uhkiin. Aiemmin tällaiset ominaisuudet olivat vain suuryritysten tietoturvakeskusten ulottuvilla. Myös pilvipohjaiset tietoturvapalvelut ovat varteenotettava vaihtoehto yrityksesi turvallisuustarpeisiin.

4. RISKIPERUSTEINEN TIETOTURVAN TIEKARTTA SELKEIN PRIORITEETEIN

Rakenna yrityksellesi priorisoitu tietoturvasuunnitelma todellisten liiketoimintariskien pohjalta kokonaisvaltaisen kertaratkaisun sijaan. Kartoita ensin yksinkertaisella riskiarvioinnilla arvokkaimpaat kohteesi – ne tiedot ja järjestelmät, joiden vaarantuminen aiheuttaisi vakavimmat seuraukset. Laadi kolmiportainen toteutussuunnitelma: kohdista resurssit ensin kriittisimpien kohteiden suojaamiseen ja laajenna suojausta asteittain resurssien puitteissa. Tällä strategisella lähestymistavalla varmistat, että rajallinen tietoturvabudjettisi suojaa juuri sitä, mikä on liiketoiminnallesi elintärkeää. Tarkastele ja päivitä arviotasi säännöllisesti kvartaaleittain liiketoimintasi ja uhkakuvan muuttuessa. Tämä on erityisen tärkeää ottaessasi käyttöön uusia tekoälyteknologioita. Jokaisella pk-yrityksellä, resurssien niukkuudesta huolimatta, tulisi olla selkeä toimintasuunnitelma tietoturvapoikkeamien varalle. Tämä ei edellytä monimutkaista teknologiaa. Riittää, että dokumentoit selkeästi vastuuhenkilöt ja toimenpiteet mahdollisen tietomurron tapahtuessa. Mikäli jotain tapahtuu, niin analysoi tapahtunut ja kehitä toimintaasi.

5. LUO YHTEISTYÖKUMPPANUUKSIA JA JAA KUSTANNUKSET

Harkitse yhteistyökumppanuuksien muodostamista muiden samalla alalla tai alueella toimivien pienyritysten kanssa kustannusten ja asiantuntemuksen jakamiseksi. Tämä voi tarkoittaa yhteisten tietoturvakonsulttien palkkaamista, uhkatietojen jakamista tai ryhmähintojen neuvottelemista tietoturvapalveluille ja -koulutuksille. Monet toimialajärjestöt tarjoavat myös kyberturvallisuusresursseja, jotka on räätälöity erityisesti niiden jäsenten tarpeisiin. Muista, että Suomessa on vahva yhteistyön kulttuuri kyberturvallisuudessa, ja pienten ja keskisuurten yritysten saatavilla on lukuisia ilmaisia resursseja. Nämä kumppanuudet tarjoavat pääsyn asiantuntemukseen ja resursseihin, joihin ei olisi varaa yksittäin. Keskittymällä näihin strategisiin lähestymistapoihin suurempien organisaatioiden tietoturvavalmiuksien jäljittelyn sijaan pk-yritykset voivat kehittää tehokasta suojaa tiedoilleen ja järjestelmilleen – mukaan lukien tekoälysovellukset – ilman budjettien ylittämistä. Tehokas tietoturva perustuu älykkääseen toteutukseen täydellisen kattavuuden sijaan. Jopa vaatimattomat, hyvin kohdennetut investoinnit voivat merkittävästi vähentää kriittisimpiä riskejäsi. Lisätietoja suomalaisista vaihtoehdoista löydät tämän asiakirjan lopusta.

YHTEENVETO STRATEGIOISTA

1. Rakenna ihmispalomuuri: Kehitä räätälöityä tietoturvakoulutusta käytännönläheisillä harjoituksilla ja nimeä jokaiselta osastolta tietoturvalähettiläät, jotka auttavat tietoturvakysymyksissä.

2. Ota käyttöön Zero Trust -malli: Aloita kriittisimmistä tiedoista ja tekoälyjärjestelmistä noudattaen periaatetta "älä koskaan luota, varmistu aina" – varmenna jokainen käyttäjä ja laite pääsyä.

3. Hyödynnä tekoälyä: Valitse kustannustehokas tietoturvakokonaisuus, joka hyödyntää koneoppimista tunnistaen automaattisesti uhat ja haavoittuvuudet PK-yritykselle sopivalla hinnalla.

4. Priorisoi toimesi riskiperusteisesti: Laadi kolmiportainen tietoturvasuunnitelma, joka suojaa ensin liiketoimintasi kannalta kriittisimmät kohteet ja laajenee resurssien mukaan.

5. Verkostoidu strategisesti: Jaa tietoturvaosaamista ja -kustannuksia muiden yritysten kanssa toimialajärjestöjen tai yhteistyöverkostojen kautta hyödyntäen myös Suomen kansallisia tietoturvaresursseja.

NÄIN INTEGROIT KYBERTURVALLISUUDEN OSAKSI TEKOÄLYPROJEKTIASI

Tekoäly tarjoaa nykypäivän nopeasti kehittyvässä teknologiamaisemassa merkittäviä mahdollisuuksia kaikenkokoisille yrityksille. Pk-yritykset, joilla on rajalliset tekniset resurssit, jättävät kuitenkin usein kyberturvallisuusnäkökohdat sivuseikaksi tekoälyratkaisuja toteuttaessaan. Tämä lähestymistapa voi johtaa vakaviin seurauksiin.

Kyberturvallisuus sisältää kaikki ne toimenpiteet, joilla estetään haitallisia toimijoita saamasta luvatonta pääsyä organisaation tietoihin, ottamasta järjestelmiä hallintaansa tai häiritsemästä liiketoimintaa. Pk-yrityksille kysymys on erityisen kriittinen, sillä vaikka niiltä puuttuu usein omistautunut IT-turvallisuushenkilöstö, ne käsittelevät silti arkaluonteisia tietoja tekoälysovellustensa kautta.

