MD Data

PK-yritysten kyberturva Suomessa 2026

Välitön uhka ja osaamisvaje

Tiivistelmä: Havainnot ja suositukset pk-yritysten kyberturvaan

Suomalaisen pk-sektorin kyberturvallisuustilannetta tarkasteleva raportti paljastaa merkittävän ristiriidan: vaikka uhkien tietoisuus on lisääntynyt, konkreettisten toimenpiteiden toteuttaminen laahaa perässä. Vaikka 29 % suomalaisista pienyrityksistä pitää kyberhyökkäyksiä yhtenä suurimmista uhista liiketoiminnalleen, 37 % niistä ei ole parantanut tietoturvaansa viimeisen kahden vuoden aikana. Tämä on hälyttävä havainto, sillä jopa 50 % suomalaisista organisaatioista koki kyberhyökkäyksen vuonna 2024, mikä osoittaa uhkien korkean kasvun niiden esiintyvyydessä.

Tämä raportti esittää analyysin uhkien todellisesta mittakaavasta, niiden taloudellisista vaikutuksista ja yritysten nykyisistä valmiuksista.

Pääsuositukset tiivistyvät kolmeen kriittiseen osa-alueeseen

- Ennaltaehkäisevät tekniset toimenpiteet: Välitön panostus monivaiheiseen tunnistautumiseen (MFA), jonka puutteellinen käyttö on edelleen merkittävä haavoittuvuus. Tämän lisäksi yritysten tulisi panostaa haittaohjelmien torjuntaohjelmiin sekä ulkoisiin palomuureihin, jotta ulkoisten hyökkäysten riskit voidaan minimoida.
- Systemaattinen varautuminen: Kattavien varmuuskopiointi- ja palautussuunnitelmien luominen, jotta liiketoiminnan keskeytysaika ja taloudelliset menetykset voidaan minimoida.
- Jatkuva koulutus ja osaamisen kehittäminen: Henkilöstön tietoisuuden ja osaamisen nostaminen on avainasemassa, sillä yleisimmät hyökkäysvektorit, kuten tietojenkalastelu, hyödyntävät inhimillisiä heikkouksia.

Johdanto: Kyberturva ja pk-yritykset Suomessa

Suomen pk-sektorin strateginen merkitys
Suomen talous rakentuu vahvasti pienten ja keskisuurten yritysten varaan. Tilastokeskuksen mukaan Suomessa oli vuonna 2021 yhteensä noin 562 000 yritystä. Näistä ylivoimainen enemmistö, 93 %, on mikroyrityksiä, joissa työskentelee alle 10 työntekijää. Vaikka mikroyritysten osuus kaikkien yritysten lukumäärästä on merkittävä, 95,5 % pelkästään henkilöstömäärään perustuen, niiden liikevaihto-osuus on pienempi kuin muiden kokoluokkien yrityksillä, mikä korostaa määritelmän merkitystä.

Kokonaisuudessaan pk-sektori työllistää yli miljoona henkeä, mikä tekee siitä Suomen kansantalouden kriittisen selkärangan. Kyberuhka tälle sektorille on siis luonteeltaan laaja-alainen, yhteiskunnallinen riski, joka ulottuu yksittäisen yrityksen rajoja pidemmälle.

Kyberturvallisuus liiketoiminnan strategisena riskinä
Perinteisesti kyberturvallisuutta on pidetty ensisijaisesti teknisenä kysymyksenä, joka kuuluu IT-osaston tai ulkoisen kumppanin vastuulle. Nykypäivän digitaalisessa toimintaympäristössä uhkakuvien monimuotoistuessa ja yleistyessä kyberturvallisuus on kuitenkin noussut yhdeksi yrityksen suurimmista strategisista riskeistä.

Tämä riskien muutos edellyttää toimitusjohtajan ja hallituksen aktiivista sitoutumista ja tietoisuutta. Uudet EU-säädökset, kuten NIS2-direktiivi, tiukentavat tietoturvavaatimuksia entisestään. Laiminlyönnit voivat johtaa koko yrityksen toiminnan vaarantaviin sakkoihin, mikä pakottaa yritykset nostamaan kyberturvallisuuden johtoryhmän tasolle.