Tekoälyteknologiat tuovat mukanaan ainutlaatuisia turvallisuushaasteita. Suuret tietomäärät tekevät järjestelmistä houkuttelevia kohteita kyberkriminaaleille, kun taas monimutkainen verkottuminen eri tietolähteisiin ja järjestelmiin laajentaa mahdollista hyökkäyspinta-alaa merkittävästi. Tämä monimutkaisuus edellyttää järjestelmällistä lähestymistapaa, joka alkaa perusteista ja ulottuu erityisiin suojatoimenpiteisiin.

TEKOÄLYSOVELLUKSET VAATIVAT USEIN YHTEYDEN ERILAISIIN TIETOLÄHTEISIIN JA VERKKOIHIN, MIKÄ LAAJENTAA MAHDOLLISTA HYÖKKÄYSPINTAA.

Tekoälyhankkeissa turvallisuuden varmistaminen vaatii huomiota useisiin tekijöihin. Kaikki käyttäjien antamat syötteet on validoitava ja puhdistettava ennen niiden käsittelyä tahattomien komentojen suorittamisen estämiseksi. Tämä validointiprosessi on erityisen kriittinen tekoälyjärjestelmille, jotka ovat vuorovaikutuksessa käyttäjien kanssa chatbot-sovellusten tai tiedonkeruulomakkeiden kautta. Ilman asianmukaista puhdistusta nämä vuorovaikutukset voivat toimia porttina haitalliselle koodille.

Vahvat käyttöoikeuksien hallintamekanismit on otettava käyttöön sekä tietojen pääsyn että toimintaoikeuksien säätelemiseksi. Vähimmäisoikeuksien periaate varmistaa, että käyttäjät ja järjestelmäkomponentit saavat pääsyn vain niihin tietoihin ja toimintoihin, joita heidän tehtäviensä suorittaminen edellyttää. Luottamuksellisia liiketietoja tai henkilötietoja käsitteleville tekoälyjärjestelmille nämä kontrollit toimivat ensisijaisena suojana luvattomalta tietojen paljastumiselta.

Tietoturvallisuus on varmistettava salausmenetelmillä, jotka suojaavat tietoja sekä siirron että tallennuksen aikana. Salaus muuntaa luettavat tiedot koodattuun muotoon, jonka käyttö vaatii erityisen salauksen purkuavaimen. Tämä tekee varastettujen tietojen hyväksikäytöstä merkittävästi vaikeampaa hyökkääjille. Arkaluontoisia tietoja käsitteleville yrityksille salaus ei ole pelkästään teknisesti paras käytäntö, vaan usein myös lakisääteinen vaatimus.

Järjestelmät on suojattava myös SQL-injektio- ja muita komentoinjektion hyökkäyksiä vastaan. Nämä haavoittuvuudet voivat antaa hyökkääjille mahdollisuuden manipuloida tietokantoja ja suorittaa luvattomia komentoja näennäisesti viattomien syöttökenttien kautta. Tämä on erityisen merkityksellistä tekoälyjärjestelmille, jotka ovat yhteydessä arvokasta dataa sisältäviin tietokantoihin.

Kyberturvallisuuden vahvistamispyrkimysten tueksi on saatavilla lukuisia pk-yrityksille räätälöityjä resursseja, mukaan lukien johdantokursseja, yksinkertaistettuja turvallisuusviitekehyksiä ja ulkoistettuja turvallisuuspalveluja. Kiinnittämällä asianmukaista huomiota turvallisuusnäkökohtiin projektin alusta alkaen kaikentasoiset yritykset voivat turvallisesti hyödyntää tekoälyn transformatiivista potentiaalia samalla suojaten arvokkaita digitaalisia omaisuuksiaan.

MITÄ TARKOITTAA PHISHING?

Phishing eli tietojenkalastelu-sähköposti on petollinen viesti, joka on suunniteltu huijaamaan vastaanottajia paljastamaan arkaluonteisia tietoja, kuten salasanoja, taloustietoja tai henkilökohtaisia tietoja. Nämä sähköpostit näyttävät usein tulevan luotettavilta lähteiltä, kuten pankeilta, työtovereilta tai palveluntarjoajilta, ja ne voivat sisältää kiireellisiä pyyntöjä, vääriä linkkejä tai haitallisia liitteitä. Tavoitteena on huijata vastaanottaja napsauttamaan haitallista linkkiä, lataamaan haittaohjelmia tai antamaan luottamuksellisia tietoja. Suojautuaksesi tietojenkalastelulta tarkista aina viestin lähettäjä, kiinnitä huomiota epätavalliseen kieleen tai muotoiluun ja vältä epäilyttävien linkkien tai liitteiden avaamista.

YHÄ ILMAN STRATEGIAA? YRITYKSESI STRATEGIAN HIOMINEN ALKAA TÄSTÄ

Nykypäivän nopeasti kehittyvässä digitaalisessa ympäristössä vankka kyberturvallisuusstrategia ei ole enää ylellisyys, vaan se on välttämättömyys. Kyberhyökkäykset kasvavat sekä monimutkaisuudessaan että yleisyydessään, ja kaikenkokoiset yritykset ovat muuttuneet ensisijaisiksi kohteiksi. Riskit ovat valtavat aina taloudellisista tappioista mainehaittoihin, oikeudellisiin seurauksiin ja arkaluontoisten tietojen mahdolliseen vaarantumiseen. Yksittäinen tietomurto voi ajaa koko yrityksen polvilleen, ja sen pitkäaikaiset seuraukset voivat kestää vuosia.

Hyvin suunniteltu kyberturvallisuusstrategia on ensimmäinen puolustuslinja tällaisia uhkia vastaan. Se varmistaa yrityksesi jatkuvuuden ja suojaa luottamusta, jonka olet rakentanut asiakkaidesi ja kumppaneidesi kanssa. Tehokas strategia ei kuitenkaan rajoitu pelkästään hyökkäysten estämiseen. Se tarkoittaa myös turvallisuuskulttuurin luomista organisaatiossa. Se varustaa työntekijät tiedoilla ja työkaluilla uhkien havaitsemiseen ja torjumiseen, vähentäen inhimillisten virheiden riskiä – keskeistä tekijää monissa tietomurroissa. Digitaalisten järjestelmien, pilvipalveluiden ja etätyön yleistyessä jokaisella yrityksellä on oltava ennakoiva lähestymistapa tietojensa ja järjestelmiensä turvaamiseen.