Kyberuhkien todellisuus: Tilastot ja trendit Suomessa ja Pohjoismaissa

Uhkakuvien yleisyys: Tilannekuva suomalaisissa organisaatioissa
Traficomin Kyberturvallisuuskeskus vastaanotti vuonna 2024 yli 18 000 kyberpoikkeamailmoitusta ja käsitteli automaattisesti noin 185 000 ilmoitusta. Traficomin mukaan nämä luvut ovat linjassa aiempien vuosien kanssa ja osoittavat kyberturvallisuuden kokonaistilanteen pysyneen vakaana. Nämä makrotason luvut eivät kuitenkaan kerro koko totuutta yksittäisen yrityksen kokemasta uhasta.

Kyberturvallisuuskeskuksen yleinen arvio tilanteen vakaudesta on ristiriidassa muiden tutkimusten tulosten kanssa, jotka kuvaavat uhkatasoa huomattavasti korkeammaksi. Konsulttiyhtiö McKinsey-raportin mukaan noin 50 % suomalaisista organisaatioista koki kyberhyökkäyksiä vuonna 2024, mikä on merkittävä luku, joka paljastaa uhkien korkean esiintyvyyden käytännön tasolla.

Tämä tilastollinen ero selittyy raportointikulttuurin ja tilastoinnin eroilla. Viralliset luvut perustuvat pääasiassa raportoituihin tapauksiin. Suomessa raportointihalukkuus on kuitenkin huomattavasti matalampaa kuin monissa muissa Euroopan maissa, mikä saattaa johtaa siihen, että viralliset luvut aliarvioivat todellista uhkatasoa. Erityisesti pk-sektorilla, jolla resursseja poikkeamien raportointiin ja selvittämiseen on rajallisesti, moni tapaus jää todennäköisesti ilmoittamatta. Tämän seurauksena McKinsey-raportin ja muiden kenttätutkimusten korkeammat luvut antavat realistisemman kuvan uhan todellisesta laajuudesta. Pk-yritysten on ymmärrettävä, että todellinen uhkataso on todennäköisesti korkeampi kuin viralliset tilastot osoittavat.

Keskeisimmät hyökkäysvektorit ja niiden kehitys
Pk-yritysten yleisimmät tietoturvauhat ovat usein luonteeltaan inhimillisiä. Tietojenkalastelu (phishing) on yleisin tunkeutumiskeino ja myös yleisin tapa levittää kiristyshaittaohjelmia (ransomware).4 Nämä hyökkäykset on suunniteltu hyödyntämään ihmisten toimintaa teknisten haavoittuvuuksien sijaan, mikä tekee henkilöstön tietoisuudesta kriittisen turvallisuustekijän.

Kiristyshaittaohjelmien määrä on kasvanut vuodesta 2021 lähtien ja niiden vaikutukset ovat olleet erityisen tuhoisia. Yksi onnistunut kiristyshaittaohjelmahyökkäys voi lamauttaa koko liiketoiminnan päiviksi tai jopa viikoiksi, kuten 5–21 päivän keskimääräinen liiketoiminnan keskeytysaika osoittaa. Lisäksi toinen merkittävä ja kallis uhka on liiketoiminnan sähköpostivaarantuminen (BEC), jossa yrityksiä huijataan tekemään väärennettyjä maksuja.

Vertailu muihin Pohjoismaihin
Suomi on useilla kyberturvallisuuden mittareilla Euroopan keskitasoa edellä. Esimerkiksi pienten yritysten osalta Suomi suoriutuu Pohjoismaiden verrokkeihinsa nähden parhaiten järjestelmien säännöllisissä turvallisuustestauksissa, vaikka Ruotsi ja Tanska ovatkin edellä keskimäärin kaikissa yrityskokoluokissa. Tästä huolimatta Suomi on kokonaisuudessaan jäämässä jälkeen muista Pohjoismaisista, kuten edellämainituista Ruotsista ja Tanskasta.

Tämä kehityserä näkyy myös yritysten asenteissa. Ifin kyselyn mukaan vain 29 % suomalaisista pk-yrityksistä piti kyberhyökkäyksiä suurimpana uhkana, kun taas Tanskassa luku oli 37 % ja Norjassa 32 %. Tämä asennepuolueellisuus voi johtaa pienempään panostukseen ja siten suurempaan haavoittuvuuteen pitkällä aikavälillä.

Kyberhyökkäysten vaikutukset: Kustannukset ja riskit

Taloudelliset menetykset ja kustannusrakenteet
Kyberhyökkäyksen aiheuttamat kustannukset voivat olla mittavia. Suomalaisessa kontekstissa kustannukset voivat nousta "kymmenistä tuhansista aina satoihin tuhansiin euroihin".

Maailmanlaajuiset tutkimukset tarjoavat yksityiskohtaisemman kuvan kustannuskomponenteista. Tutkimusten mukaan hyökkäyksen keskimääräinen kokonaiskustannus on ollut noin 254 445 dollaria, mutta se on voinut nousta jopa 7 miljoonaan dollariin. Kiristyshaittaohjelmahyökkäyksen keskimääräinen lunnasmaksu on ollut huomattava, saavuttaen ennätyksellisen 570 000 dollarin tason vuonna 2021, mikä on 82 % enemmän kuin vuonna 2020. On kuitenkin huomioitava, että 90 % kiristyshaittaohjelmahyökkäyksistä epäonnistuu tai ei aiheuta uhreilleen taloudellisia tappioita.

Kyberhyökkäyksen kustannukset ovat moniulotteisia, eivätkä ne rajoitu ainoastaan mahdolliseen lunnasmaksuun. Kun pk-yritys joutuu hyökkäyksen kohteeksi, sen toiminta voi lamautua kokonaan, jos pääsy esimerkiksi laskutus- tai varausjärjestelmiin tai asiakastietokantaan estyy. Tämä johtaa välittömiin tulonmenetyksiin ja voi olla kohtalokasta pienelle yritykselle.

Kokonaiskustannukset koostuvat useista eri komponenteista. Tutkimus osoittaa, että taloudellisten menetysten ohella syntyy lukuisia muita kustannuksia, joista merkittävimpiä ovat tutkinta- ja palautuskulut, mainevahingot sekä menetetyt liiketoimintamahdollisuudet. Seuraava taulukko havainnollistaa kyberhyökkäyksen kokonaiskustannuksia, perustuen globaaleihin aineistoihin:

Kustannuskomponentti	Keskimääräinen kustannus ($)	Korkein raportoitu kustannus ($)
Tutkinta ja palautus	77 957	3 930 000
Sakot	20 623	655 000
Mainevaikutukset	73 393	1 310 000
Menetetyt mahdollisuudet	23 806	6 550 000
Muut kulut	58 666	3 275 000
Kokonaiskustannus	254 445	7 000 000

Lähde: Microsoft SMB Cybersecurity Report - Nämä tiedot korostavat sitä, että ennaltaehkäisy on taloudellisesti huomattavasti kannattavampaa kuin vahingoista toipuminen, sillä suurin osa kustannuksista aiheutuu hyökkäyksen jälkitoimista, ei pelkästään lunnasmaksuista.

Mainevaikutukset ja luottamuksen menetys
Taloudellisten menetysten lisäksi kyberhyökkäykset voivat aiheuttaa vakavia mainevahinkoja ja asiakkaiden luottamuksen menetyksen. Tietomurron tai -vuodon jälkeen asiakkaiden luottamuksen palauttaminen on pitkä prosessi, ja vakavasta tietoturvaloukkauksesta toipuminen on monelle pienelle yritykselle vaikeaa tai jopa mahdotonta. Henkilötietojen tai muiden arkaluonteisten tietojen vuotaminen verkkoon voi aiheuttaa myös pysyviä pelkotiloja ja haavoittaa yrityksen pitkän aikavälin elinvoimaisuutta merkittävästi.

Varautumisen taso ja resurssien rajallisuus

Ifin kyselytutkimus paljastaa kriittisen puutteen: vaikka kyberhyökkäykset huolettavat pienyrityksiä, 37 % niistä ei ole parantanut tietoturvaansa viimeisen kahden vuoden aikana.1 Tämä on merkittävin varautumisen puute. Tämän reaktiivisen asenteen taustalla on usein riittämättömien resurssien ja sisäisen osaamisen puute. Tutkimuksen mukaan alle 30 % pk-yrityksistä hallinnoi tietoturvaansa itse 3, mikä korostaa ulkopuolisten asiantuntijoiden merkitystä.

Pk-yrityksillä on usein reaktiivinen asenne kyberturvallisuuteen. Ajattelu "ei ole ollut ongelmia virusten tai tietoturvan kanssa" 15 tai uskomus siitä, ettei oma yritys ole kiinnostava kohde, on suoraan ristiriidassa uhkakuvien todellisuuden kanssa. Tämä ajattelutapa, jossa uhkia aliarvioidaan, johtaa vähäisiin investointeihin ja resurssien puutteeseen. Tämän seurauksena syntyy haavoittuvien kohteiden "täydellinen myrsky". Kyberrikolliset tietävät, että pk-yrityksillä on usein puutteelliset resurssit, mutta ne käsittelevät arvokasta asiakas- ja liiketoimintatietoa, mikä tekee niistä houkuttelevia hyökkäyskohteita. Itse asiassa lähes puolet tietoturvahyökkäyksistä kohdistuu juuri pk-sektoriin. Tämä luo noidankehän, jossa alhaiset panostukset johtavat haavoittuvuuteen, mikä puolestaan tekee yrityksestä helpon kohteen.