Tämän laiminlyönti voi johtaa merkittäviin taloudellisiin tappioihin, oikeudellisiin vastuisiin ja korjaamattomaan haittaan brändisi maineelle. Kun tietosuojaa ja kyberturvaa koskevat kansainväliset säädökset, kuten GDPR, tiukentuvat, yritysten on noudatettava lakisääteisiä vaatimuksia. Tehokas kyberturvallisuusstrategia varmistaa, että yrityksesi ei ainoastaan pysy suojattuna vaan myös toimii lainsäädännön mukaisesti välttäen kovat sakot ja seuraamukset.

> **Investointi, joka kannattaa:**
> Kyberturvallisuus vahvistaa asiakkaiden luottamusta, turvaa liiketoimintaa ja antaa mielenrauhan keskittyä kasvuun ilman jatkuvaa pelkoa kyberuhista.

Kyberturvallisuus on siis investointi, joka maksaa itsensä aina takaisin: se vahvistaa asiakkaiden luottamusta, turvaa liiketoimintaa ja antaa sinulle mielenrauhan keskittyä kasvuun ilman jatkuvaa pelkoa tieto- ja kyberuhista. Siksi siihen kannattaa myös suhtautua sen mukaisesti.

TEHOKKAAN TURVALLISUUSSTRATEGIAN KEHITTÄMINEN

Tehokkaan kybertaturvallisuusstrategian kehittämiseksi voimme jakaa sen useisiin keskeisiin alueisiin. Tässä osiossa käymme läpi keskeiset eri osa-alueet, jotka voivat olla välittömiä ratkaisuja yrityksenne tieto- ja kyberturvan parantamiseksi.

1. TIETOJEN SALAUS

- **Levossa olevan tiedon salaus**: Varmista, että kaikki arkaluonteiset tiedot salataan tallennettaessa. Käytä AES-256-salausta, joka on yleisesti käytössä oleva ja vahva standardi levossa olevalle tiedolle. Sitä pidetään laajalti turvallisena ja sitä käytetään yleisesti tietokannoissa, tiedostojärjestelmissä ja pilvitallennuksessa.

- **Siirrettävän tiedon salaus**: Käytä TLS:ää (Transport Layer Security) verkkojen yli siirrettävälle tiedolle (esim. HTTPS, SFTP, VPN:t). Varmista, että kaikki API:t, viestintäkanavat ja verkkoliikenne on salattu suojautumiseksi man-in-the-middle (MitM) -hyökkäyksiltä.

- **Päästä päähän -salaus (E2EE)**: Ota käyttöön E2EE käyttäjien väliseen viestintään, erityisesti sähköpostiin, chattiin tai tiedostonjakojärjestelmiin (esim. Signal- tai ProtonMail-salausprotokollien kautta).

2. PÄÄSYNHALLINTA JA TODENTAMINEN

- **Monitekijätodentaminen (MFA)**: Vaadi MFA:ta kaikille käyttäjätileille lisätäksesi ylimääräisen turvallisuuskerroksen salasanojen lisäksi. Älä jätä ketään ulkopuolelle. Eri vaihtoehtoja ovat esimerkiksi sähköposti, puhelinnumero sekä eri toimijoiden tarjoamat authenticatorit (esim. Google ja Microsoft).

- **Roolipohjainen pääsynhallinta (RBAC)**: Ota käyttöön pienimmän oikeuden periaatteen mukaiset pääsynhallintavaltuudet, jolloin sallit käyttäjille pääsyn vain niihin tietoihin ja järjestelmiin, joita he tarvitsevat työnsä suorittamiseen. Jokainen käyttäjäoikeus on potentiaalinen riski, jonka vuoksi ne kannattaa minimoida mahdollisuuksien mukaan.

- **Säännölliset audit-lokit**: Seuraa jatkuvasti käyttäjien pääsyä eri järjestelmiin ja tietoihin kirjaamalla ne ylös lokitiedostoon. Yrityksen käytössä olevat lokit tulisi tallentaa peukaloinnin kestävään järjestelmään ja tarkistaa säännöllisesti epäilyttävän toiminnan varalta.

- **Salasanakäytännöt**: Pakota vahvat salasanat (esim. vähintään 12 merkkiä, alfanumeerisia erikoismerkkien kanssa) ja vaadi niiden säännöllisiä vaihtoja.

3. VERKKOTURVALLISUUS

- **Palomuurin konfigurointi**: Käytä sekä ohjelmisto- että laitteistopalomuureja rajoittamaan saapuvaa ja lähtevää liikennettä turvakäytäntöjen perusteella. Segmentoi verkostosi eri vyöhykkeisiin (sisäinen, ulkoinen, DMZ) minimoidaksesi riskin.

- **Tunkeutumisen havaitsemis-/estojärjestelmät (IDS/IPS):** Ota käyttöön IDS/IPS valvomaan verkkoliikennettä epätavallisten mallien tai hyökkäyssignaalien varalta.

- **Virtuaalinen yksityisverkko (VPN)**: Varmista, että etätyöntekijät pääsevät sisäiseen verkkoosi vain VPN:n kautta vahvalla salauksella (esim. OpenVPN tai WireGuard).

- **Zero Trust -arkkitehtuuri**: Omaksu Zero Trust -malli, josta kerroimme jo aikaisemmin. Tämä tarkoittaa, ettei mihinkään käyttäjään, laitteeseen tai verkkoon luoteta luontaisesti, vaan kaikkea pidentään potentiaalisena riskinä.

4. PÄÄTELAITETURVALLISUUS

- **Virus- ja haittaohjelmistot**: Asenna ajantasaiset virustorjuntaohjelmistot kaikkiin laitteisiin uhkien havaitsemiseksi ja poistamiseksi. Harkitse **endpoint detection and response (EDR)** -ratkaisujen käyttöä jatkuvaa valvontaa varten.

- **Laitteiden salaus**: Ota käyttöön täyden levyn salaus kaikissa yrityksen kannettavissa tietokoneissa ja mobiililaitteissa estääksesi tietojen paljastumisen kadottamisen tai varkauden yhteydessä (esim. BitLocker tai FileVault).

- **Mobiililaitteiden hallinta (MDM)**: Ota käyttöön MDM varmistamaan, että kaikki yrityksen laitteet on turvattu, valvottu ja voidaan etäpyyhkiä kompromissin sattuessa.

PIENIMMÄN OIKEUDEN PERIAATE?

Pienimmän oikeuden periaate ttarkoittaa, että käyttäjille ja prosesseille myönnetään vain ne käyttöoikeudet, jotka ovat ehdottoman välttämättömiä heidän tehtäviensä suorittamiseen. Tämä periaate auttaa minimoimaan tietoturvaloukkauksien vaikutusta ja ehkäisemään haavoittuvuuksia.

5. TIETOVUOTOJEN ESTÄMINEN (DLP)

Käytä DLP-ohjelmistoa valvomaan ja rajoittamaan arkaluonteisten tietojen luvatonta jakamista tai ulosvientiä. Tämä auttaa estämään tietomurtoja sisäisiltä uhilta tai vahingossa tapahtuvilta paljastuksilta.

6. PILVITURVALLISUUS

- **Salaus pilvipalveluissa:** Varmista, että pilvipalveluntarjoajasi tukee salausta sekä levossa olevalle että siirrettävälle tiedolle. Käytä asiakaspuolen salausta mahdollisuuksien mukaan hallitaksesi salausavaimia.

- **API-integraatioiden turvallisuus:** Varmista, että kaikki pilvipalvelujen integroinnissa käytetyt API:t on turvattu ja valvottu epätavallisen käyttäytymisen varalta.

- **Varmuuskopiointi ja katastrofitoipuminen:** Ota käyttöön säännölliset, salatut varmuuskopiot kaikesta kriittisestä tiedosta ja ylläpidä katastrofitoipumissuunnitelmaa järjestelmien palauttamiseksi hyökkäyksen sattuessa.

7. TIETOTURVAPOIKKEAMIEN KÄSITTELYSUUNNITELMA

Kehitä tietoturvapoikkeamien käsittelysuunnitelma (IRP) kyberhyökkäysten nopeaa havaitsemista, vastaamista ja toipumista varten. Suunnitelman tulisi sisältää:

- Määritellyt roolit ja vastuut
- Menettelytavat hyökkäysten tunnistamiseen, rajoittamiseen ja lieventämiseen
- Tapauksen jälkeinen arviointi ja opitut asiat

Testaa IRP:tä säännöllisesti simulaatioiden tai pöytäharjoitusten kautta.

8. HENKILÖSTÖN KOULUTUS JA TIETOISUUS

- Järjestä säännöllisiä koulutustilaisuuksia tietojenkalastelusta, salasanaturvallisuudesta ja tietojen käsittelyn parhaista käytännöistä.

- Ota käyttöön tietojenkalastelun simulaatio-ohjelma auttamaan työntekijöitä tunnistamaan ja välttämään tietojenkalasteluhyökkäyksiä.

- Luo käytännöt, jossa määritellään yrityksen ohjeet laitteiden hyväksyttävästä käytöstä, tietojen käsittelystä ja epäilyttävän toiminnan ilmoittamisesta.

9. KOLMANNEN OSAPUOLEN TOIMITTAJIEN TURVALLISUUS

- Suorita perusteelliset turvallisuusarvioinnit kaikille kolmannen osapuolen toimittajille. Vaadi turvallisuussertifikaatit (esim. SOC 2, ISO 27001) ja varmista, että ne noudattavat yrityksesi turvallisuuskäytäntöjä.

- Laadi vahvat tietojenkäsittelysopimukset (DPA:t) varmistaaksesi, että kaikki kolmannen osapuolen käsittelijät noudattavat sääntelystandardeja (kuten GDPR).

10. SÄÄNNÖSTEN NOUDATTAMINEN

Varmista, että noudatatte asiaankuuluvia säädöksiä (esim. GDPR, HIPAA). Suorita säännöllisiä auditointeja ja arviointeja pysyäksesi linjassa näiden standardien kanssa.

Käsittelemällä jokaista osa-aluetta asianmukaisilla ratkaisuilla voit luoda kattavan kybertaturvallisuusstrategian, joka on räätälöity yrityksesi erityistarpeisiin.

KESKEISET KYSYMYKSET

Nämä kysymykset voivat toimia esimerkiksi itsearviointityökalunasi, keskustelunavauksena koulutuksissasi tai suunnittelun tukena tekoälyhankkeissasi.

LÄHTÖTILANTEEN ARVIOINTI:

- Onko yrityksellänne **IT-turvallisuushenkilöstöä**, vai onko jokainen vastuussa?
- Mitä **arkaluonteisia tietoja** käsittelette **tekoälysovellustenne** kautta? Tee listaus eri tietoluokista, jotka ovat osa tekoälysovelluksenne toimintaa.
- Kuinka hyvin ymmärrätte **tekoälyteknologioiden** tuomat ainutlaatuiset **turvallisuushaasteet**? Onko yrityksessänne kokemusta niiden saralla?

TEKNISET SUOJATOIMENPITEET:

- Miten varmistatte, että **käyttäjien syötteet validoidaan ja puhdistetaan** ennen niiden käsittelyä? Miten tämä toteutetaan?
- Onko käyttäjillänne käytössä **vahvat käyttöoikeuksien hallintamekanismit** ja **vähimmäistarpeen tai -oikeuksien periaatteet**?
- Suojataanko hallinnoimanne tiedot riittävän vahvalla **salauksella** sekä **siirron** että **tallennuksen aikana**? Entä vastaavatko ne lainsäädännön vaatimuksia?
- Miten estätte **SQL-injektio- ja muut komentoinjektion hyökkäykset** chatboteissa, lomakkeissa sekä muissa käyttäjärajapinnoissa ja järjestelmissänne?

RISKIENHALLINTA:

- Kuinka laaja yrityksenne **hyökkäyspinta-ala** on **tekoälyjärjestelmienne verkottumisen** sekä muun **integraation** vuoksi?
- Onko tekoälyjärjestelmissänne **suuri määrä tietoa**? Entä ovatko järjestelmänne houkuttelevia kohteita kyberkriminaaleille juuri suurten tietomäärien vuoksi?
- Tiedättekö, **mistä kaikista lähteistä** tekoälyjärjestelmänne hakee tietoa, ja miten nämä lähteet on turvattu?
- Mitä vakavia seurauksia **turvallisuuspuutteet** voisivat aiheuttaa liiketoiminnallenne? Entä mitä vaikutuksia **tietomurolla** voisi olla asiakkaillenne?

RESURSSIT JA TUKI:

- Mitä **pk-yrityksille suunnattuja turvallisuusresursseja** voisitte hyödyntää? Tarvitsetteko **ulkoistettuja turvallisuuspalveluja**, vai voitteko hoitaa turvallisuuden sisäisesti? Onko verkostossanne ulkoisten palveluntarjoajia?
  Miten sisällytätte **turvallisuusnäkökohdat** tekoälyprojektiinne jo **suunnitteluvaiheessa**? Entä miten varmistatte, että niitä seurataan projektin ajan?

STANDARDIT, SÄÄNNÖKSET JA MUU TOIMINTA:

- Mitkä **lakisääteiset vaatimukset** koskevat teidän tietojenkäsittelyänne?
- Täyttävätkö salausmenetelmänne **säädösten vaatimukset**?
- Onko käytössänne **järjestelmällinen tietoturvakehys** tai **toimintamalli** tekoälyhankkeiden ja muun toimintanne tueksi?
- Miten **valmistaudutte kyberhyökkäyksiin** ja miten nopeasti pystytte **palautumaan** mahdollisesta **tietoturvaloukkauksesta**?

Toivottavasti tästä kysymyssarjasta oli hyötyä sinulle ja yrityksellesi. Muistathan, että tekoälyn käyttöönotto on strateginen investointi, joka vaatii vastuullista ja tietoturvallista toteutusta. Yritykset, jotka huomioivat kyberturvallisuuden jo projektin alkuvaiheessa, eivät ainoastaan suojaa itseään riskeiltä, vaan vahvistavat myös kilpailuasemaansa markkinoilla, joilla luottamus ja tietosuoja ovat yhä tärkeämpiä. Kun turvallisuus sisällytetään osaksi tekoälystrategiaa alusta alkaen, yritys voi luottaa tulevaisuutensa sekä hyödyntää tekoälyn mahdollisuuksia rohkeasti ja kestävällä tavalla.

LOPUKSI

Kun astut autoon, laitat turvavyön. Kun lähdet kotoa, lukitset ovet ja ikkunat. Emme juurikaan pohdi näitä toimia, koska ne ovat meille luontaisia. Kun otat lääkkeen, luet pakkausselosteen. Kun ostat vakuutuksen, perehdyt ehtoihin huolellisesti. Kun avaat pankkitilin, allekirjoitat sopimuksen tietoisena siitä, mitä hyväksyt. Nämä ovat luonnollisia varotoimia, joita noudatamme fyysisessä maailmassa – meidän on pakko. Mutta miksi sitten suhtaudumme usein niin välinpitämättömästi digitaalisiin oviin ja ikkunoihin? Miksi olemme valmiita ottamaan riskin siitä, että ulkopuoliset tunkeutuvat digitaaliseen yksityisyyteemme? Miksi hyväksymme käyttöehdot sokeasti lukematta niitä lainkaan ja luovutamme henkilötietojamme yrityksille, joiden toimintatavoista emme tiedä juuri mitään?

Jokainen verkossa tekemämme haku, jokainen ostoksemme ja jokainen viestimme kerätään, analysoidaan ja varastoidaan. Datamme on uusi öljy, mutta toisin kuin öljylähteiden kohdalla, emme useinkaan tiedä, kuka sitä louhii, mihin sitä käytetään tai kuinka arvokasta se on. Samaan aikaan kun vaadimme ruokatuotteista tarkkoja ainesosaluetteloita, annamme digitaalisille palveluille vapaat kädet kerätä kaiken mahdollisen tiedon elämästämme. Yritysten hallussa on valtavia määriä arkaluontoista tietoa asiakkaistaan, työntekijöistään ja kumppaneistaan. Henkilötunnukset, pankkitiedot, terveystiedot, sijaintitiedot ja viestintä – kaikki tämä data kulkee yritysverkostojen läpi päivittäin.

Kun yritys kerää tietoa, se hyväksyy vastuun sen suojaamisesta samalla tavalla kuin pankki kassakaappinsa sisällöstä tai sairaala potilastiedoistaan. Datan turvallinen käsittely ei ole tekninen sivuseikka, vaan keskeinen osa yritysten yhteiskuntavastuuta. Siinä mielessä tietomurto ei vahingoita vain yritystä itseään – se voi tuhota myös asiakkaiden elämän vuosiksi, kuten Vastaamon tapaus osoitti. Henkilötietojen päätyminen vääriin käsiin voi johtaa identiteettivarkauksiin, taloudellisiin menetyksiin, kiristykseen ja jopa henkilökohtaisen turvallisuuden vaarantumiseen. Sen vuoksi yritysten on rakennettava digitaalinen turvallisuus osaksi perusliiketoimintaansa – ei vain teknisenä vaatimuksena, vaan moraalisena velvollisuutena suojella kaikkien niiden ihmisten elämää, jotka ovat uskoneet heille arkaluontoisimmat tietonsa. Olethan myös sen luottamuksen arvoinen.

HYÖDYLLISIÄ LINKKEJÄ (2025)

Kyberturvallisuuden vahvistamisessa on tarjolla runsaasti tukea: johdantokursseja, yksinkertaistettuja toimintamalleja ja erityisesti pienille organisaatioille suunnattuja hallinnoituja tietoturvapalveluita. Kun tietoturvaan kiinnitetään huomiota jo alusta lähtien, kaikki yritykset voivat teknisistä valmiuksistaan riippumatta hyödyntää tekoälyn mullistavaa potentiaalia turvallisesti ja samalla suojata arvokkaita digitaalisia resurssejaan.

ALOITTELIJAYSTÄVÄLLISIÄ MATERIAALEJA

- MinnaLearning: Cybersecurity - A beginner's guide (ilmainen verkkokurssi, joka on kehitetty yhdessä EU Digital SkillUp Initiativen kanssa)
- Elinkeinoelämän keskusliitto EK: Kyberturvallisuus - mitä jokaisen yrityksen kannattaa tehdä kyberturvallisuutensa varmistamiseksi (webinaarin esitysmateriaali)
- Kyberturvallisuuskeskus: Pienyritysten kyberturvallisuusopas, Ohjeet ja oppaat organisaatioille ja yrityksille (paljon eri oppaita), TOP 5 tietoturvauhat ja -ratkaisut organisaatioille, Kyberturvallisuuden riskienhallinnan tuotteiden ja palveluiden hakemistopalvelu
- W3 Schools: Cyber Security Tutorial (W3schools-sivuston opaskokoelma, joka käsittelee olennaisia kyberturvallisuusaiheita)
- Valtioneuvosto: Kyberturvallisuusdirektiivi vahvistaa koko EU:n kyberturvallisuustasoa – kansallinen toimeenpanohanke käynnistyi (tiedote NIS2-direktiivistä)
- Synopsys: Glossary Key Terms (englanninkielinen sanakirja kyberturvallisuuden sanastolle)

KOULUTUKSIA JA MUITA MAHDOLLISUUKSIA

Kyberturvallisuuskoulutusta tarjoavat myös useat maksulliset koulutusorganisaatiot Suomessa, kuten Tieturi ja Aalto Executive Education. Yliopistoista kyberturvallisuuden opintokokonaisuuksia löytyy muun muassa Aalto-yliopistosta ja Jyväskylän yliopistosta. Ammattikorkeakouluista kyberturvallisuuden tutkintokokonaisuuksia puolestaan tarjoavat esimerkiksi XAMK, Laurea ja JAMK.

- Finnish Cyber Security Certificate: Turvaa digitaaliseen tulevaisuuteen (koulutus ja sertifikaatti)

SÄÄNTELYKEHYS

Kyberturvallisuussäännökset kattavat omistautuneen kansallisen ja EU-lainsäädännön sekä kyberturvallisuusmääräykset, jotka on sisällytetty laajempiin oikeudellisiin kehyksiin, kuten Suomen rikoslakiin. Nämä säännökset määrittelevät eri sidosryhmien vastuut digitaalisen turvallisuuden ylläpitämisessä.

Sääntelykenttää täydentävät toimialastandardit, sertifiointiohjelmat ja erikoistuneet virastot, kuten ENISA (Euroopan unionin kyberturvallisuusvirasto). Kattavan johdannon saamiseksi tähän monimutkaiseen alaan EU:n kyberturvallisuuspolitiikan yleiskatsaus tarjoaa erinomaisen lähtökohdan.

- Euroopan komissio: Euroopan unionin kyberturvallisuuspolitiikka (yleiskatsaus EU:n yhteisiin kyberturvallisuusaloitteisiin ja strategioihin)
- Euroopan komissio: NIS2-direktiivi eli verkko- ja tietojärjestelmien turvaaminen (tietoa EU:n direktiivistä, joka tiukentaa kyberturvavaatimuksia yrityksille ja viranomaisille)
- Traficom: Kyberturvallisuus ja yrityksen hallituksen vastuu (opas)
- ENISA: European Union Agency for Cybersecurity (verkkosivut)
- CRA: European Cyber Resilience Act (tietopaketti)
- ISO: ISO/IEC 27002:2022 (tietoa tietoturvallisuuden, kyberturvallisuuden ja yksityisyydensuojan ISO-standardista)

PALVELUNTARJOAJAT

Erilaisia palveluntarjoajia löytyy lukemattomia. Olemme listanneet alapuolelle muutamia, joista voit aloittaa, mutta suosittelemme sinua tekemään myös omia hakuja eri palveluntarjoajien suhteen ja etsimään juuri sinulle sopivan palveluntarjoajan.

- Robocoast EDIH: Laitteiden tietoturvatestaus (Ohjelmisto- ja järjestelmäturvallisuustestausta kohdejärjestelmien, verkkojen ja ohjelmistojen toiminnallisten heikkouksien ja tietoturva-aukkojen tunnistamiseksi. Palvelun hinta on 675€ henkilötyöpäivä +ALV)
- Centria: Centria SecuLab (sisäisten verkkojen, ohjelmistojen, laitteiden ja tietoturvatietoisuuden testausta ammattilaisten kanssa)
- JAMK: Kyberturvallisuuspalvelut (koulutukset, harjoitukset, testaukset)
- JAMK: JYVSECTEC (erilaisia palveluita ja tietopaketteja)

AMMATILLISET JÄRJESTÖT

Pysy ajan tasalla liittymällä ammattijärjestöihin:

- Suomen tietoturvaklusteri (FISC) - Blogit, tapahtumat ja resurssit suomeksi
- Tietoturva ry - Suomen tietoturvayhdistys

SANASTOA

Parantaaksemme lukukokemustasi olemme luoneet pienen sanaston, joka helpottaa oppaamme lukemista. Suosittelemme tutustumaan sanastoon ennen oppaan lukemista.

AES-256 tarkoittaa standardia, jossa käytetään 256-bittistä avainta tietojen salaamiseen ja purkamiseen. Se on symmetrinen salausalgoritmi, jolloin samaa avainta käytetään sekä salaamiseen että purkamiseen.

API tarkoittaa ohjelmointirajapintaa, joka on joukko sääntöjä ja määrityksiä, jotka mahdollistavat erilaisten ohjelmistojen tai järjestelmien välisen kommunikoinnin ja tiedonvaihdon. Se toimii kuin sovellusten välinen sopimus, jossa määritellään, miten eri ohjelmistot voivat pyytää ja vastaanottaa tietoja toisiltaan.

DDoS-hyökkäys on hajautettu palvelunestohyökkäys, jossa useat tietokoneet tai muut laitteet kuormittavat kohdejärjestelmää, kuten verkkosivustoa tai palvelinta, niin paljon, että se kaatuu tai hidastuu merkittävästi. Tämä estää laillisia käyttäjiä käyttämästä palvelua.

DLP on tietoturvamenetelmä, jonka avulla pyritään estämään arkaluontoisten tietojen vuotaminen, katoaminen tai väärinkäyttö organisaatiosta. DLP-järjestelmät valvovat ja hallinnoivat tietojen käyttöä, siirtoa ja tallennusta estääkseen tietoturvaloukkaukset ja tietojen menetykset.

DORA on EU:n asetus, joka keskittyy vahvistamaan finanssialan toimijoiden digitaalista toimintakykyä ja häiriönsietokykyä erityisesti tietoturvaan ja kyberuhkiin liittyen. Se ei ole suoraan tietoturvakehikko, mutta se sisältää useita tietoturvaperiaatteita ja -käytäntöjä osana sen vaatimuksia.

E2EE tarkoittaa päästä päähän salausta, jossa viestit salataan lähettäjän laitteessa ja puretaan vasta vastaanottajan laitteessa. Näin vain lähettäjä ja vastaanottaja voivat lukea viestin.

Haavoittuvuusarviointi tarkoittaa prosessia, jossa järjestelmän tai sovelluksen haavoittuvuuksia tunnistetaan, analysoidaan ja priorisoidaan. Sen tavoitteena on vähentää riskejä havaitsemalla ja korjaamalla heikkouksia ennen kuin ne voivat johtaa vahinkoon.

Injektiohyökkäys tarkoittaa menetelmää, jossa hyökkääjä syöttää haitallista koodia tai komentoja järjestelmään, kuten verkkosivustoon tai tietokantaan, tarkoituksenaan vahingoittaa tai kaapata järjestelmä.

Integraatiopintojen koventaminen tarkoittaa organisaation käyttämien integraatioympäristöjen ja -ratkaisujen (esim. API-gatewayt, tietovirtojen hallinta-alustat, ESB:t, pilvi-integraatiopalvelut) suojaamista ja konfigurointia siten, että tietoturvariskit minimoidaan ja niiden hyökkäyspinta on mahdollisimman pieni.

Kryptografia tarkoittaa tiedon salaamista ja salauksen purkamista sekä näihin liittyvää tutkimusta. Se on tekniikka, jonka avulla tieto muutetaan muotoon, jota vain valtuutetut henkilöt voivat lukea.

Lokitus tarkoittaa tietojärjestelmissä, sovelluksissa tai verkoissa tapahtuvien toimintojen ja tapahtumien tallentamista aikajärjestyksessä kuin päiväkirjaan. Tätä tallennettua tietoa kutsutaan lokiksi tai lokitiedoksi. Lokitusta käytetään virheiden selvittämiseen, järjestelmän toiminnan analysointiin ja turvallisuuden valvontaan.

MFA tarkoittaa monivaiheista tunnistautumista, joka on tietoturvatoimenpide, jossa käyttäjältä vaaditaan useampi kuin yksi tapa vahvistaa henkilöllisyytensä kirjautuessaan sisään.

NIS ja NIS2 tarkoittavat Euroopan unionin verkko- ja tietoturvadirektiivejä, jotka asettaa velvoitteita tietojen ja verkkojen turvallisuuteen liittyen. Niiden tavoitteina on parantaa kyberturvallisuutta kriittisillä toimialoilla ja varmistaa yhteiskunnan kannalta tärkeiden palveluiden häiriötön toiminta.

Penetraatiotesti on tietoturvan arviointi, jossa simuloidaan tietomurtoa järjestelmään, verkkoon tai sovellukseen. Tavoitteena on löytää haavoittuvuuksia ja heikkouksia, jotta ne voidaan korjata ennen kuin haitalliset toimijat voivat hyödyntää niitä.

RBAC tarkoittaa roolipohjaista pääsynhallintaa. Se on tietoturvamenetelmä, joka hallitsee käyttäjien pääsyä järjestelmiin ja resursseihin perustuen heidän rooleihinsa organisaatiossa, eikä yksittäisiin käyttäjiin.

Security by designissa tietoturvaominaisuudet ja -toimenpiteet sisällytetään tuotteiden, järjestelmien ja palveluiden suunnitteluun ja kehittämiseen alusta alkaen, ei lisäominaisuuksina jälkikäteen.

SQL-injektio on tietoturva-aukko, jossa hyökkääjä pääsee käsiksi tietokantaan ja mahdollisesti muokkaamaan tai tuhoamaan tietoja syöttämällä haitallista SQL-koodia sovelluksen syöttökenttiin. Hyökkäyksessä se hyödyntää sovellusten haavoittuvuuksia, jotka liittyvät tietokantakyselyjen muodostamiseen.

Syöte tarkoittaa tetokoneohjelmalle annettavaa ulkopuolista dataa, kuten esimerkiksi tekstiä, kuvia, yksittäisiä näppäinpainalluksia, hiiren klikkauksia yms.

TLS on tietoturvaprotokolla, jota käytetään suojaamaan tietoliikennettä internetissä ja muissa verkoissa. Se varmistaa, että tiedot siirtyvät turvallisesti ja luottamuksellisesti kahden osapuolen, kuten verkkosivuston ja käyttäjän selaimen, välillä. TLS suojaa tietoja sieppaukselta, peukaloinnilta ja muilta tietoturvauhkaavilta.

XSS-hyökkäys on tietoturvahaavoittuvuus, jossa hyökkääjä syöttää haitallista koodia, yleensä JavaScriptiä, luotetulle verkkosivustolle. Tämä haitallinen koodi suoritetaan sitten muiden käyttäjien selaimissa, kun he vierailevat sivustolla, mahdollistaen hyökkääjälle pääsyn käyttäjien tietoihin tai sivuston hallintaan.

TÄSTÄ OPPAASTA

Tämän kyberturvaoppaan on tuottanut Finnish AI Region (FAIR) – **yritysten luotettava kumppani digitaalisen tulevaisuuden rakentamisessa**. FAIR tarjoaa suomalaisille pk-yrityksille käytännönläheistä asiantuntijuutta tekoälyn, laajennetun todellisuuden, suurteholaskennan ja kyberturvallisuuden saralla. Maksuttomat palvelumme on suunniteltu nopeuttamaan ja laajentamaan tekoälyn käyttöönottoa suomalaisessa liiketoiminnassa.

MIKSI VALITA FAIR KUMPPANIKSESI?

- Maailmanluokan palveluita matalalla kynnyksellä
- Pääosin maksuton asiantuntijuus ja testauspalvelut
- Keskitymme pk-yritysten todellisiin tarpeisiin ja haasteisiin
- Suomalaisten toimijoiden verkosto, joka ymmärtää paikallista liiketoimintaympäristöä
- Aidosti hyödylliset räätälöidyt palvelut

VAHVA RAHOITUSPOHJA TAKAA LAADUN

FAIR:n toiminta on mahdollista merkittävien eurooppalaisten ja kotimaisten toimijoiden

- Euroopan komissio – digitaalisen siirtymän tukeminen
- Business Finland – suomalaisen innovaatioekosysteemin vahvistaminen
- Helsingin kaupungin Innovaatiorahasto – startup- ja kasvuyritysten tukeminen

TUTUSTU RÄÄTÄLÖITYIHIN PALVELUKOKONAISUUKSIIMME

Käy tutustumassa kattavaan palvelutarjontaamme ja ota yhteyttä, niin autamme yritystäsi ottamaan seuraavan askeleen kohti tulevaisuuden liiketoimintaa.

ERITYISKIITOKSET

Tämän oppaan ovat kirjoittaneet **Martti Asikainen** (Haaga-Helia), **Solja Sulkunen** (Business Helsinki), **Jussi Rantsi** (Aalto-yliopisto ja Helsingin yliopisto) sekä **Jenni Selosmaa** (Espoon kaupunki). Kiitämme lämpimästi myös **Marie Skavø-Sinisaloa** Kaakkois-Suomen ammattikorkeakoulusta (Xamk) arvokkaista näkemyksistä ja asiantuntevasta arvioinnista.

FINNISH AI REGION ON:

- Aalto-yliopisto ja Helsingin yliopisto
- Haaga-Helia ja Metropolia ammattikorkeakoulut
- Helsingin, Espoon ja Vantaan kaupungit
- Tieteen tietotekniikan keskus CSC
- EIT Digital
- KiraHUB
- Enter Espoo ja Helsinki XR Center

YHTEISTYÖKUMPPANEITAMME OVAT:

- ABB
- Arcada
- Google
- Microsoft
- Uudenmaan liitto
- Varian Siemens
- FCAI
- Teknologiateollisuus ry

Finnish AI Regionissa tavoitteenamme on rakentaa dynaaminen ja elävä ekosysteemi, joka vauhdittaa teknologian käyttöönottoa yrityksissä. Olemme sitoutuneet pysymään teknologisten innovaatioiden, huippututkimuksen ja osaajien kehityksen eturintamassa.

Missiomme keskittyy edistämään uraauurtavia innovaatioita erityisesti digitaalisten palvelujen, terveydenhuollon ja älykaupunkien alueilla. Yhdistämällä avaintoimijat luomme merkittäviä hyötyjä sekä kansantaloudelle että koko Euroopan unionin talousalueelle. FAIR luo uusia mahdollisuuksia ja kehittää kestäviä ratkaisuja tulevaisuuden haasteisiin.

Lue lisää palveluistamme ja partneriohjelmistamme verkkosivuilta osoitteesta:

https://www.fairedih.fi

FAIR
Finnish AI Region | EDIH

Digitaalisessa ajassa jokainen yritys on alttiina riskeille, mutta myös täynnä mahdollisuuksia. Tämä käytännönläheinen opas on suunnattu erityisesti pienille ja keskisuurille yrityksille, joilla ei ole omaa IT-osastoa, mutta jotka haluavat ottaa tekoälyn käyttöön turvallisesti ja hallitusti.

Opas tekee selväksi, mitä eroa on kyberturvallisuudella ja tietoturvalla, ja tarjoaa konkreettisia, kustannustehokkaita ratkaisuja yrityksesi digitaalisen turvallisuuden vahvistamiseen. Lukemalla saat selkeät ohjeet tekoälyn turvalliseen käyttöönottoon, helppotajuisen viitekehyksen yrityksesi suojaamiseen sekä vinkkejä siihen, kuinka koulutat tiimisi tunnistamaan ja torjumaan uhkia.

Olitpa vasta tutustumassa tekoälyyn tai jo rakentamassa sen varaan uusia palveluita, tämä opas auttaa sinua ottamaan seuraavan askeleen itsevarmasti ja vastuullisesti. Et tarvitse IT-taustaa, vaan ainostaan halua kehittää yrityksesi toimintaa älykkäästi ja vastuullisesti. Muista, että kyberturvallisuus ei vaadi suurta budjettia – vain fiksuja päätöksiä.

FAIR
Finnish AI Region | EDIH

www.fairedih.fi
Co-funded by European Union