Henkilöstön tietoisuus ja haavoittuvuudet

Monien pk-yritysten tietoturvavalmiuksia heikentää henkilöstön puutteellinen tietoisuus. Yli 80 % pk-yrityksistä pitää henkilöstön tietoturvatietoisuuden puutetta huolena. Tämä on erittäin merkittävä luku, koska yleisimmät hyökkäysvektorit, kuten tietojenkalastelu, perustuvat juuri inhimillisten heikkouksien hyödyntämiseen. Raportti korostaa, että tietoturva on koko organisaation asia ja jokaisen työntekijän vastuulla. Järjestelmällinen henkilöstön koulutus ja tietoturvakulttuurin rakentaminen ovat keskeisessä roolissa riskien vähentämisessä.

Toimintasuunnitelma: Strategiat kyberuhkien torjuntaan

Kyberuhkien torjuntaan on olemassa selkeä toimintasuunnitelma, joka keskittyy kriittisimpien haavoittuvuuksien poistamiseen ja varautumisen parantamiseen. Monivaiheinen tunnistautuminen (MFA): Monivaiheinen tunnistautuminen on yksi tehokkaimmista ja helpoimmista keinoista parantaa tietoturvaa. Se estää suurimman osan tietojenkalastelusta johtuvista tietomurroista, vaikka käyttäjätunnus ja salasana pääsisivätkin vääriin käsiin. Silti tutkimukset osoittavat, että jopa 1/5 pk-yrityksistä on vain "jokseenkin tehokas" sen käytössä. Tämän on oltava ykkössuositus kaikille yrityksille.

Varmuuskopiointi ja palautussuunnitelma: Säännöllinen ja asianmukainen varmuuskopiointi on kiristyshaittaohjelmahyökkäyksen yhteydessä avainasemassa. Se mahdollistaa tietojen palauttamisen ilman lunnaiden maksua. Hyvin valmistautuneet yritykset, joilla on säännölliset varmuuskopiot, kokivat hyökkäyksistä huomattavasti vähemmän häiriöitä palveluihinsa.

Taulukko: Keskeiset kyberturvatoimenpiteet pk-yritykselle

Toimenpide	Tärkein peruste
Monivaiheinen tunnistautuminen (MFA)	Estää yleisimmän hyökkäysvektorin, tietojenkalastelun, onnistumisen, vaikka käyttäjätunnus ja salasana vuotaisivat. Jopa 1/5 pk-yrityksistä käyttää tätä puutteellisesti.
Varmuuskopiointi ja palautussuunnitelma	Vähentää kiristyshaittaohjelmahyökkäysten vaikutuksia ja mahdollistaa nopeamman palautumisen ilman lunnaita. Hyvin valmistautuneet yritykset kokevat huomattavasti vähemmän häiriöitä.
Haittaohjelmien torjunta	Haittaohjelmien tunnistaminen asianmukaisilla ohjelmilla henkilöstön laitteilta, säännölliset tarkastukset ja valmistautuminen ovat monestii hoidettu puolitiehen tai kauan sitten
Henkilöstön koulutus	Puolet hyökkäyksistä kohdistuu pk-sektoriin, ja valtaosa hyödyntää inhimillisiä heikkouksia. Tietoisuus harhautuksista ja huijauksista vähentää riskiä merkittävästi. Yli 80 % yrityksistä pitää tätä huolena
Yhteistyö ulkopuolisten asiantuntijoiden kanssa	Alle 30 % pk-yrityksistä hallinnoi tietoturvaansa itse. Ulkopuolinen kumppani tarjoaa tarvittavaa erikoisosaamista ja resursseja.

Kun hyökkäys tapahtuu, nopea ja tehokas toiminta on elintärkeää. Yrityksen tulee varautua ennakolta ja laatia suunnitelma, joka käsittää kriisiviestinnän, teknisen tutkinnan ja toiminnan palauttamisen. Kiristyksen uhriksi joutuneita yrityksiä kehotetaan olemaan maksamatta lunnaita, sillä se saattaa johtaa lisäkiristykseen ja tietojen vuotamiseen maksuista huolimatta. Myös kybervakuutuksesta voi olla apua taloudellisten menetysten kattamisessa, mutta sen saamiseksi yrityksen on täytettävä tietyt tietoturvatason vaatimukset.

Päätelmät: Kohti digitaalista resilienssiä

Pk-yritysten kyberturvan tilanne on paradoksaalinen: tietoisuus uhista on kasvanut, mutta konkreettiset toimenpiteet laahaavat edelleen perässä. Tämä "uhka huolettaa, mutta emme tee asialle mitään" -mentaliteetti on suurin yksittäinen haaste.

Kyberhyökkäysten todelliset kustannukset ulottuvat kauas lunnaista, ja ne voivat heikentää yrityksen mainetta ja toimintakykyä pysyvästi. Taloudellisten menetysten ohella mainevahingot ja asiakkaiden luottamuksen menetys ovat uhkia, jotka voivat johtaa konkurssiin.

Uudet säädökset, kuten NIS2-direktiivi, pakottavat yritykset nostamaan tietoturvansa tasoa, mutta pelkkä sääntelyn noudattaminen ei riitä. Proaktiivinen ja strateginen lähestymistapa on ratkaiseva. Yritysten on ymmärrettävä, että kyberturvallisuus on edellytys digitalisaation tarjoamien hyötyjen maksimoimiseksi ja toiminnan jatkuvuuden varmistamiseksi.

Raportti päättyy kehotukseen siirtyä reaktiivisesta ajattelusta strategiseen ja ennakoivaan toimintamalliin, joka on elinehto nykyaikaisessa, digitaalisessa toimintaympäristössä. Samalla on huomattava, että tarkkaa tietoa kyberuhkien taloudellisista vaikutuksista Suomen kansantalouteen ja erityisesti mikroyritysten kyberturvaan on toistaiseksi vähän, mikä osoittaa tarpeen lisätutkimukselle.

Ota meihin yhteyttä ja selvitä, miten voit valmistaa yrityksesi tulevaisuuteen.

MD Data Oy
Malminkaari 23A
00700 Helsinki
Y-tunnus: 3313583-3
+358-34-399-360
apu@mddata.fi

Lähdeluettelo

1. Kyselytutkimus: Kyberhyökkäykset huolettavat pienyrityksiä – If, https://www.if.fi/tietoa-ifista/uutishuone?id=kyselytutkimus-kyberhyokkaykset-huolettavat-pienyrityksia-37-percent-ei-kuitenkaan-ole-parantanut-tietoturvaansa
2. Nordic cybersecurity | McKinsey, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/nordic-cybersecurity-the-regions-next-powerhouse
3. New research: Small and medium business (SMB) cyberattacks are frequent and costly – Microsoft https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/SMBCybersecurity-Report-Final.pdf
4. Mitkä ovat yleisimmät tietoturvauhat suomalaisille yrityksille? - JMJping Oy,
5. The Latest Ransomware Statistics (updated June 2025) | AAG IT Support, https://aag-it.com/the-latest-ransomware-statistics/
6. Mitkä ovat yleisimmät tietoturvariskit pk-yrityksissä? - VoiceLink,
7. Yritysten lukumäärä 562 000 vuonna 2021 - Tilastokeskus
8. Yritykset - Elinkeinoelämän keskusliitto, https://ek.fi/tutkittua-tietoa/tietoa-suomen-taloudesta/yritykset/
9. Mikä on pk-yritysten vaikutus talouteen – määritelmällä on väliä - Tilastokeskus, https://stat.fi/tietotrendit/artikkelit/2023/mika-on-pk-yritysten-vaikutus-talouteen-maaritelmalla-on-valia
10. Tietoturvasta huolehtiminen on äärimmäisen tärkeää myös PK-yrityksille, https://yrityksille.elisa.fi/ideat/tietoturvasta-huolehtiminen-on-tarkeaa-myos-pk-yrityksille/
11. Vuosi 2024 muistetaan isoista kybertapauksista - Traficom, https://traficom.fi/fi/ajankohtaista/vuosi-2024-muistetaan-isoista-kybertapauksista
12. Yritys kyberhyökkäyksen kohteena - Varmuuden Vuoksi, https://www.varmuudenvuoksi.fi/artikkeli/yritys-kyberhyokkayksen-kohteena
13. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? - Etla, https://www.etla.fi/wp-content/uploads/ETLA-Muistio-Brief-93.pdf
14. 100+ Ransomware Attack Statistics 2025: Trends & Cost - Astra Security, https://www.getastra.com/blog/security-audit/ransomware-attack-statistics/
15. PK-yrityksen tietoturvaopas | Data Group
16. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi - Kyberturvallisuuskeskus, https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi