Yritysvakoilu 2021

Helsingin seudun kauppakamarin yritysturvallisuuteen liittyvien selvitysten tavoitteena on saada tietoa yritysten turvallisuuden tilanteesta.

Toukokuu 2021

Helsingin seudun kauppakamari
Kalevankatu 12

Helsinki

ESIPUHE

Helsingin seudun kauppakamarin yritysturvallisuuteen liittyvien selvitysten tavoitteena on saada tietoa yritysten turvallisuuden tilanteesta. Selvitysten on tarkoitus auttaa yrityksiä sekä yritysturvallisuuden nykytilan kartoittamisessa että yritysten riskienhallinnan tukemisessa.

Selvityksen tulokset antavat yritysjohtajille eväitä toimivaan riskienhallintaan. Selvityksen avulla voi vertailla, millaisia yritysvakoilu-uhkia yrityksiin kohdistuu, mitä riskienhallinnan keinoja yritykset käyttävät ja kehittää tämän tiedon avulla oman kriittisen tiedon suojaamisen tasoa.

Vastaukset antavat arvokasta tietoa aiheesta, josta ei käydä riittävästi julkista keskustelua. Suuri avoimien vastausten määrä kertoo miten tärkeänä yritysten edustajat aihetta pitävät ja millaista tukea he tarvitsevat tästä merkittävästä uhasta.

Toukokuussa 2021

Helsingin seudun kauppakamari

Panu Vesterinen
selvityksen kirjoittaja

SISÄLLYS

1 JOHDANTO

Tämän selvityksen tavoitteena on tutkia millaisia yritysvakoilu-uhkia yrityksiin kohdistuu ja miten yritykset ovat varautuneet niihin. Tutkimustuloksista yritykset saavat käsityksen tietoaan uhkaavista vakoiluriskeistä ja muiden yritysten käyttämistä riskienhallintakeinoista. Selvitys on osa Helsingin seudun kauppakamarin edunvalvontaa. Se on myös yksi tapa kauppakamarille edistää yritysten toimintaedellytyksiä.

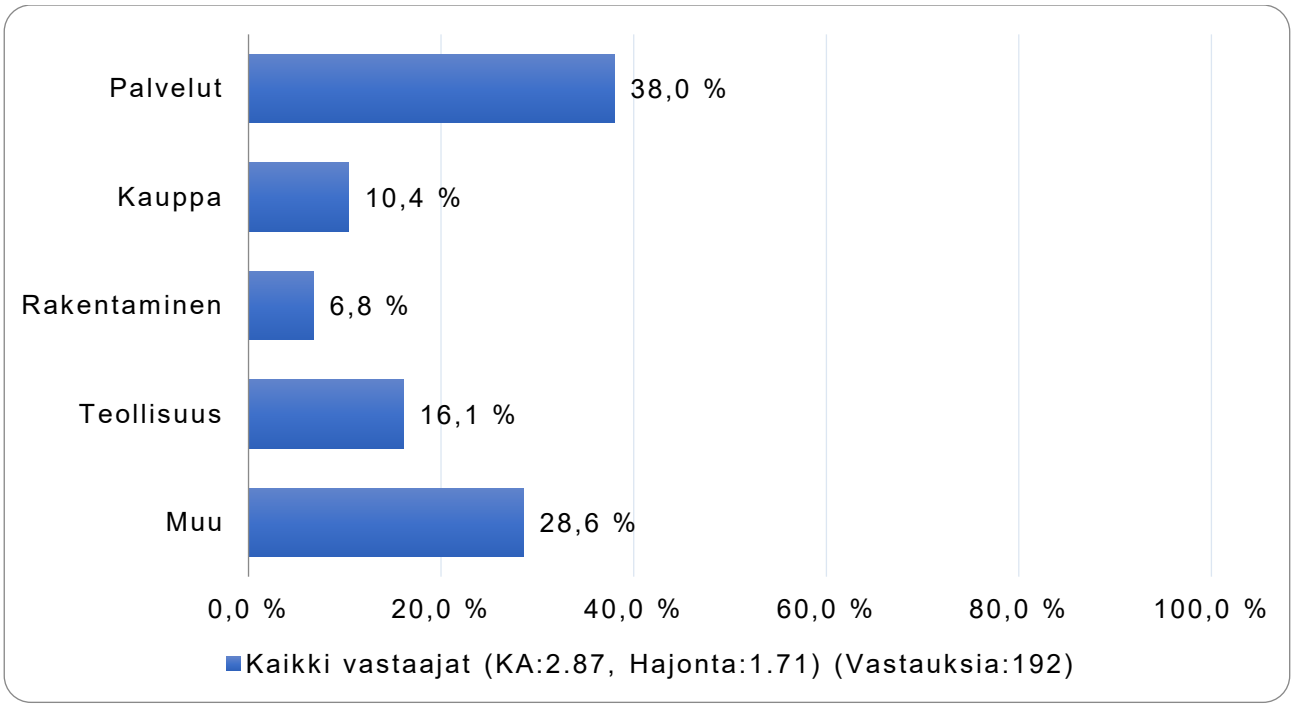
Tässä selvityksessä yritysvakoilusta käytetään muun muassa sanoja vakoilu, tiedustelu, tiedonkeruu, jututtaminen ja urkkiminen. Näin siksi, jotta aiheeseen liittyvää salamyhkäisyyttä ja kasvottomuutta voitaisiin vähentää sanojen tuottamien mielikuvien kautta. Kysymysten joukkoon valittiin vain muutama kyberturvallisuuteen liittyvä kysymys tai vaihtoehto. Siihen on kaksi syytä. Ensimmäinen on se, että olemme vuosina 2015, 2016 ja 2019 toteuttaneet erillisen, kyberuhkiin liittyvän selvityksen ja tulevaisuudessa tulemme jatkamaan näitä selvityksiä. Toinen syy on se, että ammattilaisten viljelemä kyberjargoni on johtanut siihen, että ihmisen keskeinen rooli myös kyberrikoksissa on osin jäänyt teknisten ratkaisujen ja termien taakse piiloon. Haluamme herättää yritykset miettimään ihmisten roolia kaikenlaisessa vakoilussa, tapahtui se sitten tietoverkossa tai reaalimaailmassa.

Koska selvitys laadittiin nyt ensimmäistä kertaa, kysyimme usean kysymyksen kohdalla kysymyksen ”Muu, mikä?”, jotta huomaisimme, jos jokin olennainen asia olisi jäänyt kysymyksistämme pois. Selvitykseen on koottu yritysten antamia avoimia vastauksia kyseisen kysymyksen alle, mutta joitakin näistä vastauksista on myös poimittu herätteiksi eri kohtiin selvitystä.

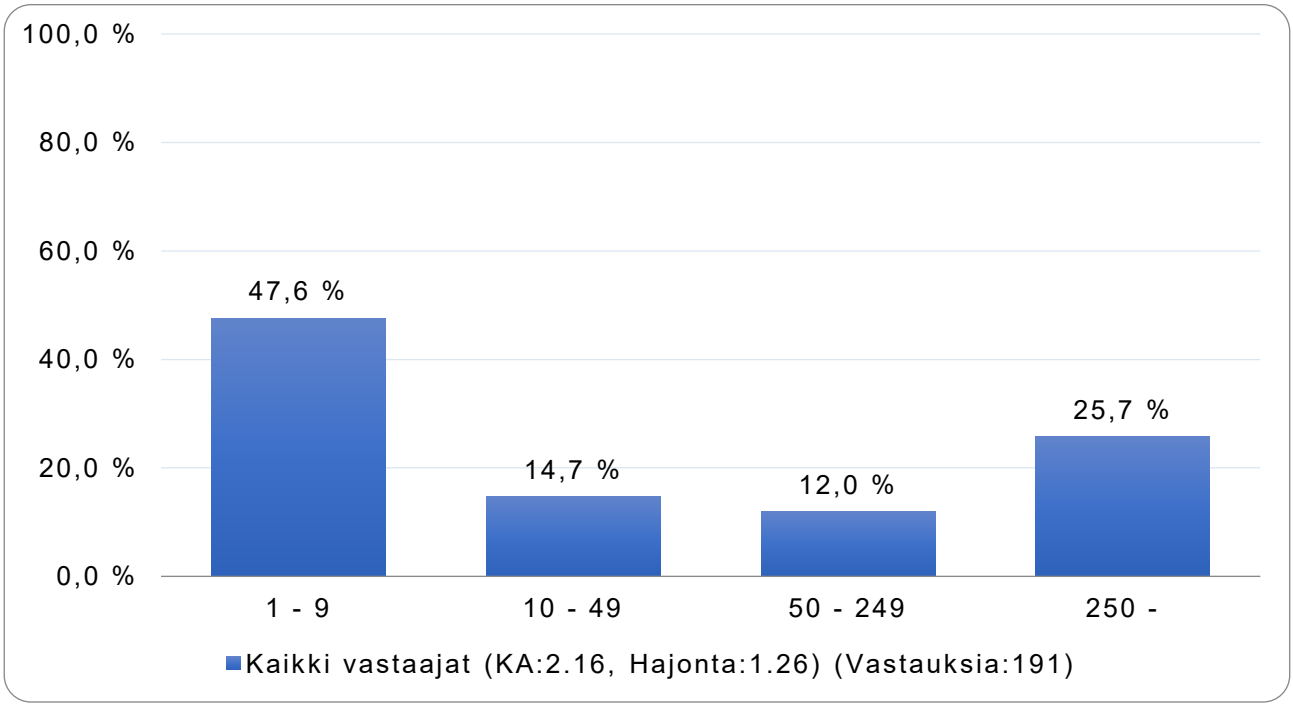
Tutkimuksen toteuttaminen ja vastaajien taustatiedot

Yritysvakoilu 2021 selvitys kattaa kaikki toimialat ja yrityskoot. Selvitys perustuu 192 yrityksen vastauksiin. Helsingin seudun kauppakamari laati kysymykset yhdessä Avarn Security Oy:n ja Elisa Oyj:n kanssa. Selvityksen on laatinut Panu Vesterinen.

Vastanneista yrityksistä 38 prosenttia edustaa palveluita, 16 prosenttia teollisuutta, 10 prosenttia kauppaa ja seitsemän prosenttia rakentamista. Vastaajista 29 prosenttia ilmoitti jonkin muun toimialan kuin yllä mainitun.



Selvityksen vastaajayrityksistä suurin osa (47 %) oli alle 10 henkeä työllistäviä yrityksiä. Toiseksi suurin vastaajaryhmä oli isot yritykset, joita vastaajista oli 26 %. Alle 50 henkeä työllistäviä oli 15 % ja alle 250 henkeä työllistäviä 12 %.



2 YRITYSVAKOILUSTA

Yritysvakoilu on todellinen uhka kaikenkokoisille yrityksille. Maailmalla on jopa olemassa vakoiluun erikoistuneita yrityksiä, jotka varastavat yrityksiltä tietoja ja myyvät niitä muille yrityksille. Tai toimivat suoraan toimeksiannosta ja kohdeyritys määrittyy tällöin toimeksiantajan tarpeen mukaisesti.

Yritysvakoilu ei kohdistu perinteisestä käsityksestä huolimatta vain puolustusalan yrityksiin. Maailmalla on ollut tapauksia, joissa vakoilu on kohdistunut yrityksiin, jotka ovat tuottaneet kaikkea alkaen riisistä ja maissinsiemenistä tuuliturbiinien ohjelmistoihin sekä huippuluokan lääkinnällisiin laitteisiin. Ja vakoilua ei ole kohdistettu vain innovaatioihin ja tuotekehitystoimintaan, vaan kohteeksi on kelvannut esimerkiksi kustannus- ja hintatiedot, sisäiset strategia-asiakirjat ja työntekijöiden henkilökohtaiset tiedot. Yritysvakoilua kohdistetaan myös yliopistojen huippututkimukseen, eikä akateeminen maailma muutoinkaan ole millään tavalla immuuni vakoilulle. Päinvastoin, mitä avoimemmin yliopisto toimii, sitä houkuttelevampi kohde se voi olla.

> ***”Oma kokemus yliopistosta kauppatieteistä v. 2000; Kiinalaiset opiskelijat tulivat ryminällä opiskelemaan, opetuskieli vaihtui englanniksi, mikä heikensi opetuksen tasoa. Ahkerina nämä hankkiutuivat iltatöihin esim. Nokialle. En usko että Suomen reissu oli kaikille pyyteetöntä. Yliopisto tuijotti vain omia intressejään valmistuneiden määrissä ja kansallinen turvallisuus unohtui mielestäni. Luulen, että teollisuusvakoilua tapahtui. Samalla kotimaan opetuksen laatu kärsi. => valtiollisten toimijoiden (esim. yliopisto) ansainta ei saisi ajaa kansallisten turvallisuus- ja ekonomististen tavoitteiden ohitse.”***

Yritysvakoilun määrän kehitystä on käytännössä mahdotonta arvioida pelkästään poliisin tilastojen perusteella. Piilorikollisuuden suuri osuus johtuu pääasiassa yritysvakoilurikosten ilmoittamishalukkuudesta Yritykset eivät läheskään aina ilmoita epäilyistä poliisille.

Yritysvakoilun kohteena voi siis olla mikä tahansa seikka, joka voi antaa vakoilevalle taholle kilpailuedun tai välillisesti mahdollisuuden saada tällainen tieto haltuunsa. Yritysvakoilu kohdistuu lähes mille tahansa liiketoiminnan sektorille ja siihen käytetään kaikkia mahdollisia keinoja - laillisia ja laittomia - ja siksi myös vastatoimien pitäisi olla nykyistä laajemmin tunnettuja ja käytössä yleisemmin, yhteistyön viranomaisten ja elinkeinoelämän kanssa tiivistä ja viranomaisille tehtävien ilmoitusten tekokynnyksen matalalla.

> ***”Lisää henkilötyövuosia viranomaisille tutkintaan ja koulutukseen. Tutkinta on voimatonta, liian varovaista ja tuloksetonta.”***

Tehokkaaseen vastatoimintaan tarvitaan aina sekä viranomaisia ja elinkeinoelämää. Siksi viranomaisten tulisi antaa laajemmin tukea ja antaa tietoa yrityksille ja yliopistoille suomalaisen tietopääoman suojelemiseksi. Viranomaisten tulisi toiminnassaan tarkastella jo ulkomaisia investointeja sellaisiin suomalaisiin yrityksiin, jotka kehittävät tai jo tuottavat kriittistä teknologiaa tai muita kriittisiä tuotteita tai keräävät kansalaisten arkaluonteisia henkilötietoja. Yritysostot ovat yksi laillinen tapa saada haluttu teknologia tai muu liikesalaisuus haltuunsa. Jos kyseinen tieto on esimerkiksi kansalliselle turvallisuudelle merkittävä, on viranomaisten oltava ajan tasalla estääkseen lain mahdollistamassa tapauksissa vaikutusvallan siirtyminen ulkomaisille ostajille. (Ulkomaalaisten yritysostojen seurannasta annetun laki.)

Usein yritysvakoilu keskittyy ihmisiin tai tapahtuu ihmisten kautta. Julkisuudessa haastatellut hakkeritkin ovat kertoneet, että pääsy yrityksen verkkoon on usein nopeinta ja helpointa käyttämällä sähköpostia ja siinä klikattavaa linkkiä tai tiedostoa, joka lataa tarvittavan haittaohjelman. Sen kautta voi käynnistyä vuosia kestävä verkkovakoilu, jota kyseisen sähköpostin vastaanottanut henkilö ei koskaan huomaa eikä se millään tavalla kohdistu hänen hallussaan olevaan tai pääsyn alaiseen tietoon. On työläämpää ja hitaampaa murtautua yrityksen tietoverkkoon ilman ihmisen hyödyntämistä tavalla tai toisella. Ja rikoksesta jää myös enemmän jälkiä puolustajien havaittavaksi ja sitä kautta rikollisen toiminta-aika voi lyhentyä huomattavasti.

> ***”Tieto on ammattitaitoisen henkilöstön lisäksi tärkein "omaisuus". Jos tieto menetetään, menetetään maine ja sen seurauksena luottamus…”***

Toisinaan tarvittava tieto voidaan saada arkisesti ”jututtamalla” henkilöä kasvokkain, puhelimessa, Teamsissä tai sähköpostilla. Henkilöitä, jotka saavat tietoa manipuloimalla ihmisiä, kutsutaan englanninkielisellä termillä social engineer eli sosiaalisiksi ”insinööreiksi”. Turvallisuusammattilaisten jargon johtaa joskus tilanteeseen, jossa työntekijä ymmärtää uhan väärin. Turvallisuuden kannalta tehokkaampaa olisi kutsua uhkia ammattitermien sijaan sellaisilla nimityksillä, jotka kohtaavat työntekijän arjen paremmin kun kömpelöt käännökset. Mikäli näitä yritysvakoilijoita kutsuttaisiin nimillä urkkija tai jututtaja, voisi useampi työntekijä tunnistaa tilanteen jossa häneltä yritetään urkkia jotain tietoa. Työntekijän pitäisi tunnistaa

sosiaalinen manipulointi jutusteluksi tai keskusteluksi ja ymmärtää että tavallinen jutustelu on juuri sitä mitä mystinen ”social engineer” tekee.

> ***”Meille tullut sähköposti ja sosiaalisen median kyselyitä, joissa kyselijää ei voitu yhdistää todelliseen henkilöön.”***

Nämä ”jututtajat” ovat tunnustaneet haastatteluissa, että ihmiset ovat heikoin lenkki lähes minkä organisaation turvallisuudessa. Jos yritysvakoilun tieksi on valittu kyberrikos, turvallisuusjärjestelyiden ohittaminen ja paljastumiselta välttyminen, tiedustelun suorittaminen ja vakoilun kohdentaminen saattavat viedä aikaa. Jos vaakakupissa on muutama hyvin valittu puhelu tai rento tapaaminen baarissa, jotka voivat helposti antaa jututtajille riittävän suuren osan tarvitsemastaan tiedosta, on aika helppo nähdä kumpaan vakoilija päätyy. Saatu tieto voi olla myös ”avustavaa tietoa”, jonka avulla kyberrikoksen tekeminen ja vakoilun toteuttaminen voidaan kohdistaa suoraan haluttuun henkilöön tai osaan tietojärjestelmää ja näin nopeuttaa operaatiota huomattavasti.

> ***”Keskustelua työntekijän kanssa ja jutustelua toimintatavoista.”***

3 YRITYSVAKOILU UHKANA YRITYKSILLE

Tämän luvun lopussa on vastauksia avoimiin kysymyksiin. Ne avaavat yritysten kokemuksia ja näkökantoja.

Yritysten välisessä vakoilussa on helpointa käyttää sisäpiiriläisiä, värvättyjä tai ”sijoitettuja” henkilöitä. Silloin hyötyvän tahon ei tarvitse käyttää kyberrikoksia eikä teoista lähtökohtaisesti jää mitään arjen työtehtävästä poikkeavaa jälkeä, josta voisi helposti epäillä yritysvakoilua tapahtuneen. Tietoa havitteleva taho saa aina etulyöntiaseman, kun tietoa havitteleva taho käyttää henkilöä jolla on syystä tai toisesta pääsy kohdeyrityksen tiloihin tai tietojärjestelmiin, koska tietoa haettaessa ei lähtökohtaisesti tehdä mitään normaalista poikkeavaa.

Harvemmin tapahtuvaa, mutta mahdollista varsinkin suurempien yritysten kohdalla on, että kilpailijat voivat istuttaa kohdeyritykseen ”myyriä”, jotka toimivat säännöllisinä työntekijöinä ja keräävät alusta alkaen salaa tietoa todelliselle työnantajalleen. Merkittävä tätä riskiä lisäävä tekijä on yrityksen kansainvälinen toiminta ja sitä kautta näkyvyys laittomia keinoja herkemmin käyttäville kilpailijoille. Kilpailukeinot Suomen ulkopuolella ovat toisenlaisia ja toimintakulttuuri voi maasta riippuen olla suvaitseva tai välinpitämätön rikollisilla keinolla hankittua tietoa kohtaan. Ja kuten myöhemmistä vastauksista käy ilmi, suomalaisetkin toimijat vakoilevat toisiaan.

> ***”Työsuhteeseen valittuja henkilöitä, jonka taustat ja koulutushistoria koettiin tarkemman tarkastelun perusteella epäselviksi. Pyrkivät oikeiden työtehtäviensä sijasta verkostoitumaan silmiinpistävän tehokkaasti eri asiakkaiden päättäjien ja avainhenkilöstön kanssa, usein ilman työnantajan valtuutusta tai omiin työtehtäviin liittyvää tarvetta. Työtehtäviin liittyvissä asioissa esim. ulkoisten asiakkaiden kanssa, työote oli "tiedusteleva" jolloin pyynnöt usein ylittivät normaaleissa työtehtävissä tarvittavat tarpeet.”***
>
> ***”Sama identtinen malli tuli markkinoille kahden vuoden kuluttua. Samalla aikaisemmat yhteistyökumppanit siirtyivät tämän yhtiön palvelukseen.”***

Kilpailija tai tämän palkkaama taho voi lähestyä kohdeyrityksen luotettavina pidettyjä työntekijöitä, joilla on pääsy luottamukselliseen tietoon, pyytämällä heiltä liikesalaisuuksia ja muuta arvokasta tietoa tarjoamalla heille vastineena rahaa tai kiristämällä heitä yhteistyöhön. Tällaisten työntekijöiden haitallista toimintaa on paljon vaikeampi havaita kuin hakkerointihyökkäyksiä, mikä tekee siitä paljon turvallisemman tavan toimeksiantajalle.

Sisäpiiriläinen tai sen lähellä oleva henkilö voidaan myös houkutella vapaaehtoisesti tarjoamaan tietoja. Kohde vaihtelee osin sen mukaan, halutaanko suoraan liikesalaisuuksia vai halutaanko löytää henkilö jolta tietoa halutaan ja päästä kontaktiin kanssa. Sisäpiirin lähellä olevaa henkilöä voidaan käyttää varsinaisen kohteen osoittajana ja heikkouksien kertojana, Hyödyllisiä tietoja vakoilijalle voivat olla elämäntilanne, urakehitys, todellinen asema yrityksessä ja heikkoudet, Vaihtoehtona on painostaa tai kiristää henkilö luovuttamaan tietoa, mutta tällöin riski jäädä kiinni kasvaa. Kohdehenkilö voi reagoida yllättävällä tavalla ja ilmoittaa asiasta omalle työnantajalleen. Houkuteltu ihminen taas ei aina ymmärrä tai halua ymmärtää asianlaitaa, vaan oikeuttaa tekonsa henkilökohtaisilla perusteillaan.

Maailmalla on tunnettu käsite MICE, joka tulee sanoista ”money, ideology, coersion ja ego”. On olemassa tutkimuksia, jotka osoittavat että oikeaan työntekijään kohdistettuna jokin näistä neljästä - raha, ideologia, painostaminen tai ego - on tie työnantajan liikesalaisuuksiin.

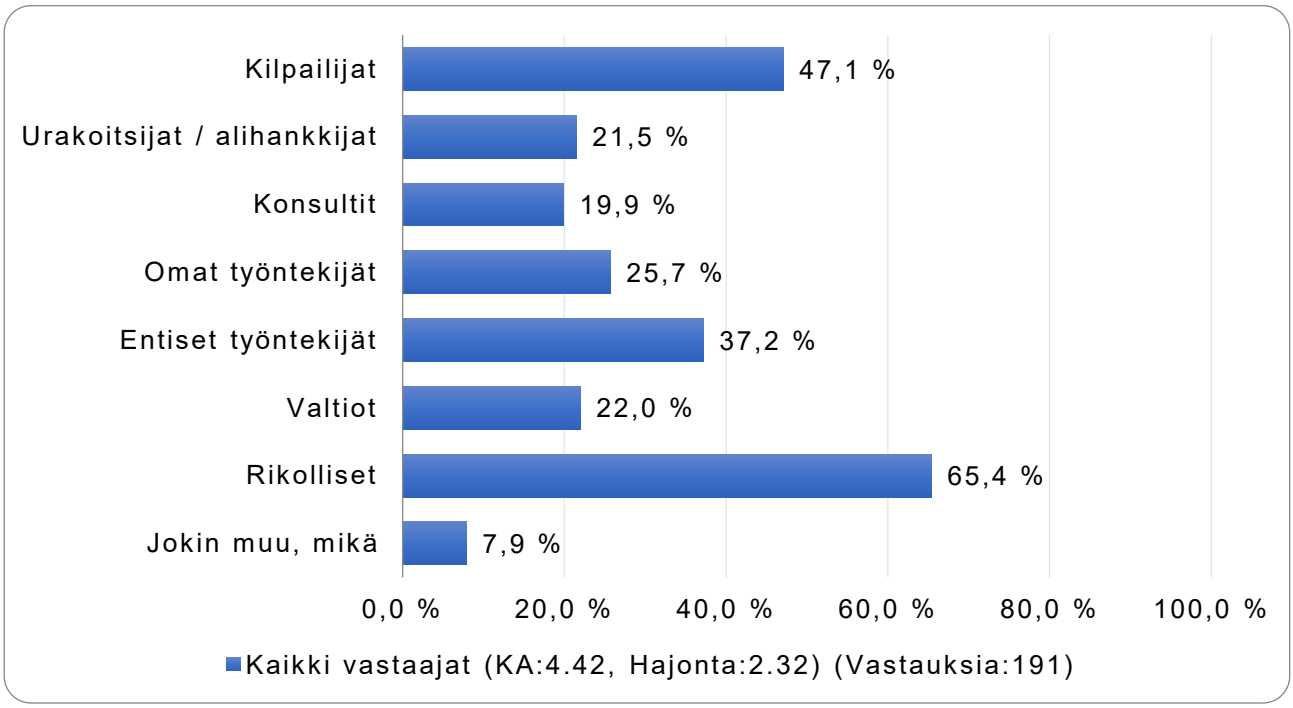
Sisäpiiriläiseltä tai hänen lähellä olevaa henkilöä voidaan aluksi pyytää merkityksettömiä tietoja ja kun hän on vähitellen saatu luovuttamaan tietoa, jonka antaminen on täyttänyt rikoksen tai sen antamisen paljastaminen vahingoittaisi sen antajaa, häntä kiristetään ja painostetaan luovuttamaan aina vain arkaluonteisempaa materiaalia. Askel askeleelta luodaan tilanne, jossa henkilö ei voi kuin totella vaatimuksia paljastumisen pelossa.

Maailmalta löytyy valitettavasti laaja joukko yritysvakoilua harjoittavia ihmisiä. Kohteeksi voi valikoitua messuilla, seminaareissa, työmatkoilla, ulkomaan komennuksilla tai melkein missä vain. Yleisempää se on tilanteissa, joissa kohdehenkilö on yksin ja häntä on helppo lähestyä ilman kiirettä.

Työntekijät voivat myös tahattomasti auttaa tai olla välikätenä yritysvakoilussa. Toimistolle tai aulaan on voitu jättää satunnainen USB-tikku, jonka utelias työntekijä voi huomata ja kytkeä työtietokoneeseensa. Toinen työntekijä voi saada huolellisesti kirjoitetun sähköpostin, joka saa vastaanottajan napsauttamaan linkkiä tai avaamaan liitetiedoston. Nämä esimerkit ovat vain kaksi monista tavoista, joiden kautta haittaohjelmat voivat

päästä yrityksen tietojärjestelmään. Tällainen haittaohjelma voi sitten avata vakoilijalle täyden pääsyn arkaluonteisiin tietoihin.

Ketkä seuraavista voisivat mielestäsi olla suurin uhka yritysvakoilijoina?



Vastaajayritysten mukaan viisi suurinta vakoilu-uhkaa yritykselle ovat:

1. Rikolliset
2. Kilpailijat
3. Entiset työntekijät
4. Omat työntekijät
5. Valtiot

Yritykset mieltävät rikolliset suurimmaksi uhaksi. Tämä tarkoittaa, että yritysten suojautuminen rikoksia vastaan nostaa myös yrityksen turvallisuutta yritysvakoilua vastaan. Kilpailijat voivat käyttää ”tavallisia” rikollisia ja pyrkiä näin häivyttämään omaa rooliaan, jos tekijä jää kiinni. Työntekijöiden rooli vakoilussa on merkittävä ja vastaajat ovat tämän huomioineet hyvin. Sisäinen uhka on tekijä, jota on haastava torjua, mutta sen aiheuttamaa vahinkoa voidaan rajata ja kynnystä nostaa alkaen aktiivisesta pääsyoikeuksien rajaamisesta ja ylläpidosta. Viidenneksi suurimpana uhkana vastaajat pitivät valtioita. Jotkut valtiot tukevat omien lakiensa valtuuttamina maansa elinkeinoelämää ja vakoilulla hankittu tieto voi olla osa tätä toimintaa. Jotkut valtiot voivat velvoittaa ulkomaille opiskelemaan tai työskentelemään lähteviä henkilöitä keräämään tietoa koko ulkomailla oloaikansa ja tuomaan tai lähettämään sen kotimaahansa ja haastattelevat näitä henkilöitä säännöllisesti.

On tärkeä varmistaa, että irtisanotut työntekijät eivät pääse enää irtisanomisaikana tai sen jälkeen yrityksen tietoihin. Näin käy kuitenkin yllättävän usein. Ei tarvita kuin yksi entinen työntekijä, jolla on motiivi vahingoittaa entistä työnantajaa.

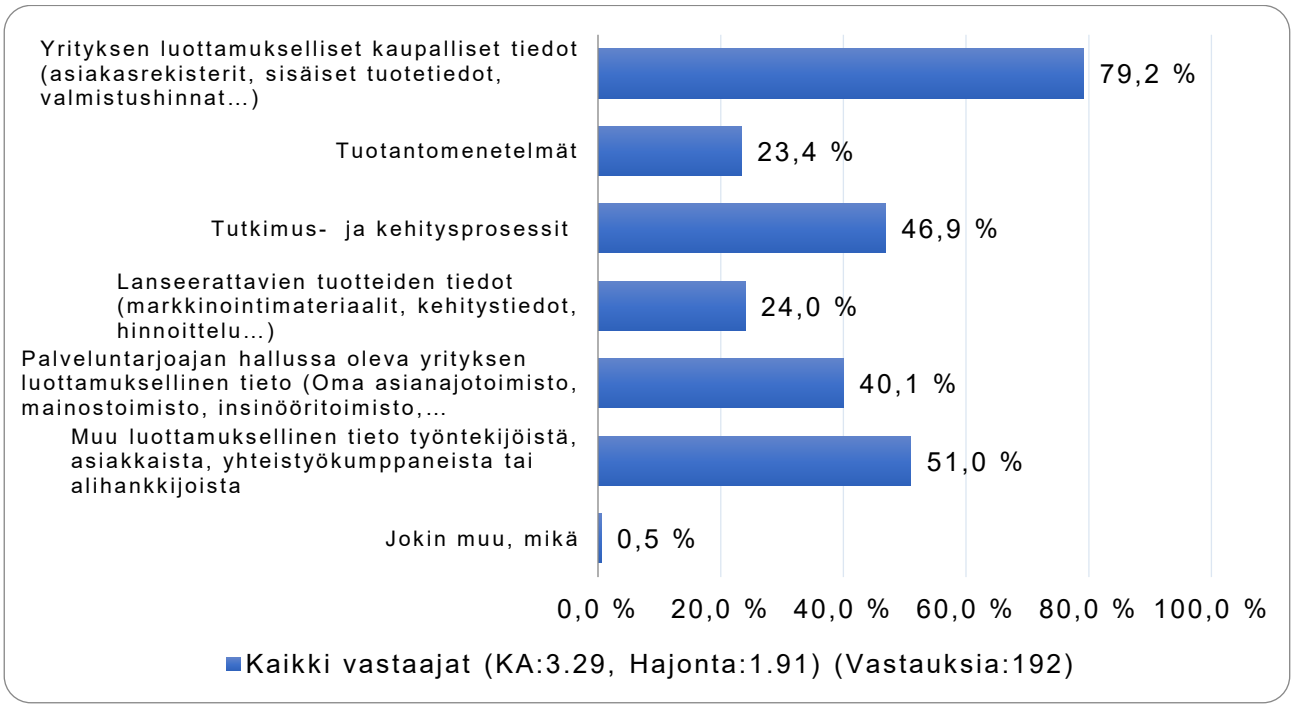
Joissain tapauksissa yritysvakoilu suoritetaan käytännössä parin viimeisen työviikon aikana. Jos työntekijöiden tunnukset ja salasanat ovat edelleen voimassa irtisanomisen jälkeen, he voivat käyttää arkaluontoisia tietoja haitallisiin tarkoituksiin työntekovelvoitteen päätymisen jälkeenkin.

Yrityksen kannattaa kehittää ja ottaa käyttöön asianmukainen irtisanomismenettely, joka suojaa yritystä entisten työntekijöiden mahdollisilta rikoksilta. Käyttö- ja pääsyoikeuksia tietoon ja työnantajan tietokoneita ei joissain tilanteissa voi jättää edes irtisanomisajaksi työntekijälle.
Vastausvaihtoehto ”Muu., mikä?” keräsi seuraavanlaisia vastauksia:

- ulkomaiset edustajat, edustajat tarjouskilpailuissa ulkomailla

- pääomasijoittajat
- NGO järjestöt (Non Governmental Organisation)
- oikeudenkäynnin vastapuolet
- media
- aktivistit
- johto, joka ei ymmärrä, että vakoiluriski koskee myös meitä eikä siten luo edellytyksiä suojautumisen edistämiselle.
- asiakkaat, joille on luotettu salassa pidettävää materiaalia, josta he maksavat lisenssimaksuja
- asiakkaat
- virkamiehet ja poliitikot
- työntekijä joutuu ulkopuolisen kiristyksen kohteeksi , syystä tai toisesta
- ihan vaan häiriköt ja ilkivaltaa tekevät ihmiset.

Millaisiin tietoihin yritysvakoilua mielestäsi kohdistetaan?



Yleisimmät yritysvakoilun mielenkiinnon kohteet vastaajien mukaan olivat:

1. yrityksen luottamuksellinen kaupallinen tieto
2. muu luottamuksellinen tieto työntekijöistä, asiakkaista tai alihankkijoista
3. tutkimus- ja kehitysprosessit
4. palveluntarjoajan hallussa oleva luottamuksellinen tieto
5. lanseerattavien tuotteiden tiedot.

Merkittävä seikka näissä vastauksissa on se, että vastaajayritykset mielsivät yrityksen kaupallisen luottamuksellisen tiedon vakoilun kohteeksi. Yli 15 vuoden aikana toteutetuissa kauppakamarin selvityksissä vain osa yrityksistä on mieltänyt sillä olevan tietoa, jonka joku voisi haluta. Jokaisella yrityksellä on asiakasrekisteri, hintatietoa ja muuta, jota epärehellisillä keinoilla kilpaileva taho voi haluta ja mistä se voi hyötyä yrityksen kustannuksella. Myös tieto työntekijöistä, asiakkaista tai alihankkijoista voi olla vakoilijan haluamaa.

"Kohteena oli lautapelin rakenne."

Jo vuosien ajan palveluntarjoajat ovat olleet vakoilijoiden kohteena. Kaikki asianajotoimistot, mainostoimistot tai insinööritoimistot eivät suojaa tietoa yhtä hyvin kuin tiedon omistava toimeksiantaja. Ja johtuen palveluntarjoajien toimialasta, hallussa oleva tieto on usein luottamuksellista tai salassa pidettävää. Helsingin seudun kauppakamari on varoitellut asiasta jo kymmenen vuoden ajan. On hyvin tärkeää, että tiedon omistaja - pieni tai suuri yritys - varmistaa sen, että palveluntarjoaja ei ole tiedonsuojaamisen heikko

lenkki. Vakoilijat osaavat hyödyntää palveluntarjoajien heikkouden. Miksi hakea tieto suojatusta toimitilasta erilaisten turvallisuusjärjestelmien takaa, kun sen voi saada helpommin palveluntarjoajan hallusta?

Vastausvaihtoehdossa ”Muu, mikä?” nousi esille seuraava vastaus:

- kansallinen turvallisuus -> huoltovarmuuskriittiset yritykset ja toimijat.

Esimerkkejä miten yrityksen joitain tietoja voidaan hyödyntää ja miksi vakoilija haluaisi tiedon

1. **Liikesalaisuudet**
   Vaikka liikesalaisuuden määritelmä vaihtelee maittain, se tarkoittaa yleensä suojattua yritykselle arvokasta tietoa olemassa olevista tai kehitteillä olevista tuotteista, menetelmistä tai muista kaupallisista yksityiskohdista. Nämä tiedot voivat auttaa kilpailijaa tekemään tuotteistaan kilpailukykyisempiä tai jopa tuoda samanlaisen tuotteen markkinoille nopeammin kuin kohdeyritys.

2. **Asiakastiedot**
   Asiakkaiden tietoja, mukaan lukien taloudelliset tiedot, voidaan käyttää markkinaosuuden tai liiketoiminnan viemiseen tai ne voivat vuotaa vahingoittamaan kohdeyrityksen mainetta.

3. **Taloustiedot**
   Yrityksen taloudellisia tietoja voidaan käyttää tarjoamaan parempia tarjouksia asiakkaille ja kumppaneille, voittamaan tarjouksia ja jopa tekemään parempia tarjouksia tärkeille työntekijöille.

4. **Markkinointitiedot**
   Niiden avulla kilpailijat voivat valmistautua oikeaan aikaan kohdeyrityksen markkinointikampanjoihin, mikä voi syödä niiden toivottua vaikutusta myynnille ja kannattavuudelle.

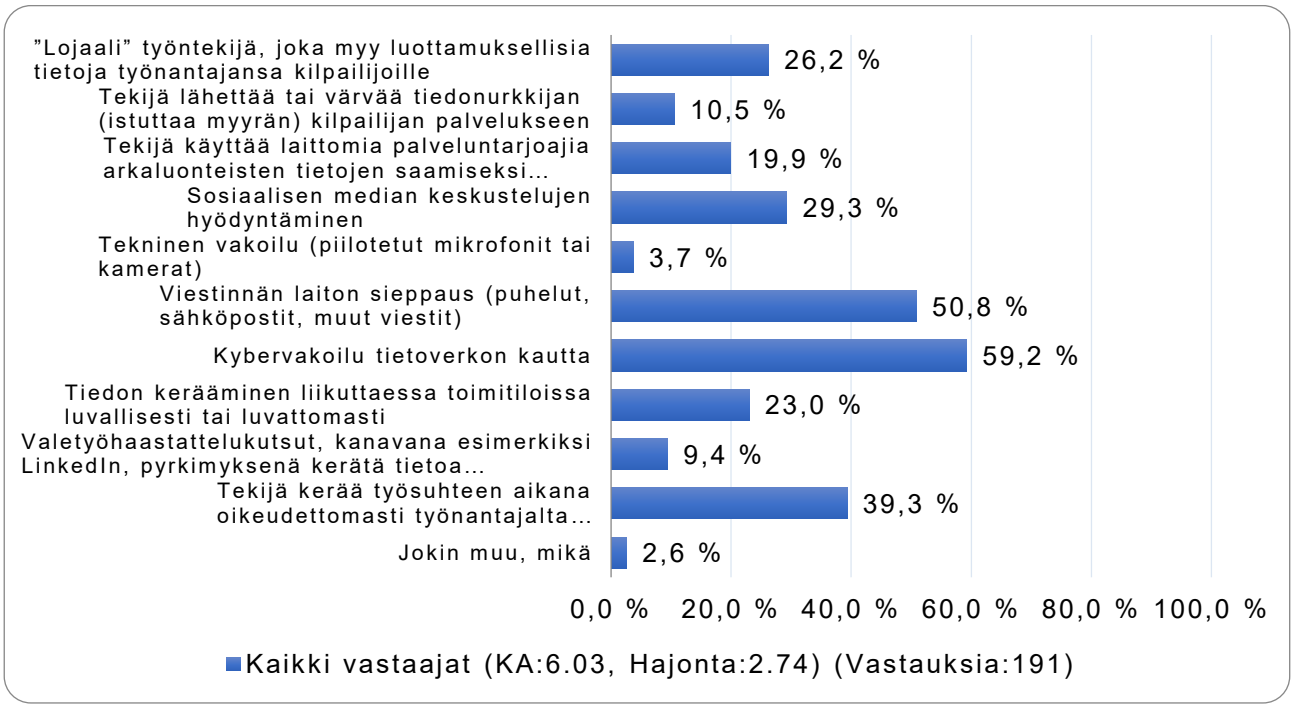
“Globaali ohjelmistokehityshanke kiinnostaa alan toimijoita”

”Vakoilu kohdistui yritykseni tarjouslaadintaprosessiin, tarjousdokumentteihin, hinnoitteluun…”

”Olemme huoltovarmuuskriittisen toimialan yritys. Kehittämistyö (uusia tuotantomenetelmiä ja
-tekniikoita) herättää kiinnostusta.”

”Asiakaspohja todennäköisesti kiinnostava tiettyjen valtioiden osalta.”

Mitkä kolme seuraavista ovat käsityksesi mukaan yleisimmät tavat vakoilla yrityksiä?



Yleisimmät tavat vakoilla yritystä ovat vastaajien mukaan seuraavat:

1. kybervakoilu tietoverkon kautta
2. viestinnän laiton sieppaus
3. työntekijä kerää laittomasti työsuhteen aikana työnantajan luottamuksellista tietoa
4. ”lojaali” työntekijä myy työnantajansa luottamuksellisia tietoa kilpailijoille
5. sosiaalisen median keskustelujen hyödyntäminen.

Vastaajat pitivät kybervakoilua yleisimpänä vakoilutapana. Se on yleistä, mutta sijoitukseen vaikuttaa myös sen julkisuus. Viimeisen kymmenen vuoden aikana kyberuhasta on tullut julkisempi keskustelunaihe kuin ennen. Aiemmin uhasta ei ollut juurikaan puhuttu julkisuudessa Suojelupoliisin varoituksia lukuun ottamatta. Julkisuuden mukanaan tuoma tietoisuus on osaltaan osoitus siitä, että julkinen keskustelu on tehokas tapa lisätä yritysten tietoisuutta.

Vaikka on helppoa puhua erilaisista tavoista vakoilla ja samalla tuoda esille miten vaikeaa voi olla torjua vakoilua, on hyvä mieltää seuraava. Yritys voi torjua vakoilua ja sen kannattaa aina aloittaa tiedon suojaaminen siitä, että se selvittää itselleen mitkä tiedot ovat tärkeitä ja vain yrityksen omassa hallussa.

Sen jälkeen kannattaa miettiä miten tietoa käytetään ja säilytetään yrityksen toiminnassa. Sitten voi alkaa miettiä miten sitä on tarpeen suojata eri tilanteissa. Tiedon suojaaminen kannattaa siis aloittaa tiedosta käsin, ei siitä miten monella eri tavalla se voi päätyä vääriin käsiin.

Suojattavan tiedon löytämisen ja suojaamisen tarpeen selvittämisen jälkeen voi miettiä tiedon arvoa ulkopuoliselle taholle ja sitä mikä taho voisi hyötyä tiedosta. Näin voi saada käsityksen siitä miten haluttua ja arvokasta tieto voi ulkopuoliselle olla. Yksinkertainen kysymys voi olla: ”Mitä tietoamme minä arvostaisin, jos olisin kilpailija?”

> ***“Ulkomaalainen, vastakkaista sukupuolta edustava henkilö yrittänyt hakeutua useita kertoja seuraan uskonnollisen yhdyskunnan tilaisuuksissa.”***
>
> ***”Yrityksiä ujuttautua yrityksen liiketoiminnan ostajaksi ja tarkoitus vakoilla yrityssalaista tietoa.”***

Kun arvo ja mahdollisesti siitä hyötyvät tahot on selvillä, voi alkaa miettiä sitä, miten joku voisi tietoa tavoitella. Tätä kautta voi päästä ymmärrykseen siitä miten tietoa tarvitsee suojata. Kaikkea ei tarvitse

suojata samalla intensiteetillä. Johonkin tietoon voi riittää hyvin hallinnoidut pääsyoikeusprosessit ja jotain tietoa ei esimerkiksi kannata käsitellä missään tietolaitteessa, josta on yhteys internettiin.

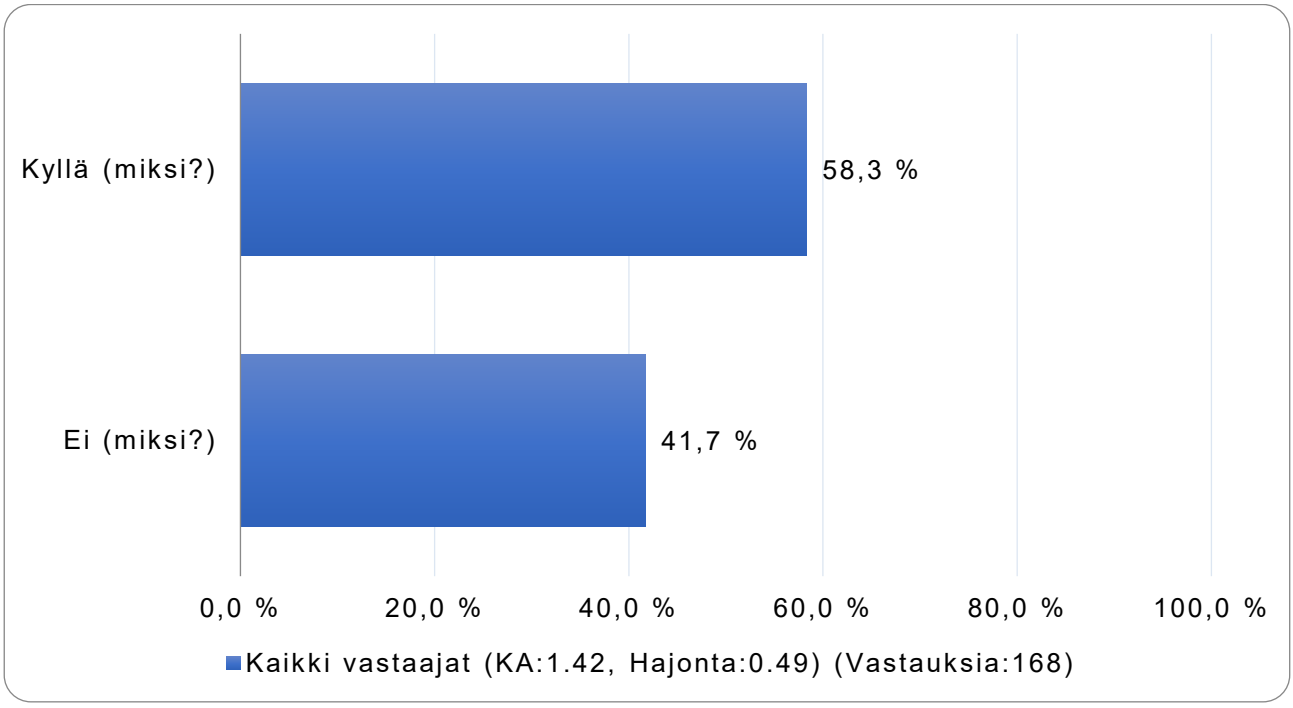
Työntekijän kerätessä tietoa ja viedessään sen mukanaan kyse ei automaattisesti ole yritysvakoilusta. Jos työntekijä vielä lähtiessään työsuhteesta tietoa, johon hänellä on pääsy- ja käyttöoikeus ja käyttää sitä tai paljastaa sen uudessa työpaikassaan, on kyse yrityssalaisuuden rikkomisesta ja mikäli työntekijällä on ollut salassapitositoumus, voi hän joutua korvausvelvolliseksi sen rikkomisesta.

Mikäli työntekijä hankkii tai kerää työsuhteen aikana liikesalaisuuksia, joihin hänellä ei ole pääsy- tai käyttöoikeutta, syyllistyy hän tällöin yritysvakoiluun. Ratkaisevaa näiden osalta on se, oliko työntekijällä edellä mainittu oikeus vai ei.

Vastausvaihtoehto ”Muu, mikä?” keräsi seuraavanlaisia vastauksia:

- pääomasijoittajien tutkimukset yrityksestä (joskus NDA joskus ei) yhtälailla IPRistä niin tekniset kuin taloudelliset selvitykset
- välillä tulee vastauspyyntöjä erinäisiin tutkimuksiin ja joukossa on mahdollisesti pelkkää tiedon urkintaa.
- ex-työntekijä kertoo tietonsa eteenpäin
- hölösuisten työntekijöiden juttujen kuuntelu ja niiden lypsäminen
- virkamiehet ja poliitikot.

Luuletko yrityksesi ja / tai toimialasi olevan potentiaalinen kohde yritysvakoilulle?



Yli puolet (58 %) vastaajayrityksistä mieltää olevansa potentiaalinen kohde yritysvakoilulle. On vaikea varmasti sanoa, mikä yrityksistä on todennäköinen kohde, siksi kysymys muotoiltiin näin. Totta on, että kaikilla yrityksillä on jotain tietoa, josta joku kilpailijoista voisi hyötyä. Kaikki kilpailijat eivät kuitenkaan käytä vakoilua ja jokaisen yrityksen luottamuksellinen tieto ei ole tarpeen kilpailijalle.

Yksikään yritys ei kuitenkaan voi olla varma, ettei olisi potentiaalinen kohde, mutta jokainen yritys ei kuitenkaan todennäköisyyden perusteella päädy yritysvakoilun kohteeksi. Jokaisen yrityksen on kuitenkin tunnistettava liikesalaisuutensa ja päätettävä mikä on riittävä tapa suojata niitä.

Luuletko yrityksesi ja / tai toimialasi olevan potentiaalinen kohde yritysvakoilulle?
– Kyllä (miksi?)

- lähes kaikki toiminta netissä.
- ei oma yritys, mutta väylä asiakkaisiin.
- yhteiskunnallisesti merkittävä rooli
- asiakkaina on suuria suomalaisia yrityksiä
- kova kilpailuasetelma
- huoltovarmuuskriittisen toimialan yritys. Kehittämistyö (uusia tuotantomenetelmiä ja -tekniikoita).
- johtava alallaan
- kilpailu alalla asiakkaista sekä palveluiden hinnoista
- media-alalla infromaatiovaikuttaminen ja painostaminen
- kiinnostus yhteiskunnalliseen toimintaan
- uusien innovaatioiden luulisi kiinnostavan kilpailijoita maailmalla
- kaikki yritykset ovat
- kyseessä on valtakunnallinen terveysalan yritys
- alansa suurin toimija Suomessa.
- asiakkaamme ovat ulkomaisia viranomaisia ja joskus tekemisissä armeijan kanssa.
- käsittelemme arkaluontoisia tietoja, joiden paljastuminen ulkopuolisille olisi paitsi suuri maineriski, myös taloudellinen riski. Rikollinen taho voisi yrittää kiristää meiltä rahaa haltuunsa saamillaan tiedoilla.
- sähköntuotanto on yhteiskunnan kannalta kriittinen toimiala
- tilitoimistossa liikkuu paljon arkaluonteista asiakasdataa ja rahavirtoja ja erilaisia huijausviestejä saamme viikoittain.
- palvelemme useita erilaisia asiakkaita erilaisilla korkean profiilin toimialoilla, esimerkiksi r&d, valmistava teollisuus sekä turvallisuuskriittiset toimijat.
- paljon luottamuksellista tietoa asiakkaista
- sivutoimiala ohjelmistokehitys on tuotekehitystä, joka aina kiinnostaa
- asiakkuudet ovat merkittäviä ja alalla tuotekehitys on keskeisessä asemassa.
- meillä on erittäin laaja asiakas- ja yhteistyökumppaniverkosto ja olemme haasteista huolimatta menestyneet erinomaisesti
- paljon asiakkaiden sensitiivistä tietoa, paljon teknologista tuotekehitystietoa
- tuotantomenetelmät
- paljon henkilötietoja, paljon tietoja eri alojen yrityksistä, heikko suojaus (olemme julkisen sektorin toimija).
- korkean teknologian yritys
- edellä mainituista syistä. yksi entinen työntekijä teki juuri noin, kun lomakkeessa sanottu.
- uusi toimiala, potentiaalisia kilpailijoita kiinnostaa ja halu saada tietoa tuotteista, tuotekehityksestä ym. niche-toimala
- tiedon ja koulutustapojen suojaaminen on hyvin vaikeaa
- tietotekniikka ja sen innovaatiot kiinnostavat.
  Lisäksi toimin useammassa innovaatio-organisaatiossa.
- olemme dynaaminen, alan kärkipään toimija.
- merkittävä markkina-asema
- asiakaspohja todennäköisesti kiinnostava tiettyjen valtioiden osalta
- asiakasrekisterien takia
- kaikki on aina mahdollista
- tieto on ammattitaitoisen henkilöstön lisäksi tärkein "omaisuus". jos tieto menetetään, menetetään maine ja sen seurauksena luottamus jne.
- paljon asiakkaiden henkilökohtaisia tietoja
- taloudelliset resurssit eivät riitä torjumiseen.
- yrityksissä käsitellään henkilöiden yksityisyyteen liittyviä tietoja esim. hetu ja muita vastaavia asioita.
- turvallisuusala
- yritys on suuri ja globaali, ja ilmoittanut investoivansa lähitulevaisuudessa suuria summia tuotekehitykseen ja innovaatioihin.
- uutta teknologia tuotteessa
- puolustusvälineteollisuus, jota edustan, on aina vakoilun kohteena
- käytössä tekniikkaa, jota ei ole muualla käytössä
- kriittinen infra kiinnostaa
- yritys käsittelee yhteiskunnan toimintojen kannalta kriittisiä tietoja.
- teletiloihin pääsyyn liittyen.
- toimiala
- kriittistä infraa

- paljon henkilötietoja
- turvallisuusalan liike, avaintiedot ja avaimet ym.
- luottamuksellista tietoa asiakkaistamme
- finanssialan palvelutuottajana olemme tekemisissä rahoituslaitosten kanssa
- hallussa paljon tietoa yrityksestä, joka voidaan luokitella liikesalaisuudeksi.
- käsittelemme arkaluonteisia tietoja
- käsittelemme luottamuksellisia asiakstietoja
- käsittelemme viranomaisten luottamuksellista tietoa
- globaali ohjelmistokehityshanke kiinnostaa alan toimijoita
- tuotesisältö kilpailutuksissa
- finanssialan yritys, pankkisalaisuuden alaista tietoa, tietoa rahaliikenteen prosesseista ja kohteista
- hyvien tuotteiden tekeminen vaatii erittäin korkeaa tietotaitoa
- raha kiinnostaa rikollisia
- teknologinen osaaminen, tuotteet ja palvelut.
- henkilöstöpalvelua ala on vahvassa murroksessa kilpailumielessä ja ala sisältää paljon henkilötietoa.
- arkaluontoinen tieto
- kehitetään kokoajan uusia ohjelmistoratkaisuja tuleviin tarpeisiin
- ainutlaatuinen osaaminen hyvin kapealla sektorilla.
- uudet menetelmät kiinnostaa
- olemme maailmalla laajalti levinneitä ja tuotteemme ovat suht kalliita.
  Kopioijat pyrkivät tekemään samantyyppistä halvemmalla.
- tietoja käsitellään paljon ja laajassa mittakaavassa, luottamuksellista henkilötietoa
- kilpailijat haluavat saada pois markkinoilta
- pankkiala houkuttaa myös yritysvakoilua
- uuden teknologian kehittäminen, jolle on potentiaalisesti suuret markkinat, etenkin kiinassa.
- meillä käsitellään paljon arkaluonteista tietoa
- uudet tuotteet palveluiden alla, ja supply chain, asiakkaamme kiinnostavat muita.
- terveydenhuolto
- merkittävä taloudellinen ala
- avainhenkilöillä tietoja useista merkittävistä yrityksistä.

Luuletko yrityksesi ja / tai toimialasi olevan potentiaalinen kohde yritysvakoilulle?
– Ei (miksi?)

- emme käsittele taloudellisesti merkittäviä asioita. maineella on toki jokin hinta.
- toimimme palvelualalla
- varsin vähäinen määrä mitään tietoa mitä voi hyödyntää
- toimiala on avoin
- tuotteemme ovat sellaisia, että niille ei haeta patentteja, eikä muita oikeuksia, joten samankaltaisia tuotteita voi helposti olla kilpailijoilla.
- tuotamme koulutuspalveluja.
- valmistusmenetelmämme ovat yleisesti markkinoilta saatavia. tuotteet ovat kopioitavissa ostamalla tuote ja tutkimalla se.
- vastaus on ehkä ei, koska muutamaan vuoteen emme enää ole olleet osallisena sellaisissa projekteissa joiden uskoisimme olevan alttiita yritysvakoilulle.
- tilinpäätökset ovat julkista tietoa
- tuotteet
- pieni palvelutoimisto tuskin kiinnostaa ketään
- pieni toimija marginaalituotteilla
- low tech
- ei merkittävä toimija.
- en osaa sanoa, ehkä liian pieni ja merkityksetön rosvoille mutta enhän minä voi olla tästä varma
- liian pieni business
- opetus on pääosin julkista.
- meidän hommat eivät ole niin innovatiivisia että niiden vakoilusta olisi kenellekään mitään riemua
- ala on hieman konservaativinen, eikä ns uraa uurtavia tuotteita hirveästi keksitä.
- teen henkilöstökonsultointia - yleensä henkilöstöasiat eivät ole niin mielenkiintoisia
- toimiala
- tarkasti useiden viranomaisten valvoma ala, ei etätyömahdollisuutta
- ei sellaista tietopääomaa, jota muu taho kaipaisi.

- pyöritämme aika pientä rahamäärää
- liiketoiminnan volyymi alhainen, toimintaa lopettelemassa.
- toiminta liian pientä
- pieni toimija
- meillä ei ole omia keksintöjä
- pieni
- ei ole rahaa niin paljon yrityksessä ja sen ideoissa
- liian pieni yritys ollakseen kiinnostava vakoilulle.
- sosiaalialan järjestönä emme ole välttämättä kiinnostava kohde.
- tilitoimistot harvoin kehittävät uusia rahakkaita innovaatioita. osa täältä tehdyistä töistä on kuitenkin julkisia, kuten yritysten voitot ja ihmisten verotettavat tulot.
- melko pieni talo, ei mediassa, ei hypeä
- olemme alan toimija ja osaamme varautua asioihin
- käännöstyötä tekevällä yksinyrittäjällä ei ymmärtääkseni ole hallussaan juurikaan mitään sellaista salaista tietoa, joka voisi kiinnostaa ketään muuta. oma toimintani on sitä paitsi minimaalista, koska olen jo lähes 80-vuotias.
- luottamuksellisen tiedon hyödyntämisellä saavutettavat hyödyt ovat niin pienet.
- ei ole mitään sellaista tietoa.
- tilinpäätöstiedot saa laillisesta esim. kaupparekisteristä
- yhden naisen viestintätoimisto, en käsittele asiakkaiden luottamuksellisia tietoja
- liikevaihtotaso alhainen
- on pieni ja liikevaihto alhainen
- liiketoimintamme on vielä aika pientä
- hyödynnettävä tieto ja osaaminen ihmisissä
- emme valmista mitään. lisäksi olemme tehneet monen vuoden ajan yhteistyötä useampien kilpailijoiden kanssa, joten vakoilu ei liene tarpeen.

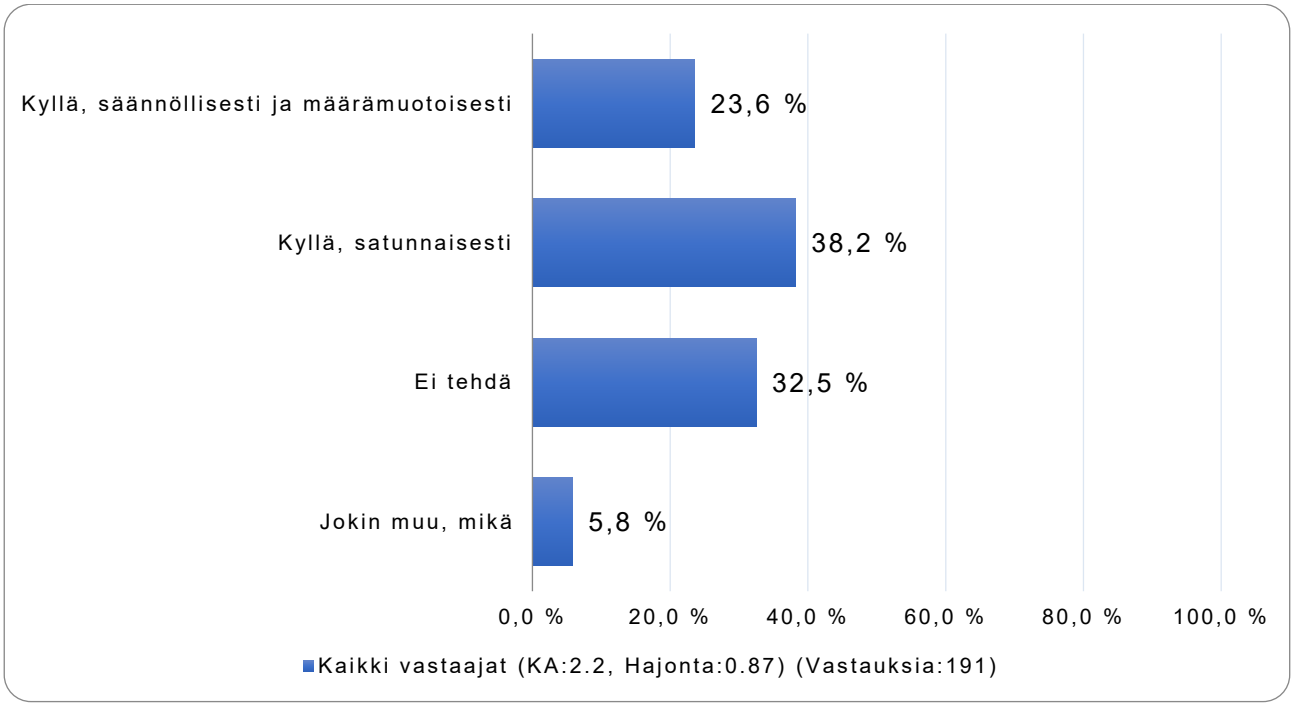
4 YRITYSVAKOILUUN VARAUTUMINEN

Yritysvakoilun torjunnassa riskienarviointi on avain järkevään lähestymistapaan. Kyberriskien tulisi olla huomioituna jokaisen organisaation yritysturvallisuudessa. Yritysvakoilun torjuminen ja vaikeuttaminen ei ole varsinaisesti oma yritysturvallisuuden osa-alueensa, vaan siinä käytetään yritysturvallisuuden eri osa-alueiden, kuten toimitilaturvallisuuden, tietoturvallisuuden ja rikosturvallisuuden, keinoja.

Yrityksen on hyvä laatia epäiltyjen tietoon kohdistuneiden rikosten varalta toimintasuunnitelma ja varmistaa sen toimivuus harjoittelemalla sitä. Parhaimmillaan toimiva suunnitelma auttaa yritystä reagoimaan erilaisissa tietoturvaloukkauksissa ja minimoimaan vaikutukset yritykseesi.

Kyberriskit saattavat kohdistua muita vakoilutapoja todennäköisemmin pieniin ja keskisuuriin yrityksiin. On helpompaa pyrkiä käsiksi pienemmän yrityksen tietoihin tietoverkon kautta kuin käyttää ihmistä tiedon poiminnassa. Tämä ei poissulje ”jututtajien” toimintaa tai työntekijän värväämistä, mutta kyberrikosten ollessa jo varsin yleisiä ja nopeita tapoja päästä yrityksen tietoon, kustannustehokkaasti ajatteleva vakoilija voi ainakin aloittaa vakoilun tietoverkon kautta.

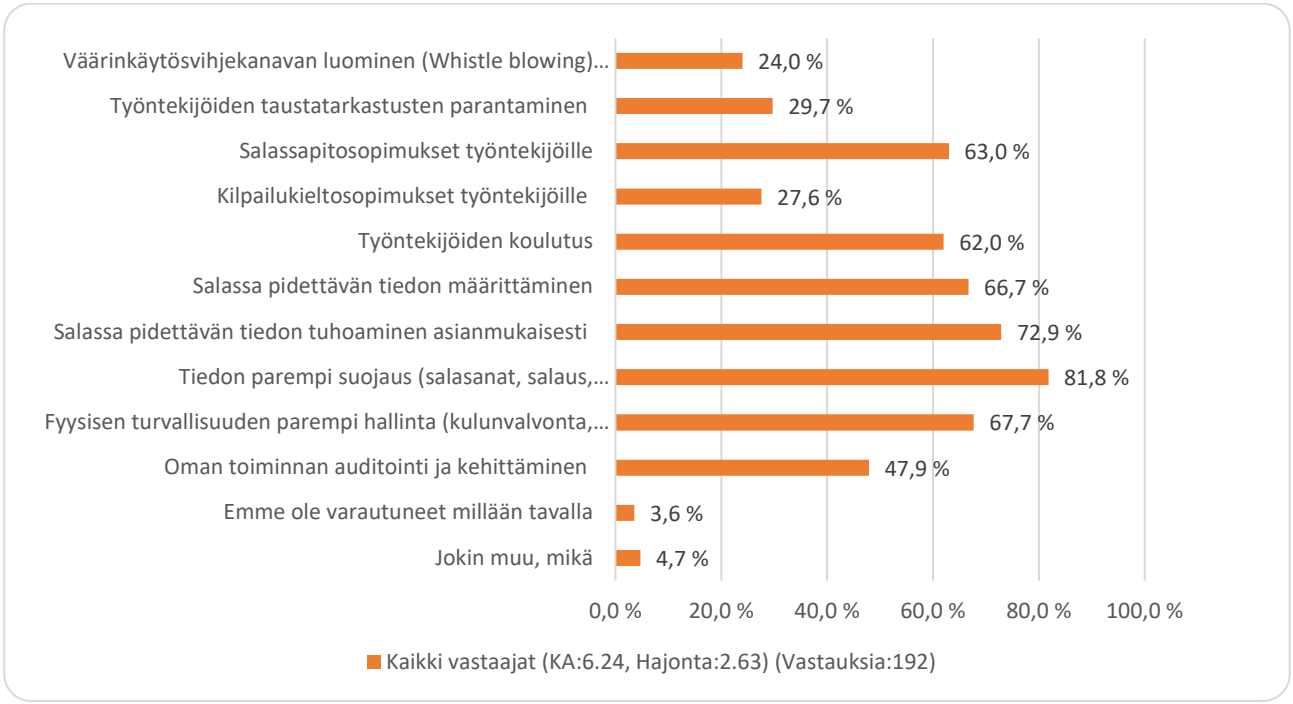
Tehdäänkö yrityksessäsi kybervakoiluun liittyvää riskienhallintaa?



Vastanneista yrityksistä neljäsosa (23 %) teki säännöllistä riskienhallintaa kyberturvallisuuden osalta. Riskienhallintatyö on yleensä edellytys suunnitelmalliselle ja pitkäjänteiselle uhkiin varautumiselle. Satunnaisesti riskienhallintaa harjoitti kaksi viidesosaa (38 %) vastaajista. Huonoin tilanne oli kolmasosalla (32 %) vastaajista, jotka eivät tehneet lainkaan riskien arviointia.

Yritys voi selvitä ilman riskienhallintaakin, mutta sen toteuttaminen helpottaa voimavarojen suuntaamista merkittäviksi riskeiksi havaittuihin asioihin ja sen mukaan voidaan saada paras vastine sijoitetuille resursseille. Ilman säännöllistä riskienhallintaa yrityksen pitää tuntea liikesalaisuutensa, mikä niitä uhkaa ja miten suojata niitä tehokkaasti. Näillä tiedoilla voi jo sellaisenaan päästä riittävälle tasolle tiedon suojaamisessa.

Mitä toimia yrityksesi on tehnyt yritysvakoilun torjumiseksi?



Yleisimmät tavat varautua yritysvakoilun uhkaan ovat:

1. tiedon parempi suojaaminen (salasanat, salaus, pääsyn hallinta, tietoverkkoturvallisuus)
2. salassa pidettävän tiedon asianmukainen hävittäminen tarvittaessa
3. fyysisen turvallisuuden parempi hallinta
4. salassa pidettävän tiedon määrittäminen
5. salassapitositoumukset
6. työntekijöiden koulutus.

Yritysvakoilu on uhka, jonka toteuduttua yrityksen on vaikea rajata vahinkoa. Vakoilun paljastaminen ja tekijöiden kiinnisaaminen on vaikeaa. Myös vahingonkorvauksen saamisen todennäköisyys on häviävän pieni. Suurin osa yritysvakoilusta jää paljastumatta ja se on yksi syy siihen, että jotkut epärehellisesti toimivat yritykset käyttävät sitä parantaakseen omaa kannattavuuttaan. Koska liikesalaisuuksia ja vakoilua koskevat lait ovat erilaiset kaikkialla, ulkomaisten yritysten ja hallitusten saattaminen vastuuseen voi olla hyvin vaikeaa. Ja vaikka tekijä olisi kotimainen, näytön saaminen ja korvausvastuun osoittaminen on vaikeaa.

> ***”Kiinan kaupassa tämä on lähtöoletus teknologiayrityksellä. On sinänsä vaikea vetää selvää rajaa laillisen BI:n ja kilpailija-analyysin ja varsinaisen yritysvakoilun välille.”***

Yritykselle tehokkainta on varautua uhkaan etukäteen, yleensä on myöhäistä reagoida, kun tieto on jo viety. Yritysvakoilun toteuttavat usein sisäpiiriläiset, joilla on jo työtehtävänsä vuoksi pääsy arkaluontoisiin tietoihin. Vakoilutoiminta on vaikeasti erotettavissa normaalista jokapäiväisestä työtehtävän mukaisesta toiminnasta, joten vakoilun sisältävää toimintaa on haastavaa havaita ja vielä vaikeampaa todistaa tuomioistuimessa.

Vastaajayritysten keskuudessa tietoverkon suojaaminen on yleisin tapa varautua, se on luonnollista koska harva yritys ei nykypäivänä toimi digitaalisesti tavalla tai toisella. Julkisuudessa jo vuosien ajan esille nousseet kyberrikostapaukset ovat nostaneet kyberrikosten yleisyyden ammattilaisten ohella myös yritysten yleisempään tietoisuuteen.

On ilahduttavaa, että yritysten keskuudessa huomioidaan myös fyysinen turvallisuus (toimitilat) ja hallinnolliset toimet kuten salassapitositoumukset ja salassa pidettävän tiedon määrittäminen osana yritysvakoilun torjuntaa. Jos tietoa ei ole luokiteltu, yrityksen on vaikea tehokkaasti suojata kriittistä tietoaan. Myöskään kouluttaminen ja salassapitositoumusten käyttö eivät tällöin saavuta sitä tehoa, joka niille on tarkoitettu. Kouluttaminen on tehokkain tapa nostaa yrityksen turvallisuuden tasoa. Ja kääntäen kouluttamaton henkilökunta voi virheellisellä toiminnalla tehdä turvallisuuteen ja turvallisuusjärjestelmiin tehdyt investoinnit hyödyttämiksi ja tehdä yritykselle kalliita virheitä.

Kouluttamisesta

Kouluttaminen kannattaa aloittaa antamalla työntekijöille tietoa yritysvakoilusta uhkana ja ”jututtajien” käyttämistä tekniikoista. Toiseksi koska sosiaalisen median sivustoja käytetään usein yhteydenpitoon tai tiedon keräämiseen yrityksen työntekijöistä, on työntekijöitä hyvä kouluttaa sosiaalisen verkottumisen riskeistä ja turvallisista toimintatavoista, kuten siihen mitä työasioita saa ja mitä ei saa paljastaa sosiaalisten verkostojen sivustoilla.

Toinen keskeinen kouluttamisen osa-alue on toimitilojen turvallisuus. Kun jollakulla on pääsy organisaatiosi tietokoneisiin ja tiloihin, on hyvin todennäköistä, että hän pystyy keräämään tietoja. Varmista, että vieraat saatetaan toimitiloissa. Vieraiden tulee kirjautua sisään ja henkilökunnan edustajan tulee seurata heitä. Työntekijöiden tulisi lukita työpisteet ja tietokoneet, kun niitä ei käytetä, ja organisaation tulisi harkita puhtaan työpöydän käytäntöä. Nämä ovat vain joitain esimerkkejä toimista, jotka voivat suojata toimitilojen turvallisuutta yritysvakoilulta.

Kolmantena työntekijöitä tulee kouluttaa siihen, mikä heidän roolinsa yrityksen kyberturvallisuudessa on ja miten he voivat tukea kyberturvallisuutta. Ennen kyberrikollisuuden julkituloa, harva työntekijä kykeni pelastamaan tai ajamaan työnantajansa pulaan tietokoneensa tai puhelimensa äärestä. Nykyään työntekijät ovat yrityksen rikos- ja kyberturvallisuuden eturintamassa tavalla, jollaista ennen ei ole ollut. Paras tapa estää työntekijöitä vahingossa auttamasta rikollisia on valistaa työntekijöitä. Työntekijöiden tulee olla tietoisia roolistaan ja merkityksestään organisaation turvallisuudessa. Työntekijöille on hyvä kertoa mahdollisista uhista ja siitä mitä tietoa on suojattava ja miten.

Hyvä tapa aloittaa kyberturvallisuuden parantaminen on opettaa työntekijöille yksinkertaisia tietoturvakäytäntöjä arjen työntekoon. Näin työntekijät omaksuvat turvallisen ajattelutavan helpommin voidessaan päivittäin toimia oikein perusasioissa ja tehdä asioita turvallisesti ja oikein. Tästä seuraa tunne, että yksittäinenkin työntekijä voi tehdä osansa ”kasvottoman” yritysvakoilun torjumiseksi. Tällainen koulutus valmentaa henkilökuntaa varautumaan jututtajien ja urkkijoiden yksinkertaisia yrityksiä saada tietoa tai pääsy yrityksen tietoverkkoon.

Yrityksen tietojen suojaamisen aloittaminen

Yrityksen on osattava itse tunnistaa mahdolliset arvokkaimmat kohteet. Yrityksen on selvitettävä asia kerrallaan mitä liikesalaisuuksia ja muuta arvokasta tietoa yrityksellä on ja minkä arvoisia ne ovat. Yksinkertainen ja suuntaa-antava tapa arvioida liikesalaisuuden arvoa on vertaamalla sitä markkinoilla jo oleviin vastaaviin tuotteisiin tai kilpailijoiden julkisiin arvioihin vastaavien tietojen tai prosessien arvosta heidän omalle toiminnalle.

Kun arvokkaimmat tiedot on tunnistettu, voi seuraavaksi miettiä mitkä tunnistettavat tahot voisivat haluta niitä tai hyötyä niistä. Tällä tavalla voi arvioida mahdolliset uhat liikesalaisuuksille ja mahdollisesti myös oletetut tavat yritysvakoilulle. Tämän jälkeen on helpompi pohtia mitä haavoittuvuuksia omassa suojautumisessa mahdollisesti on.

Vastausvaihtoehto ”Muu, mikä?” keräsi seuraavanlaisia vastauksia:

- kyberturvallisuuskoulutus
- phishing -koulutus
- avainhenkilöiden turvallisuuskartoitus ja vaaditut toimenpiteet
- ulkoiset auditoinnit ja tarkastukset
- salassapitosopimukset myös kumppaneille
- toimialalla jo lainsäädäntö asettaa tiukat vaatimukset salassapidolle
- ulkopuolinen yritys auttaa tietoturvassa.

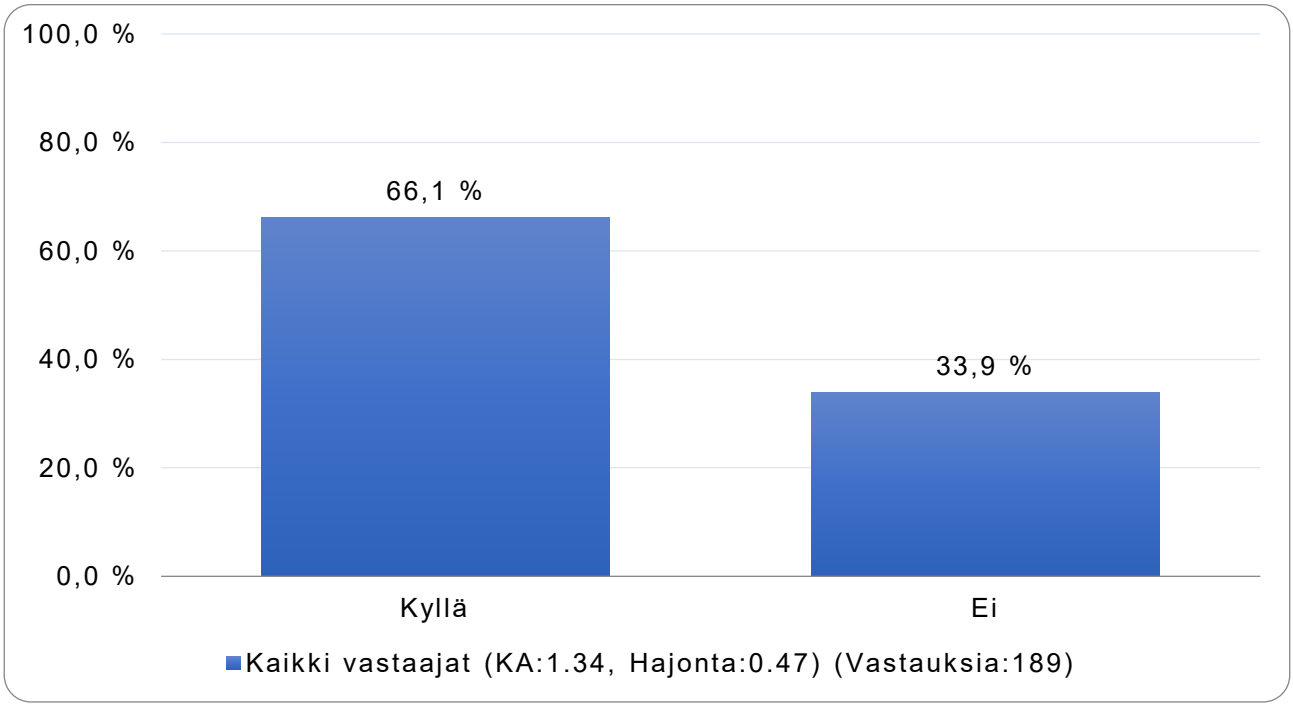
5 ETÄTYÖ JA TIEDON SUOJAAMINEN

Kun digitalisaatio etenee, yritysten on yhä vaikeampaa valvoa aineettoman omaisuuden ja liikesalaisuuksien laitonta siirtoa pois yrityksestä. Vuosien tutkimus- ja kehitystyö, tekniset kaaviot ja muut liikesalaisuudet voivat livahtaa pilveen muutamassa sekunnissa tai ne voidaan ladata nopeasti muistitikkuun ja sujauttaa se taskuun. Etätyö on korostanut tietoon pääsyn rajaamisen ja kouluttamisen merkitystä yrityksen tietoturvallisuudelle. Rajoittamalla kriittisiin tietoihin pääsevien ihmisten määrää pienennetään osaltaan sitä riskiä, että kilpailija tai joku muu kolmas taho saa nämä tiedot haltuunsa.

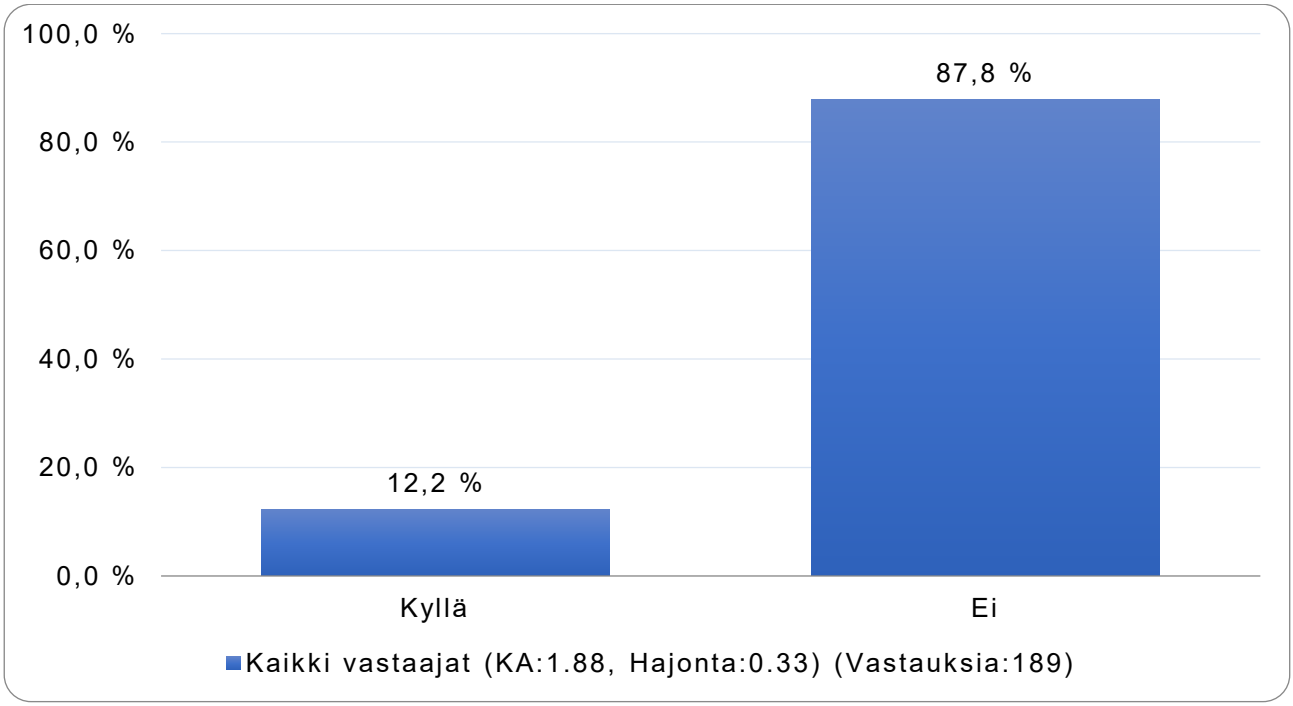
Jotkut työnantajat tarjoavat työntekijöille oletuksena pääsyn kriittisiin tietoihin. Se voi olla helppo tapa toimia, mutta se ei ole turvallinen tapa toimia. Yrityksen tulisi noudattaa ”vähäisimpien oikeuksien periaatetta” ja estää työntekijän pääsy kaikkiin niihin tietoihin, joihin se ei ole tarpeen. Mitä vähäisempään määrään tietoja pääsee käsiksi jättämättä normaalista työnteosta jääviä jälkiä, sitä pienemmän vahingon voi aiheuttaa. Tieto jälkien jäämisestä voi toimia myös ennalta estävänä tekijänä. Tämä ”vähäisimpien oikeuksien periaate” on työläämpi vaihtoehto, mutta turvallisempi.

Niin sanotun "tarve tietää" -periaatteen soveltaminen tarkoittaa, että pääsy liikesalaisuuksiin annetaan vain niille työntekijöille, jotka todella tarvitsevat kyseistä tietoa. Jos yksittäisten työntekijöiden on toisinaan työskenneltävä luottamuksellisten tietojen kanssa, he voivat tehdä sen esimerkiksi valtuutetun henkilöstön valvonnassa ja tilapäisellä oikeudella, jonka jälkeen työntekijän haltuun päätyneiden tietokopioiden hävittäminen tulee varmistaa.

Onko työntekijöitä erikseen ohjeistettu suojaamaan yrityksen tietoa etätyössä?



Onko yrityksessänne yrityssalainen tieto vaarantunut työntekijöiden etätyöskentelyn seurauksena?



Etätyö on korona-aikana lisääntynyt huomattavasti, mutta siitä huolimatta kolmasosa (34 %) vastaajayrityksistä ei ole erikseen ohjeistanut työntekijöitä tiedonsuojaamisessa etätyössä. Ja joka kymmenennen (12 %) vastaajayrityksen yrityssalainen tieto on vaarantunut etätyöskentelyn seurauksena.

Etätyön yleistyminen ei ole vähentänyt tietoon kohdistuvaa uhkaa, ja samalla on kasvanut tarve kouluttaa tietoturvaa työntekijöille. Etätyöskentelevät työntekijät ovat tietyllä tapaa omillaan ja tietoturvallisuuteen liittyen virheiden tekeminen on helpompaa ja ne jäävät helposti ilmoittamatta. Siksi yritysten pitäisi kehittää tietoturvan koulutusta ja paneutua siihen, miten etätyöntekijät saadaan pidettyä valppaina erilaisten tietoon kohdistuvien rikosten osalta.

6 YRITYSVAKOILUTAPAUKSET JA SEURAUKSET

Yritysvakoilu on tiivistettynä toimintaa, jossa laittomin tarkoituksin pyritään saamaan haltuun jonkin yrityksen liikesalaisuuksia. Keinoina voidaan käyttää suoraan laittomaksi tunnistettavia keinoja, kuten tilojen salakuuntelu, sähköpostiviestin sieppaaminen tai murtautuminen yrityksen tietojärjestelmiin.

Vakoilija voi käyttää myös keinoja, jotka eivät ole suoraan tunnistettavissa laittomiksi teoiksi. Tällaisia voivat olla työntekijöiden jututtaminen kasvokkain messuilla tai muussa vastaavassa luonnollisessa ympäristössä. Tai toiminta, jota värvätty työntekijä tekee ja joka käytännössä näyttää sivullisen silmiin normaalilta, työntekoon liittyvän tiedon käsittelemiseltä.

Vakoilija voi käyttää peiteroolia ja esiintyä esimerkiksi toimittajana, head hunterina tai potentiaalisena palveluntarjoajana ja pyrkiä tässä yhteydessä keräämää vakoilussa hyödynnettävää tietoa joko suoraan siitä mitä halutaan tietää tai sitten tietoa luottamukselliseen tietoon pääsevien henkilöiden henkilökohtaisista oloista ja heikkouksista, joita voidaan sitten käyttää hyväksi värvättäessä tai hyödynnettäessä tällaista henkilöä.

Suuri osa yritysvakoilusta voi tapahtua yksinkertaisesti ”sisäpiiriläisenä”, joka luovuttaa keräämiään liikesalaisuuksia yrityksestä toiseen - esimerkiksi palkkaansa tai uraansa tyytymätön työntekijä tai työntekijä, jonka kilpailija on värvännyt ja joka viimeistään työpaikka vaihtaessaan ottaa mukaansa tietoja, joihin hänellä ei ole ollut pääsy- tai käyttöoikeutta. Teon toteennäyttäminen on huomattavasti helpompaa kuin vaikka kybervakoilun, edellyttäen että yrityksen turvallisuustoimet ovat sillä tasolla että jälkiä teosta on helppo saada. Myös se, että työntekijä usein siirtyy kotimaassa toimivalle kilpailijalle, mahdollistaa sen että entinen työnantaja tunnistaa tai saa kuulla liikesalaisuuksiaan käytetyn uuden työnantajan hyväksi laittomalla tavalla.

“Vakoilu paljastui kilpailijoiden tuotejulkistuksen myötä.”

Kilpailija tai ulkomainen hallitus voi haluta kohdeyrityksen tietoja omien teknologisten tai taloudellisten etujensa edistämiseksi ja käyttää siihen erilaisia vakoilutapoja. Joskus valtiollinen tai kilpailija palkkaavat mieluummin kolmansia henkilöitä vakoilijoiksi kuin käyttävät ”omia” vakoilijoitaan. Hallitusten esimerkiksi uskotaan usein käyttävän akateemisia henkilöitä, liike-elämän edustajia ja opiskelijoita tiedon keräämisessä. Joidenkin maiden on raportoitu järjestelmällisesti haastattelevan opiskelijoita kotiin palaamisen jälkeen. Toisinaan hallitustenkin edustajat saattavat käyttää rikollisia välikäsinään.

Tietyllä tapaa yrityksen ei siis kannata aluksi keskittyä liikaa erilaisiin tapoihin vakoilla, vaan yrityksen olisi tärkeämpää ensin tunnistaa liikesalaisuutensa ja muu toiminnan kannalta kriittinen tieto tai tieto, jota kannattaa salata. Näiden tietojen suojaamiseen keskittymällä yritys voi pyrkiä estämään tai vaikeuttamaan yritysvakoilun kohteeksi joutumista ja sen toteuttamista.

Tämän luvun lopussa on lista yritysten avoimista vastauksista.

Keskeiset havainnot epäillyistä yritysvakoilutapauksista ja niihin liittyvistä seikoista.

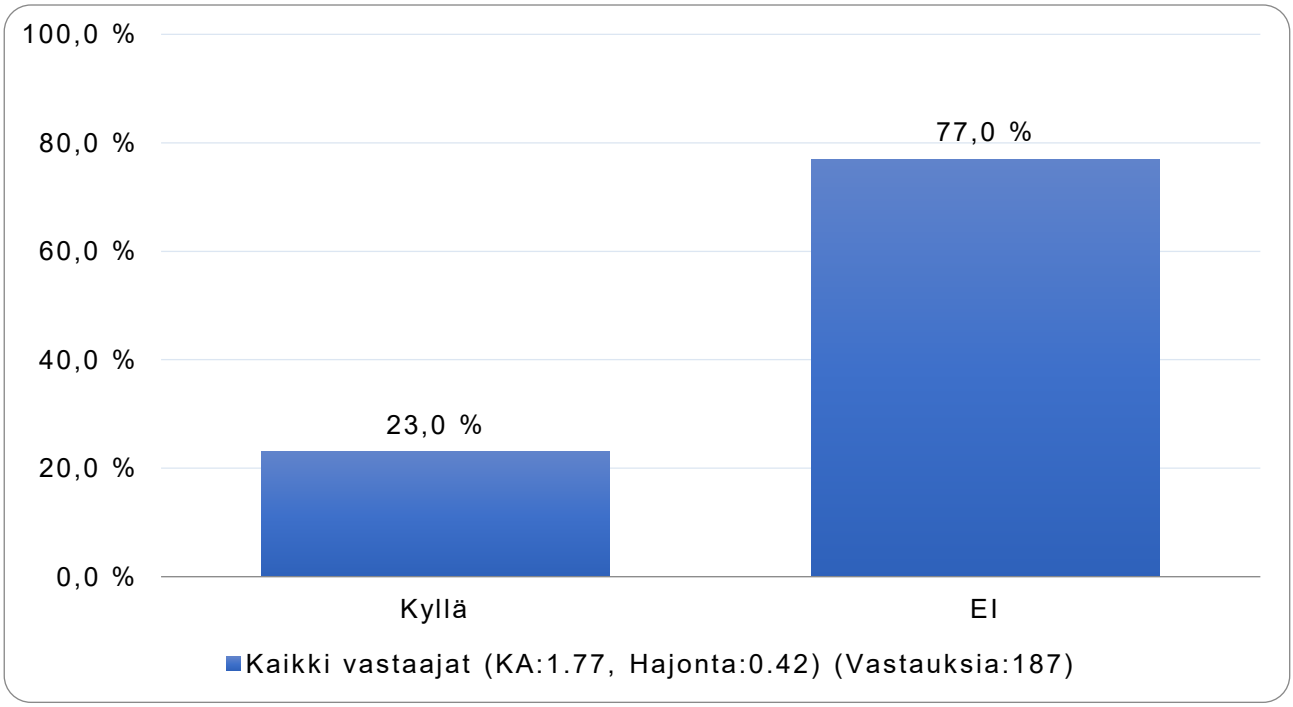
1. Joka neljäs (23 %) vastaajayritys on **epäillyt siihen kohdistuneen yritysvakoilua.**
2. Paljastuneista tekijätahoista **kaksi kolmasosaa (64 %) oli ulkomaalaisia** ja yksi kolmasosa (36%) kotimaisia tahoja.
3. **Yli puolesta tapauksia (53 %) ei tehty minkäänlaista ilmoitusta viranomaisille**. Neljäsosassa (24%) tehtiin rikosilmoitus ja viidesosassa (22 %) kerrottiin muutoin viranomaisille epäilystä.
4. Yrityksen kärsimää vahinkoa arvioitiin seuraavasti:
    a. 52 %:ssa tapauksista vahinko oli 0-100 000 euroa
    b. 27 %:ssa vahinko oli 100 001-1 000 000 euroa
    c. 12 %:ssa vahinko oli 1 000 001-10 000 000 euroa
    d. 9 %:ssa vahinko oli yli 10 000 000 euroa.

5. Vastaajayrityksistä 15 prosenttia oli huomannut kilpailijan tuoneen markkinoille vastaavan tuotteen juuri ennen oman tuotteensa lanseerausta markkinoille.

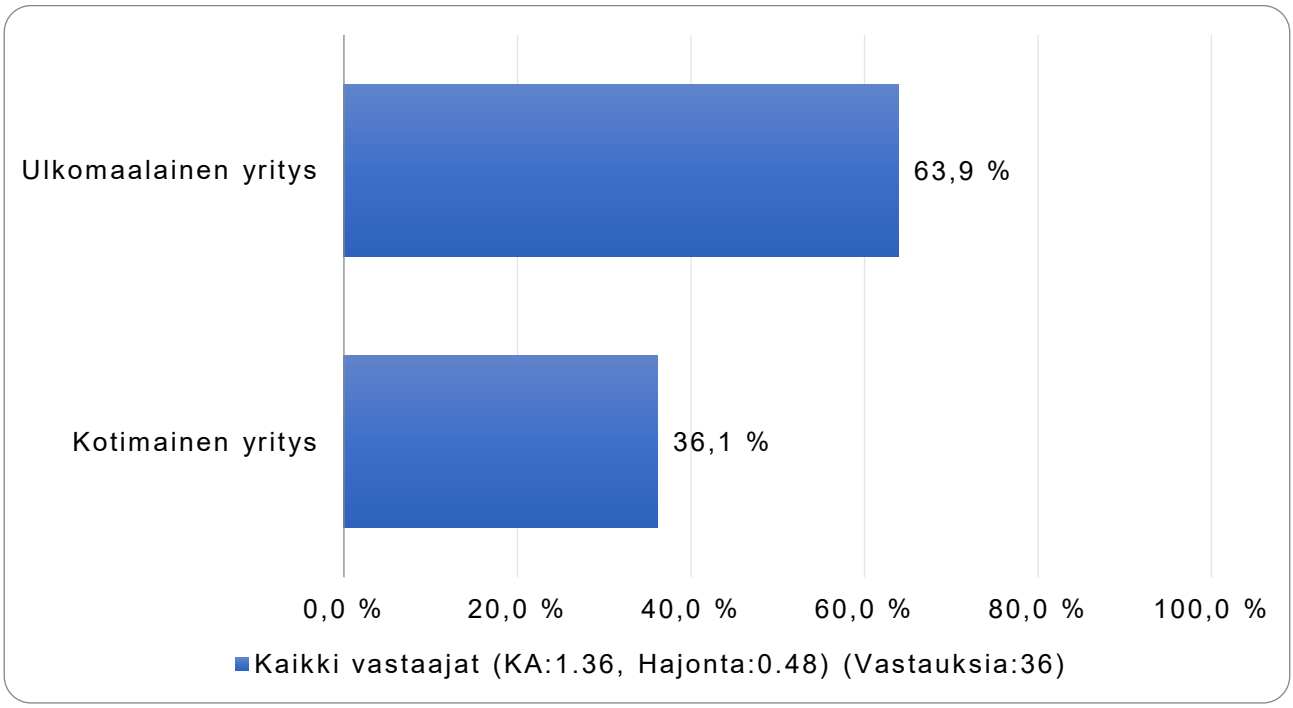
Kun arvioidaan aiheutuneen taloudellisen vahingon suuruutta, kannattaa pitää mielessä, että jokainen menetetty euro katetaan kate-euroilla. Jos kate on 10 prosenttia, on vahingon kattamiseen tarvittava työmäärä eli liikevaihto kymmenen kertaa katteen suuruinen. Tämän jälkeen on muistettava arvioida edellä mainitun vahingon aiheuttaneen vajeen kattamiseen kulunut kate. Jotta yritys saa aiheutuneen vahingon nollattua ja ansaittua sen, mitä se olisi ilman vahinkoa ansainnut, on kyseessä kymmeniä kertoja vahinkoa

suuremmasta liikavaihdosta ja ajallisesti pitkästä kannattavan liiketoiminnan ajanjaksosta. Tämänkin vuoksi tietoja kannattaa suojata etukäteen eikä pyrkiä saamaan vahingonkorvausta ja ehkä tuomiota rikolliselle. Estäminen kannattaa huomattavasti paremmin kuin tapahtuneen rikoksen selvittely ja oikeudenkäynti ja menetetyt kaupantekomahdollisuudet.

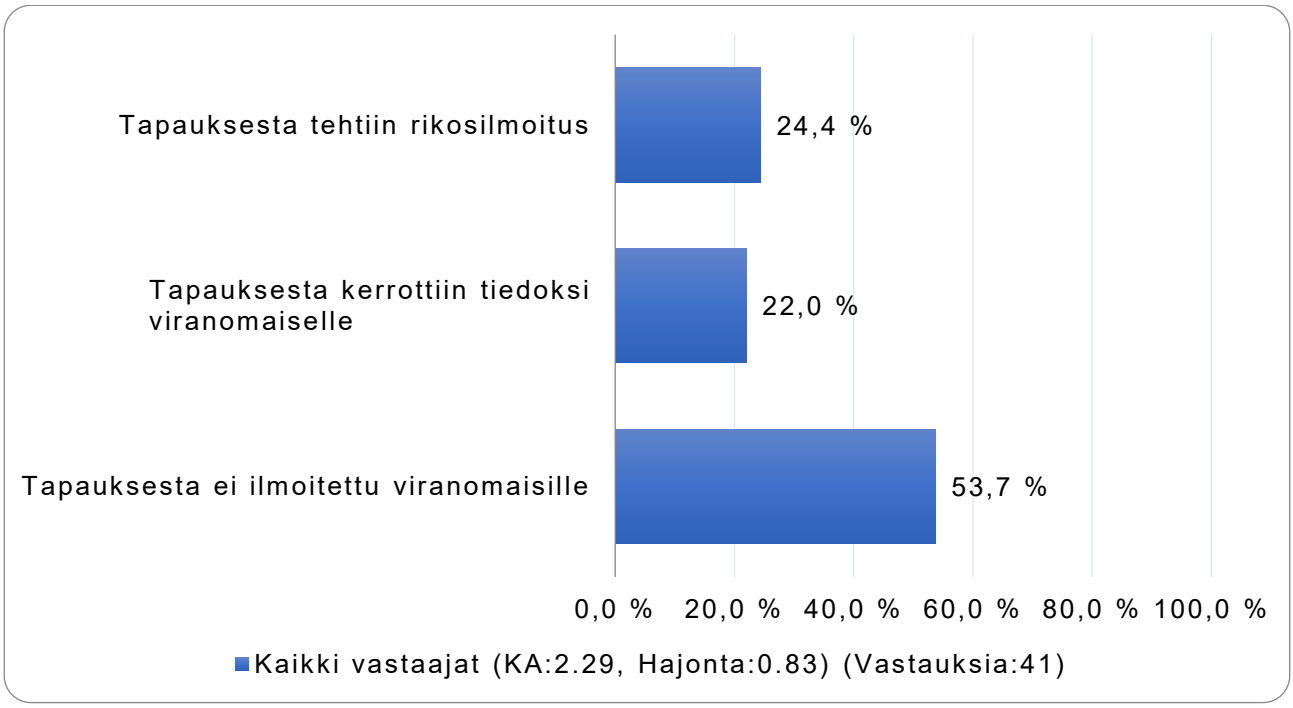
Onko nykyinen yrityksesi / työnantajasi tai jokin aiempi työnantajasi ollut epäillyn yritysvakoilun kohteena?



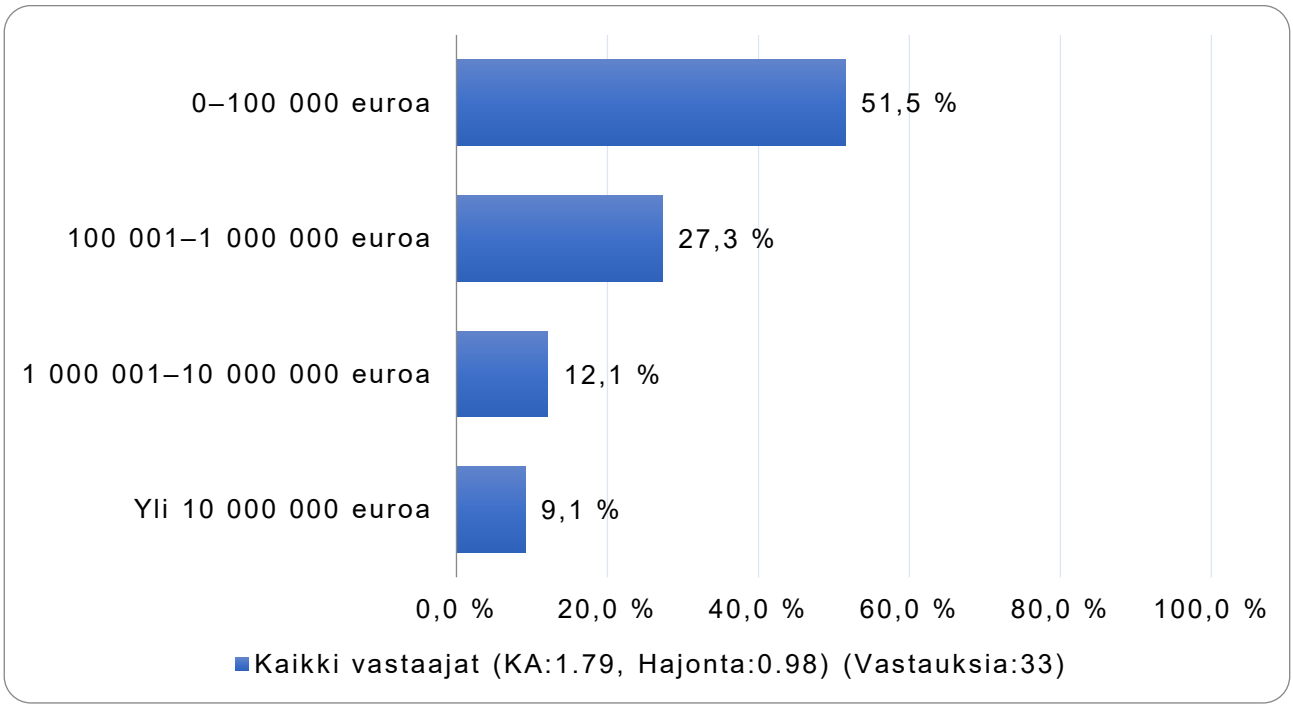
Jos teon toimeksiantaja / hyötyjä selvisi, oliko kyseessä:



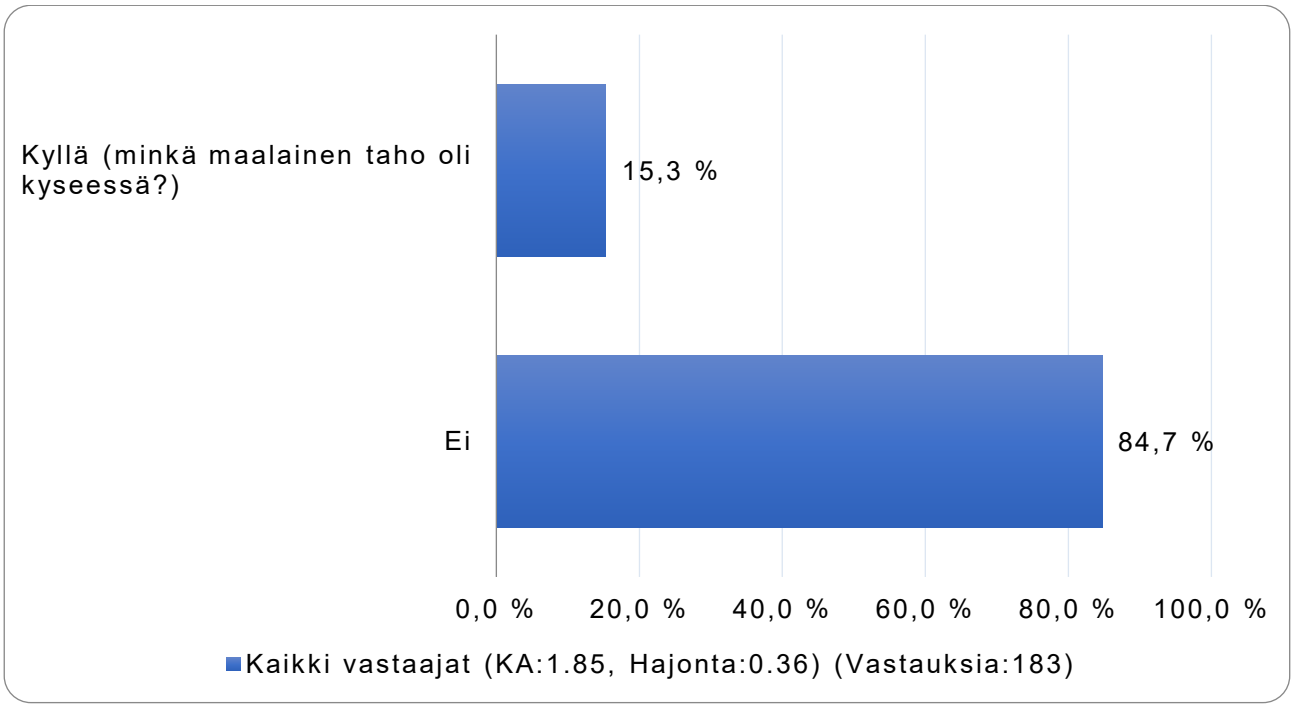
Ilmoititteko yritysvakoilutapauksen viranomaisille?



Anna arvio yrityksesi kärsimän vahingon suuruudesta.



Oletteko joskus havainneet, että kilpaileva yritys tai muu taho on julkistanut tuotteen, joka vastaa yrityksen kehitysvaiheen loppusuoralla olevaa tuotetta tai palvelua?



Minkämaalainen taho oli julkistanut tuotteen, joka vastaa yrityksen kehitysvaiheen loppusuoralla olevaa tuotetta tai palvelua?

Kysymys keräsi seuraavanlaisia vastauksia:

- suomalainen (6)
- kiinalainen (6)
- yhdysvaltalainen (3)
- liettualainen (2)
- saksalainen (2)
- englantilainen (2)
- korealainen
- ruotsalainen
- hollantilainen
- latvialainen
- virolainen

Vastauksista käy ilmi, että kuvitelma suomalaisten toimijoiden rehellisyydestä on osin pelkkää sanahelinää. Vakoilijoita on niin idästä kuin lännestäkin ja se vahvistaa näkemystä siitä, että suomalaisen yrityksen tieto houkuttelee kansainvälisesti. Siksi tietoa on suojattava jokaiseen ilmansuuntaan nähden.

Miten epäilty yritysvakoilu tai -tapaukset tunnistettiin tai havaittiin?

- Ei voi kertoa.
- Ilmaantui täsmälleen samanlainen tuote kuin meillä.
- Yksityiskohtia ei kerrota ns. tavallisille työntekijöille.
- Näitä ollut lukuisia, mm väärentämällä yrityksen rahoitusdokumentit, jotka vuotivat sijoittajien kautta kyselyinä takaisin meille, asiasta on jopa tuomittu kotimainen väärentäjä petoksesta oikeusteitse, jotkut keissit ovat paljastuneet muuten, ulkomaisia ei ole saatu oikeusteitse vastuuseen!
- Omat selvitykset.
- Meitä lähestyttiin tarjouspyynnöllä, joka osoittautui harhaanjohtavaksi. Kilpailutuksessa kerättiin tietoa yrityksestäni entiselle työnantajalleni, eikä kyse ollut aidosta kilpailutuksesta.
- Kilpailijoiden tuotejulkistukset.
- Saatiin tieto asiakkaalta, että entinen työntekijä oli ollut yhteydessä ja tarjonnut "hyvin samankaltaista" palvelua kuin mitä jo hankkivat meiltä.
- Työntekijät kopioineet materiaalia pois lähtiessään.
- Tieto havaittiin tiedon siirtymisenä.
  Minulle tieto tuli KRP:n kautta (yritys ei tiedottanut).
- Sähköposti hakkeroitiin, ei välttämättä suoraa yritysvakoilua mutta haittaa oli, koska viestintää häirittiin ja saatiin virheellisesti maksetun laskun kautta myös rahallista hyötyä. Havaitsin itse, kun viestit eivät kulkeneet, IT toimittaja ei havahtunut mitenkään ennen omia toimia.
- Kiinalainen yritys ei maksa sopimuksen mukaisia vuosittaisia lisenssimaksuja materiaalin käyttöoikeudesta. Kuitenkin he käyttävät saamaansa materiaalia.
- Sähköposti ja sosiaalisen median kyselyitä, joissa kyselijää ei voitu yhdistää todelliseen henkilöön.
- Kyberhyökkäys, kiristysviestit.
- Sama identtinen malli tuli markkinoille kahden vuoden kuluttua. Samalla aikaisemmat yhteistyökumppanit siirtyivät tämän yhtiön palvelukseen.
- Oman turvallisuusorganisaation toimesta.
- Sähköposti kaapattiin.
- Admin-tunnuksien käyttö väärässä yhteydessä. Tämä ei kuitenkaan onnistunut.
- Oma havainto, viranomaisen yhteydenotto.
- Työntekijä epäili yhteydenoton asiallisuutta ja keskusteli asiasta turvallisuudesta vastaavan kanssa.
- Tuotteen ulkonäöstä.
- Omien selvitysten kautta vuosien mittaan. Aluksi asiakirjat salattiin ja osa tuhottiin.
- Outo saapunut telefax herätti epäilykset (hinnoittelutietoja).
- Urkintapuheluita työntekijöiden yhteystietoihin liittyen. Kyberturvallisuuden puolella havaittuja hyökkäysyrityksiä.
- Kilpailijoiden patenttihakemuksista.
- Omavalvonnan sekä viranomaisyhteistyön tuloksena.
- Syntyi epäily liittyen hinnoitteluun.
- Lokitiedoista.
- Aika ilmeistä tiedonkalastusta, myös penetroitumisyrityksiä verkon kautta.

- Käsittämättömän pitkät roikkumiset netissämme. Markkinoille tuodut kopiot.
- Asioista kysyminen oli erittäinen läpinäkyvää (harjoitellut kysymykset etukäteen).
- Epäily heräsi epätavallisesta yhteydenotosta sosiaalisessa mediassa.
- Kiinan kaupassa tämä on lähtöoletus teknologiayrityksellä. On sinänsä vaikea vetää selvää rajaa laillisen BI:n ja kilpailija-analyysin ja varsinaisen yritysvakoilun välille.
- Toinen tapaus sisäisessä tutkimuksessa joka liittyi tiedon tekniseen valvontaan, ja huomattiin että sitä käytettiin kummallisesti. Toisessa tapauksessa viranomainen otti yhteyttä.
- Kun kilpaileva tuote ilmestyi nettikauppaan. Muutamaa kuukautta aikaisemmin ko. lautapelin hahmofiguurien muotit olivat kadonneet Kiinan postissa.
- Työntekijä ilmoitti kalastelun yrityksestä.

Millaiseen tietoon yritysvakoilu kohdistui?

- yritystietoon
- tuotteen tekniikkaan
- ipr sekä yrityksen rahoitus
- tietotekniikkaan
- yritykseni tarjouslaadintaprosessiin, tarjousdokumentteihin, hinnoitteluun yms.
- ohjelmistospeksi
- tuotesisältöihin-, hintoihin ja toimitustapoihin.
- asiakkuudet (lista), tuotantomenetelmät, asiakirjamallit
- henkilötietoihin
- ainutlaatuinen koulutusmateriaali.
- tuotekehitykseen
- teollisuutta palveleva ohjelmisto.
- yhteystietoihin
- prototyyppi
- kaikkeen tietoon
- arkaluontoiseen tietoon maanalaisista tiloista kaupungissa.
- suunnitteludokumentteihin
- asiakastiedot, hinnoittelu, tarjoukset- - -
- tietyissä tehtävissä olevien työntekijöiden yhteystietoihin.
  kyberpuoleen en osaa ottaa kantaa
- varhaisen vaiheen tuotekehitystietoon
- hintatiedot
- kehitettyyn ohjelmistoon
- ipr:iin
- valmistusmenetelmiin
- olemassaolevien asiakkaiden nimien saaminen
- tuotteen ominaisuuksien yksityiskohtiin
- tuotantoteknisiin ratkaisuihin
- tuotekehitykseen
- lautapelin rakenne
- henkilön sähköpostiin.

Onko muutoin tiedossasi epäiltyä yritysvakoilutapausta, millainen se oli?

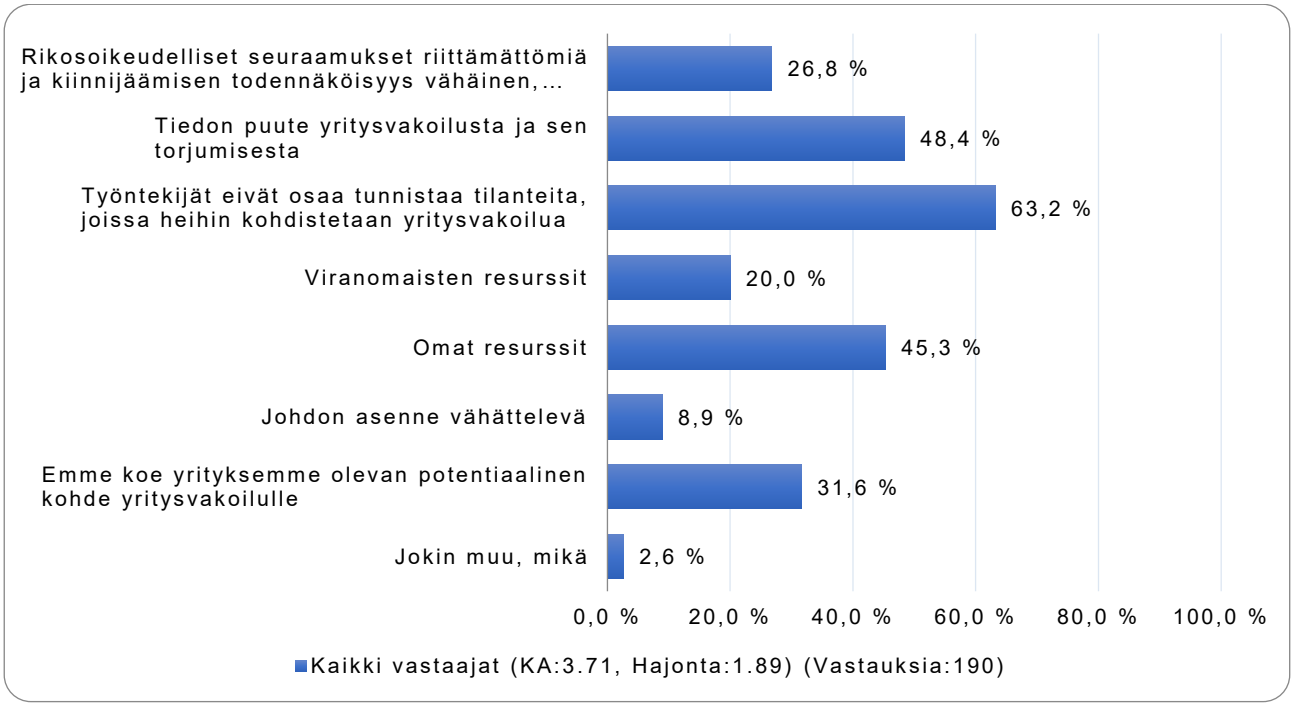
- Kilpailijalle siirtyneet entiset työntekijät ovat vieneet tietoa mukanaan.
- Lähinnä kokemusta on toisten valtioiden kiinteistö/maakauppaostoista strategisesti tärkeiden alueiden lähettyviltä. Venäjän toiminta on tiedostettu, mutta Kiinaa ei niinkään.
- Keskustelua työntekijän kanssa ja jutustelua toimintatavoista.
- Työsuhteeseen valittuja henkilöitä, jonka taustat ja koulutushistoria koettiin tarkemman tarkastelun perusteella epäselviksi. Pyrkivät oikeiden työtehtäviensä sijasta verkostoitumaan silmiinpistävän tehokkaasti eri asiakkaiden päättäjien ja avainhenkilöstön kanssa, usein ilman työnantajan valtuutusta tai omiin työtehtäviin liittyvää tarvetta. Työtehtäviin liittyvissä asioissa esim. ulkoisten asiakkaiden kanssa, työote oli "tiedusteleva" jolloin pyynnöt usein ylittivät normaaleissa työtehtävissä tarvittavat tarpeet.
- Eräs myyjähenkilö perusti oman yrityksen ja latasi tietoja entisen työnantajansa tunnuksilla. asiakasrekisterin ja muita mahdollisia tietoja käyttöönsä.
- On. Liittynyt tuotekopiointeihin ja näiden kaupalliseen hyödyntämiseen.
- Ei muuta kun mitä on julkisen median kautta kuullut tapauksia.

- Yrityksiä ujuttautua yrityksen liiketoiminnan ostajaksi ja tarkoitus vakoilla yrityssalaista tietoa.
- Ei laitonta, mutta yhteistyötä ehdotetaan ja kuitenkin vaikutta siltä, että halutaan tietää vain tehtyjä ratkaisuja.
  Ei itselle, mutta sekä Helsingin Keksijöiden että Keksijöiden Keskusliiton koneisiin murtauduttiin useampia kertoja, kun ne olivat WordPress alustalla. Kun siirryttiin Microsoftin pilvipalveluihin, murtautumisia ei ole ollut (havaittu).
- Kyberhyökkäys.
- Tietoliikenteen yllättävä ja nopea hidastuminen.
- Valtion kehittämisorganisaation siivooja oli työntekijän tuttu ja penkoi iltaisin tämän ohjeiden perusteella toimiston lukitsemattomat arkistot roskakoreista alkaen.
- Vastaamo (2020).
  Puolustusvoimien tietovuoto (2018, Hesari).
- Työntekijää lähestytty tiedon urkintamielessä.
- Aikaisemmassa työsuhteessa eräs työntekijä vei mukanaan asiakastietokannan.
- Aina ne ovat menetelmiemme ja tulevien mallien kopiointiyrityksiä.
- Tarjouskilpailujen urkkiminen.
- Vastakkaista sukupuolta edustava, kiinalainen nuori nainen yrittänyt hakeutua useita kertoja seuraan uskonnollisen yhdyskunnan tilaisuuksissa.

7 YRITYSVAKOILUN TORJUNNAN ESTEET JA MILLAISTA TUKEA YRITYKSET TARVISEVAT

Tämän luvun lopussa on vastauksia avoimiin kysymyksiin.

Mitkä ovat suurimmat esteet yritysvakoilun torjunnan kehittämiselle yrityksessäsi?



Yleisimmät esteet yritysvakoilun torjunnan kehittämiselle ovat:

1. työntekijät eivät tunnista tilanteita, joissa heihin kohdistetaan yritysvakoilua
2. tiedon puute yritysvakoilusta ja sen torjunnasta
3. omat resurssit
4. yritys ei koe olevansa potentiaalin kohde yritysvakoilulle
5. rikosoikeudelliset seuraukset riittämättömiä ja kiinnijäämisen todennäköisyys pieni.

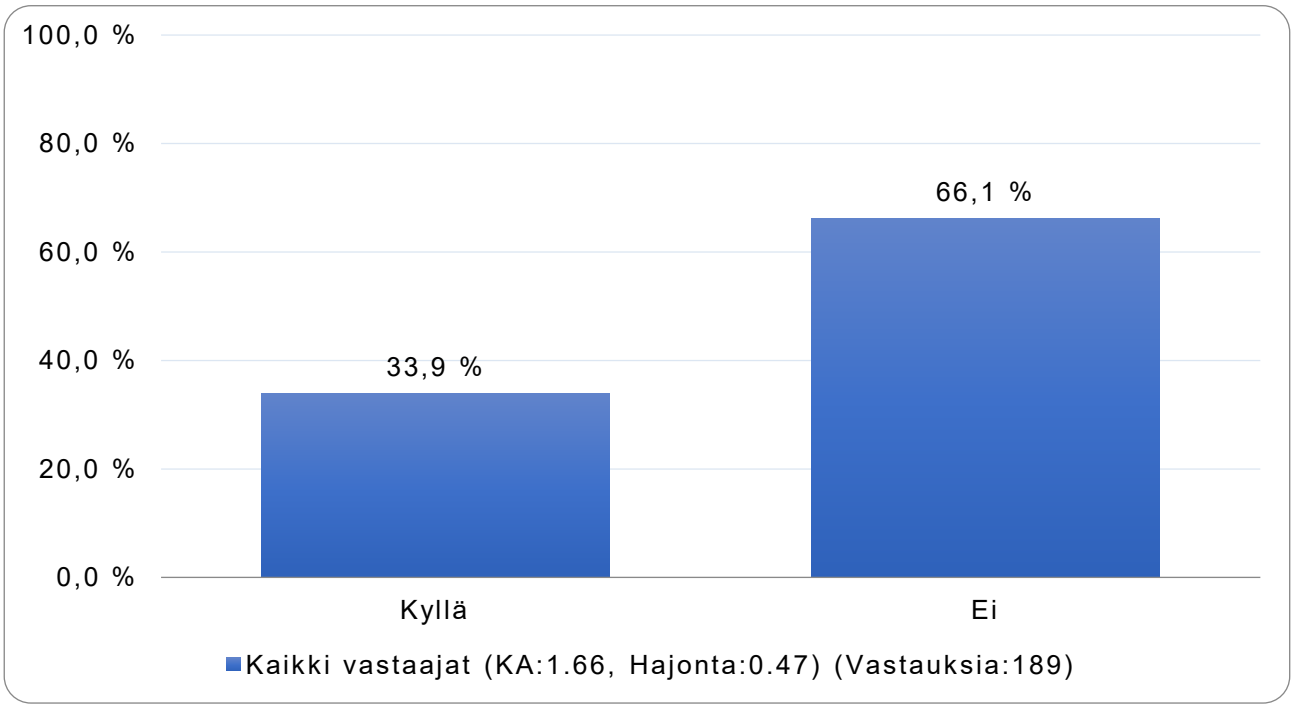
Kuten muissakin kauppakamarin yritysturvallisuuteen liittyvissä selvityksissä on käynyt ilmi, yritykset tarvitsevat tietoa niihin kohdistuvista uhista ja siitä miten suojautua niitä vastaan. Nämä ovat juuri niitä syitä, miksi tämä selvitys on laadittu. Tarvitaan yritysten käytettävissä olevaa tietoa ja avointa keskustelua yritysten tietoon kohdistuvista uhista.

Tahallisten tekojen lisäksi liikesalaisuuksia voi päätyä vääriin käsiin, vaikka työntekijällä ei olisi pahoja aikomuksia. Joskus he eivät ymmärrä antaneensa tietoa väärille henkilöille, toisinaan taas he eivät ymmärrä, että kyseessä oli tieto, jota ei olisi saanut antaa. Työntekijä saattaa vain auttaa opiskelijaa lopputyössään tai johtajatason henkilö saattaa vastata kyselyyn, jossa kysytään asioita, joihin ei pitäisi vastata. Messujen iltatilaisuuksissa ja muissa edustustilaisuuksissa vietetään aikaa ravintoloissa ja alkoholi vaikuttaa ihmisten varovaisuuteen ja tarkkaavaisuuteen. Näihin tapauksiin voi auttaa henkilöstön koulutus. Vakoilussa yritetään usein löytää yksilön heikkoudet ja käyttää niitä hyväksi. Ja vakoilijat tietävät miten jututtaa ihmistä ja saada tämä paljastamaan haluttu tieto. Tällaiseen toimintaan tehoaa kouluttamisen kautta kehitetty valmius tunnistaa tilanne ja tieto siitä miten toimia tilanteessa.

Vastausvaihtoehto ”Muu, mikä?” keräsi seuraavanlaisia vastauksia:

- teknisen osaamisen rajoittuneisuus, vaikeus arvioida it-palveluntuottajien luotettavuutta ja osaamista
- ei tunneta tietoteknisiä mahdollisuuksia varautua/estää yritysvakoilua
- vaikka työntekijöitä ajoittain koulutetaan esimerkiksi tietojen urkintaan liittyen, tätä puolta voisi vielä vahvistaa ja nimenomaan ulkopuolisen, asiantuntevan tahon avulla
- hidas tuomioistuinkäsittely, joka imee yritykseltä valtavasti resurssia.

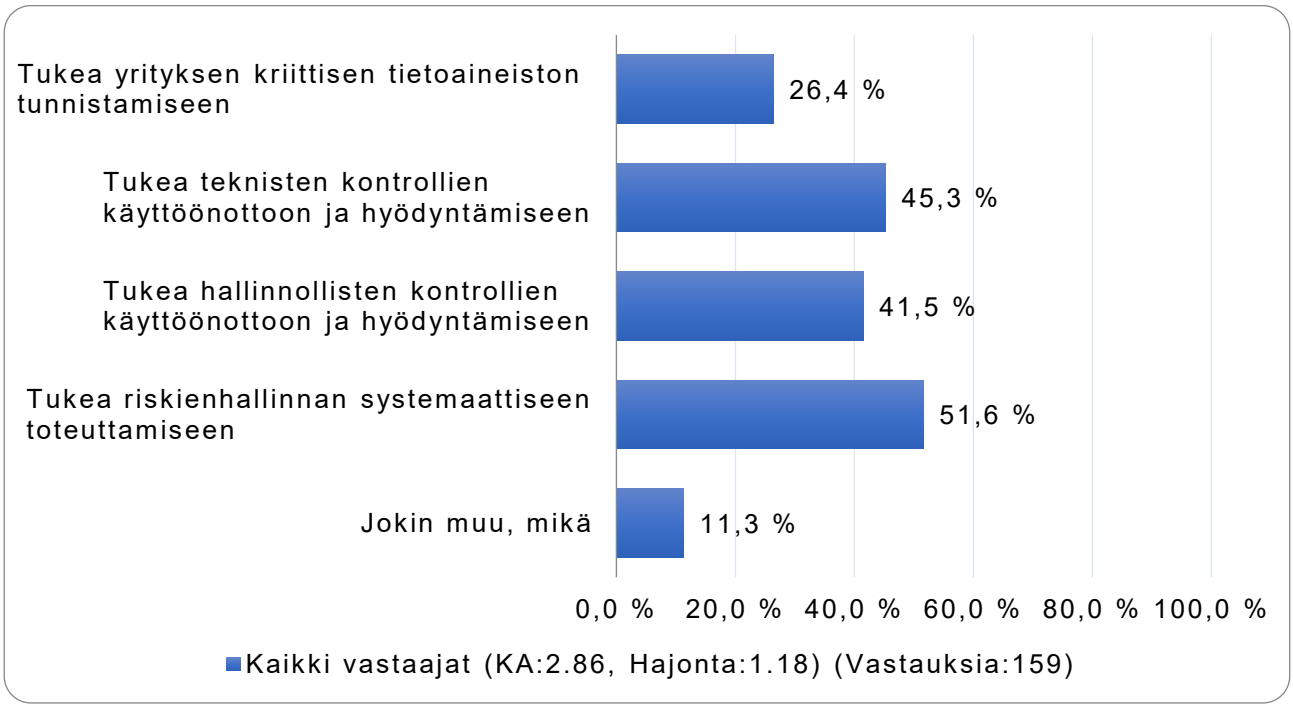
Onko jokin viranomainen toimittanut yrityksellesi tai alallesi tietoa tai ohjeita yritysvakoilun vaaroista ja riskeistä tai antanut apua sen torjunnassa?



Kolmasosa (34 %) vastanneista yrityksistä on saanut neuvoja tai ohjeita viranomaisilta. Huomattavasti useammat yritykset tarvitsevat tietoa yritysvakoilusta ja sen torjumisesta. Kyse on kansantalouteen kohdistuvasta uhasta ja tietoa ei ole keskitetysti saatavilla. Monessa maassa viranomaiset jakavat neuvoja ja ohjeita yrityksille jo sen takia, että viranomaisilla on usein paras käsitys vakoilun yleisyydestä ja siitä mitkä elinkeinoelämän alat ovat alttiimpia vakoilun kohteeksi joutumiselle.

On kuitenkin paljon yrityksiä, jotka ovat potentiaalisia kohteita ja joita viranomaisten ponnistelut eivät tavoita. Viranomaisten ja elinkeinoelämän järjestöjen tulisi tehdä enemmän julkista materiaalia ja pitää aihetta julkisuudessa, jotta tietoa tarvitsevat yritykset aina start upeista jo vakiintuneesti toimiviin yrityksiin saisivat helposti perustietoa ja tiedon siitä, mistä saa lisää tietoa ja apua yritysvakoilun torjuntaan. Yritysten ei tällä hetkellä ole helppoa saada tätä tietoa ja siksi tiedonjakamiseen olisi panostettava aiempaa enemmän.

Minkälaista tukea yrityksesi kaipaisi kybervakoilun havaitsemiseksi ja torjumiseksi?



Kyberrikollisuus kohdistuu kaikenkokoisiin yrityksiin. Kybervakoilu on yksi näistä rikoksista. Kybervakoilun käynnistäminen on nopeaa, helppoa ja kiinnijäämisriski on minimaalinen. Kybervakoilua voi toteuttaa mistä päin maailmaa tahansa, eikä tekijän tarvitse olla fyysisesti lähellä kohdeyritystä tai sen tiloissa. Siksi kybervakoilu on uhka, johon on panostettava ja se pitää tuoda yritysten tietoisuuteen.

Yli puolet (52 %) vastaajayrityksistä tarvitsee tukea riskienhallinnan systemaattiseen toteuttamiseen. Riskienhallinta on järkevä tapa havaita yritykseen kohdistuvat kyberriskit ja tehdä suunnitelma niiden torjunnan toteuttamiseksi. Lähes puolet (45 %) tarvitsee apua teknisten kontrollien käyttöönottoon ja hyödyntämiseen. Näitä ei kannata hankkia ennen kuin on käynnistänyt riskienhallinnan toteuttamisen ja tehnyt suunnitelman varautumisen suhteen.

Neljä kymmenestä (42 %) kokee tarvitsevansa apua hallinnollisten kontrollien suhteen. Kokonaisuuden kannalta hallinnolliset kontrollit ovat yhtä tärkeitä kuin teknisetkin. Kun aiemmin mainittuja teknisiä kontrolleja on otettu käyttöön, on tarve hallita ja ohjata niitä keskitetysti. Hallinnollisen tietoturvan tarkoituksena on tasapainottaa tietoturvan toteuttamista kustannukset huomioiden. Neljäsosa (26 %) kaipaa tukea kriittisen tiedon tunnistamisessa. Mikäli kriittistä tietoa ei tunnista, on vaikea varmistua siitä, että suojaa sitä mikä on tärkeää.

Vastausvaihtoehto ”Muu, mikä?” keräsi seuraavanlaisia vastauksia:

- mahdollinen verkkovalvonta
- yritysturvallisuus yleensä
- ei tarvetta, tuotantotietokoneet eivät yhteydessä nettiin
- käsitystä siitä, että uhka koskee myös julkista sektoria eikä yksin yrityksiä (sana yritys tarkoittaa julkisella sektorilla "ei koske meitä").
- henkilöstön kouluttaminen tietoaineiston tunnistamisessa sekä vakoiluyritysten tunnistamisessa.

Yritysten luottamuksellinen tieto on merkityksellistä kansantaloudelle. Mitä viranomaisten pitäisi mielestäsi tehdä tulevaisuudessa yritysvakoilun torjumisen kehittämiseksi?

- Lisätä tietoisuutta yrityksissä ja yrittäjillä, helpot ilmoituskanavat epäillyistä kyberhyökkäyksistä.
- Viestintä.
- Informaation ja tiedon jakamista.
- Kokonaisvaltainen kartoitus yritysvakoilun tilasta Suomessa. Koulutustarjonta kriittisten toimialojen (esim. huoltovarmuuskriittisyyden perusteella) henkilöstölle.
- Parantaa suojausta.
- Valistaminen ja jatkaa esim. noita Shodanin avointen porttien skannauksia ja ilmoituksia. Vaikuttaminen lainsäädäntöön myös kuten esim. Vastaamossa oli b-luokka eikä a-luokka.
- Koulutuksia, seminaareja, tiedonjako.
- Lisätä koulutusta (mm. informaatiolukutaito ja vakoilun keinot), edellyttää yrityksiltä aiempaa parempaa datan suojaamista.
- Tarjota yrityksille tietoturvaan liittyvää tukea niin taloudellisesti kuin yhteistyön merkeissä.
- Laitteisto ja ohjelmisto suositukset.
- Pitää lainsäädäntö ajan tasalla.
- Järjestää konkreettista maksutonta apua yrityksille.
- Lainsäädäntö ja valtiotasoinen suojaus uhkia vastaan. Tiedustelulainsäädännön ajantasaisuus.
- Aktiivisemmin sulkea rikollisten palvelimia ja estää kyberrikollisuutta kaikin mahdollisin keinoin. Esimerkiksi estämällä dataliikenne maista, joista ei saada viranomaisyhteistyötä rikosten selvittämiseen (Intia).
- Aktiivinen tiedottaminen, ohjeistaminen ja soveltuvin osin yhteydenotot matalalla kynnyksellä sekä parempi yhteistoiminta viranomaisten ja yritysten välillä. Esim. tiedotus mikäli yhtiöön koetaan kohdistuvan vakoilun uhkaa. Esimerkkinä myös uusien työntekijöiden turvaselvitysten kautta ilmenevien tietojen jakaminen jollain tasolla mikäli niissä havaitaan epäselvyyksiä. Nykyinen sopii tehtävään vs. ei sovi tehtävään ei anna kaikilta osin mahdollisuutta arvioida mahdollista tiedustelun tai vakoilun riskiä.
- Vastuiden määrittely laissa. Vaatimustason määrittäminen lailla, kuten on esim. velvoite nimettömän ilmoituskanavan tarjoamiselle.
- Helpottaa ja edistää sitä, miten näissä asioissa voitaisiin tehdä yhteistyötä, esim. tietyn alan sisällä.
- Tarttua terävämmin epäiltyihin tapauksiin.
- Tuntuva korotus rangaistuksiin ja vahingonkorvauksiin.
  Nopeammat ja paremmat resurssit tutkintaan.
- Oma kokemus yliopistosta kauppatieteistä v 2000; Kiinalaiset opiskelijat tulivat ryminällä opiskelemaan, opetuskieli vaihtui englanniksi, mikä heikensi opetuksen tasoa. ahkerina nämä hankkiutuivat iltatöihin esim. Nokialle. En usko että Suomen reissu oli kaikille pyyteetöntä. Yliopisto tuijotti vain omia intressejään valmistuneiden määrissä ja kansallinen turvallisuus unohtui mielestäni. Luulen, että teollisuusvakoilua tapahtui. Samalla kotimaan opetuksen laatu kärsi. => valtiollisten toimijoiden (esim. yliopisto) ansainta ei saisi ajaa kansallisten turvallisuus- ja ekonomististen tavoitteiden ohitse.
- Sitouttaa julkiset ja yksityiset toimijat, ei yksin tiedottaa nettisivuilla.
- Laki kaiken suoramainonnan muuttamisesta tilauspohjaiseksi. Keskitetty rekisteri, jossa tilauksia voi hallita. Jos markkinointi ei tilattua, niin merkittävä sakko lähettäjälle.
- Ohjeistaa ja laatia paremmat mahdollisuudet puuttua asioihin.
- Ohjata, kehittää turvaamistoimenpiteitä, pitää lainsäädäntö ajantasalla (totaalisen jäljessä nykyajan digitalisaatiosta), palkata itselleen digitalisaation asiantuntijoita ja poistaa toisesta päästä tarpeettomissa hommissa olevia työntekijöitä, olla ajan hengessä.
- Tukea kaikin laillisin ja vaikka laittomin keinoin nykyisen hallituksen hajoittamista. Se jos mikä olisi merkityksellistä kansantaloudelle.
- Jättää asia yritysten hoidettavaksi.
- Antaa neuvoja ja resursseja ulkomaan kauppaan liittyvissä hankkeissa. eritoten Kiina on vaikea maa suojata yrityssalaisuudet sekä saada siellä oikeusapua saatavien perinnässä.
- Luoda kansallinen digitaalinen luottamusportaali, jossa mm. turvasähköposti ja asiakirjojen salaukset ja avaukset aikaleimoilla.
- Tarjota tietoa ja valistusta laaja-alaisemmin.
- Lisätä tiedotusta, jotta yritysvakoiluun suhtaudutaan vakavasti.
- Kouluttaa yrityksiä vakoilun tavoista, sekä miten havaitaan vakoilu yrityksen sisällä.
- Myös yritysten pitäisi voida tehdä työnhakijasta turvaselvitys.
- Tiedotuksen ja ohjeistuksen lisääminen sekä avoin keskustelu/"nostot" yritysten luottamuksellisten tietojen vaikutuksesta kansantaloudelle. Eli "iso kuva" asiasta, sen haasteista ja vaikutuksista sekä merkittävyydestä.

- Avoin vuorovaikutus viranomaisten ja yritysten välillä. Salaiset tiedustelumenetelmät eivät kehitä yhteiskuntaa, vaan korruptoi sitä. Tiedon luokittelu ja arkaluontoisen tietoja käyttävien tahojen arkistointi kuten mitä ovat hakeneet ja mihin tarkoitukseen. Viranomaisella ei saa olla peruustettomaa pääsyä kaikkeen tietoon.
- Valistusta, jatkuvaa valistusta yrittäjille, johtajille, palkkalaisille, alihankkijoille jne. Nettipoliiseja (oikea poliisi, jonka voi hälyttää nopeasti samalla tavoin kuin fyysisen murtovarkaan perään).
- Suojata järjestelmät paremmin.
- Viestintää toimintatavoista.
- Vaatia yritykseltä seurantaa/jäljitettävyyttä siitä, mitä yritys/yrityksen työntekijät viestivät verkossa. Jos joku varastaa netin kautta yrityksen tietoja, yrityksen on ehdottomasti tiedettävä mitä, milloin on varastettu. (vrt Vastaamo). Suomessa ymmärtääkseni on tarjolla palveluja tietoliikenteen taltiointiin.
- Tiedotus, koulutus.
- Ohjeita kuinka varautua riskeihin. Riskienhallintatyökaluja.
- Ilmoittaa yritykselle mikäli sen luottamuksellisia tietoja löytyy luvattomasta paikasta. Ilmoittaa mahdollisista epäilyttävistä työntekijöistä tai työntekijöiden yhteyksistä ulkoisiin valtiollisiin tai rikollisiin tahoihin.
- Tiukempi suositus ja määräys yhteisten teletilojen valvonnan ja vastuun osalta.
- Lisätä nettiliikenteen peilausta.
- Valvonta on puutteellinen. Virkamiehiä ja poliitikoita ei saada vastuuseen tekemisistään. Hyvä veli järjestö toimii.
- Lisää henkilötyövuosia tutkintaan ja koulutukseen. Tutkinta on voimatonta, liian varovaista ja tuloksetonta.
- Entistä tehokkaampi tiedottaminen.
- Lopettaa passiivisuus (odottaa kuuta nousevaa, eli toimitaan vasta kun on jo myöhäistä)
- Voida helpommin rajoittaa esimerkiksi kansalaisuuden tai ulkomaanyhteyksien vuoksi henkilöiden pääsyä työtehtäviin, tietoihin ja toimitiloihin ilman, että asia tulkitaan syrjiväksi. Tosiasia on, että eräät valtiot eivät tunnusta esimerkiksi kaksoiskansalaisuutta ja toisaalta velvoittavat kaikki kansalaisensa välittämään hyödyllistä tietoa tiedustelupalveluilleen esimerkiksi painostamalla tai uhkaamalla.
- Selkeät ohjeistukset/suositukset perustyöntekijöille, johdolle ja tietoverkoista/tietoliikenteestä vastaaville.
- Huomattavasti kovemmat rangaistukset.
- Tiedottaa yrityksiä uusista trendeistä tai uhkista, jotka yleisesti, lähialueilla, maansisäisesti tai tietyllä toimialalla yritysvakoiluun liittyy. Antaa yritysten turvallisuus- ja riskienhallinta väelle koulutusta tai tietopaketteja.
- Kertoa avoimemmin toteutuneista tapauksista ja jakaa oppia niistä.
- Antaa yleistä tietoa kyberrikollisuudesta ja petoksista jonkin yleisen kanavan (lehdistö) kautta.
- Epäillyn rikoksen esitutkinnan ja yleisempien ehkäisevien toimien yhdistäminen viranomaisyhteistyössä.
- Tuoda viestintä lähemmäksi yrityksiä.
- Lisätä tietoisuutta ja aggregoida koulutusta parhaiden asiantuntijoiden kanssa hyvinkin nopeasti kehityvistä tekniikoista.
- Tiedottaa, kouluttaa, antaa konkreettisia vinkkejä torjumiseen, sekä mahdollistaa nopea reagointi. Toisaalta, kuten ollaan nähty, tämä on niin paljon yrityksen omasta toiminnasta kiinni, ettei siinä viranomaisten tekeminen paljoa auta, jos tuuletin on jo täynnä sitä itseään. Ennaltaehkäisevä toiminta, kenties sanktiot ja esim. tietynlaiset (pakolliset?) mittarit yritysten tietoturvalle pitäisi olla vakiotoimintaa.
- Antaa alakohtaisia suosituksia menettelytavoista, joilla yritysvakoilua voidaan vaikeuttaa.
- Tärkeintä olisi varmaan tiedon levittäminen aiheesta ja käytännön neuvojen ja opastuksen tarjoaminen.
- Ohjeistaa ja herätellä kohdennetusti.
- Tietoisuuden lisääminen, etenkin siitä, että yritysvakoilua voi kohdistua myös pieniin yrityksiin. Pienillä yrityksillä on vähiten resursseja suojata kriittistä tietoaan, mutta esim. lupaavan liikeidean tai tuotteen varastaminen voi estää pienen yrityksen kasvun.
- Tehostaa tiedottamista ja suhtautua hieman vakavammin uhkiin. Esimerkiksi kiinteistökaupat yms.
- Varoittaa yrityksiä aina kun tämmöinen vakoilu on meneillään.
- Viranomaisten pitäisi proaktiivisemmin lähestyä yrityksiä ja sidosryhmiä ja kertoa näistä asioista. Kun itse pyrkii oikeisiin ryhmiin, tietoa ja kontakteja löytyy. Myös kansalliset frameworkit ja ohjeistukset ovat hyvin lisiä. KTK tekee tässä hyvää työtä, vaikka ei suoraan yritysturvallisuuteen suoraan ota kantaa.
- Lisätä tietoisuutta asiasta.
- Rakennusala on saareke.
- Varoittaa vakoilun konkreettisesta vaarasta.

8 TARKISTUSLISTAT RISKIENHALLINNAN TUKENA

1. Ihmisiin ja yhteistyötahoihin liittyvään vakoiluriskiin varautuminen

- Turvallisuusasiat osaksi perehdyttämiskoulutusta
- Työntekijöiden säännöllinen turvallisuuskoulutus
- Ilmoituskanavan käyttöönotto (Whistleblowing)
- Turvallisuuskulttuurin luominen ja ylläpitäminen
- Työntekijöiden kannustaminen kertomaan havaitsemistaan turvallisuuspuutteista
- Henkilötietojen suojaus
- Kriisiviestintäsuunnitelma
- Matkustamisen turvallisuusohjeet
- Taustaselvitykset (ml. referenssien tarkistaminen) työntekijöistä
- Taustaselvitykset avainhenkilöistä
- Yhteistyökumppanien luotettavuusselvitykset
- Alihankkijoiden referenssien tarkastaminen
- Avainhenkilöiden salassapitositoumus
- Kilpailukieltosopimus tarvittaessa (lain rajoitukset)
- Tehtävienmukaiset pääsy- ja kulkuoikeudet

2. Tiedon suojaaminen yritysvakoilulta

- Tiedon tekniset suojauskeinot (palomuuri, virustorjunta, ajantasainen käyttöjärjestelmä, varmuuskopiointi, palvelimet)
- Tietojen luokittelu
- Liike- ja ammattisalaisuuksia koskeva luokittelu- ja käsittelyohje
- Henkilökunnan koulutus salaisten / luottamuksellisten tietojen käsittelyyn
- Tiedottaminen yrityksen tietoon kohdistuvasta uhasta
- Ohjeet viranomaisten ja yhteistyökumppanien luovuttamille luottamuksellisille asiakirjoille ja tiedoille
- Varautuminen siihen, että yritys voi olla yritysvakoilun kohteena

3. Tuotanto- ja toimitilojen suojaaminen

- Eriytetyt tuotanto-, toimisto – ja tuotekehitystilat
- Murtohälytys
- Kulunvalvonta
- Videovalvonta
- Vierailujen ohjeistus
- Vartiointi
- Henkilöstön koulutus
- Valvontajärjestelmien säännöllinen toimivuustestaus

4. Yrityksen turvallisuusjohtaminen

- Yrityksen johto osallistuu henkilökohtaisesti turvallisuuden kehittämiseen
- Turvallisuusasioita käsitellään henkilöstön kanssa
- Työntekijät voivat vaikuttaa turvallisuutta koskevaan päätöksentekoon
- Yrityksen eri osastot/toimialat tekevät yhteistyötä turvallisuusasioissa
- Yrityksen riskien säännöllinen arvioiminen riskikartoituksen avulla, toimenpiteet riskien vähentämiseksi ja toimenpiteiden seuranta.
- Yrityksellä on toimintaohje poikkeustilanteita varten
- Yritysturvallisuus on osa yrityksen vuotuista strategiasuunnittelua ja budjetti- ja toimintasuunnittelua
- Turvallisuus on osa yrityksen toiminta- tai laatujärjestelmää

9 JOHTOPÄÄTÖKSET

Neljäsosa vastaajista kertoi yritysvakoilua tapahtuneen – uhka on todellinen ja tietoa tarvitaan

Vastaajayrityksistä neljäsosa oli kertomansa mukaan ollut yritysvakoilun kohteena. Kauppakamarin aiemmissa selvityksissä syksyllä 2020 viidesosa vastaajista ja vuonna 2017 vain kahdeksan prosenttia vastaajista kertoi yrityksiinsä kohdistuneesta yritysvakoilusta tai tiedon urkkimisesta. Laiton kiinnostus yritysten tietoon on kolmessa vuodessa lähes kolminkertaistunut.

Yritysvakoilua ei ole helppo tunnistaa, siksi monet yritykset luulevat etteivät ne ole potentiaalinen kohde vaikka ne ovat jo aikaa sitten voineet olla rikoksen kohteina tai ovat sitä juuri nyt. Varattomat eivät vakoile, ostettu yritysvakoilu ei ole halpaa, koska se vaatii taitoa. Sitä toteuttavat useimmin kyberrikolliset, omat ”värvätyt” työntekijät tai ammattimaiset tietovarkaat, jotka osaavat työnsä.

Yritykset kaipaavat tietoa ja neuvoja viranomaisilta – vain neljäsosa vakoilun kohteeksi joutuneista tehnyt rikosilmoituksen

Kaksi kolmasosaa vastaajayrityksistä ei ole kertomansa mukaan saanut tietoa tai ohjeita yritysvakoilun torjumiseen. Aiheesta ei käydä riittävän aktiivisesti julkista keskustelua ja siksi tietoakaan ei ole yleisesti saatavilla.

Yritykset toivovat viranomaisten tiedottavan, antavan ohjeita ja neuvoja sekä myös kouluttavan yrityksiä aiempaa enemmän. Tiivis yhteistyö yritysten ja viranomaisten kesken on edellytys tehokkaille toimenpiteille vakoilua vastaan. Kaksi kolmasosaa vastaajista kertoo, että työntekijät eivät osaa tunnistaa yritysvakoilua riittävän hyvin torjuakseen sitä.

Neljäsosa vakoilun kohteeksi joutuneista ei tehnyt rikosilmoitusta tapahtuneesta. Syynä voi olla maineriski, mutta viranomaisten aktiivisuus tiedon jakamisessa saattaisi lisätä rikosilmoituksen tehneiden lukumäärää.

Suomi on kansainvälisesti kiinnostava kohde ja vakoilun aiheuttamat vahingot voivat kasvaa suuriksi – viidesosa vakoilluista yrityksistä kärsinyt yli miljoonan euron vahingon

Suomi on viimeiset vuosikymmenet ollut ylpeä koulutuksen korkeasta tasosta, tutkimus- ja kehitystyöstä, suomalaisen työn laadusta ja maailmalla tunnetuista, suomalaisia ”high tech” -yrityksistä. Kaikki nämä suomalaiset ylpeydenaiheet ovat rikollisten silmissä ensiluokkaisia mielenkiinnon kohteita. Yritysten mukaan vakoilutapauksien tekijät ovat niin globaaleja kuin kotimaisiakin tahoja.

Viidesosa yritysvakoilun kohteeksi joutuneista yrityksistä arvioi siitä syntyneen vahingon olleen suurempi kuin miljoona euroa. Puolet näistä arvioi vahingon ylittäneen jopa kymmenen miljoonan euron summan. Yli neljäsosa oli kärsinyt yli sadantuhannen, mutta alle miljoonan euron vahingon.

Vakoilua on yrityksissä tapahtunut niin ulkomaisten kuin kotimaistenkin tahojen toimesta. Kahdessa kolmasosassa tapauksista jäljet johtivat ulkomaille. Suomi, Kiina, Yhdysvallat, Englanti ja Saksa mainittiin taas useimmiten maina, joista kotoisin oleva kilpailija oli lanseerannut uuden samanlaisen tuotteen juuri ennen suomalaista yritystä vieden etulyöntiaseman markkinoilla. Yritysvakoilua ei ole helppo tunnistaa ja siksi monet yritykset luulevat yhä, että ne eivät ole vakoilun kohteena.

Miten paljon suomalaiselta yrityksiltä viedään laadukasta tietoa kilpailijoiden hyödynnettäväksi? Arviot vaihtelevat sadoista miljoonista miljardiin vuositasolla. Tätä summaa arvioitaessa kannattaa mieltää, että sen kattamiseksi tarvitaan yrityksen kate-euroja. Mikäli vahinko on 100 miljoonaa ja alan keskikate 20 %, on alan uhreiksi joutuneiden yritysten tehtävä lisää liikevaihtoa 500 miljoonan edestä. Ja vasta sen jälkeen on päästy menetetyn summan nollaamiseen. Kerrannaisvaikutukset yritysvakoilusta ovat huomattavasti ankarammat kuin yleisesti tunnutaan ymmärtävän. Siksi vakoilun torjuntaan ja tiedon suojaamiseen olisi panostettava huomattavasti enemmän kuin aiemmin.

Kyberrikoksia ja sisäistä uhkaa pidetään yleisimpinä tapoina vakoilla – torjuminen vaatii työtä

Yleisimmät tavat vakoilla yrityksiä olivat vastaajien mukaan kybervakoilu, viestien laiton sieppaaminen ja vanhat ja nykyiset työntekijät. Kaikille neljälle tavalle on yhteistä se, että varatumattomalla yrityksellä ei ole juurikaan mahdollisuuksia torjua vakoilua tai saada tekijöitä kiinni.

Yritysten vakavimpina pitämien vakoiluriskien torjunta vaatii järjestelmällistä riskienhallintatyötä ja investointeja turvallisuuteen. Niiden torjuminen vaatii tahtoa suojata tietoa. Vaihtoehtona voi olla myyntitulojen menetys, joka suurella todennäköisyydellä on suurempi summa kuin torjuntaan sijoitettavat resurssit. Sekä kyberrikollisten että omien työntekijöiden luoman uhan torjunta vaatii järjestelmällistä turvallisuustyötä. Jos uhkaan ei varauduta, on tieto kenen tahansa vietävissä.

Yritysten olisi hyvä aloittaa tiedon turvaaminen selvittämällä itselleen, mitkä tiedot ovat salassa pidettäviä, miten arvokkaita ne ovat ja sen jälkeen pohtia kuka voisi hyötyä niistä. Sen jälkeen on suunniteltava miten tietoa suojataan sen elinkaaren ajan. Lähtökohtana pääsylle tietoon voi olla ”vähimmän tarpeellisen pääsyn” -politiikka. Se vaatii työtä, mutta pienentää mahdollisia vahinkoja.

Koulutuksen merkitys ymmärretään

Jokaisen tietoaan suojaavan työnantajan on koulutettava työntekijöitään. Kyselyn mukaan kaksi kolmasosaa vastaajayrityksistä kouluttaa työntekijöitään. Koulutettu henkilökunta osaa toimia oikein ja toisaalta työnantaja voi edellyttää työntekijöille koulutettujen toimintatapojen noudattamista työntekijöiltä. Osaamaton työntekijä voi tehdä tyhjäksi turvallisuuteen sijoitettujen investointien tarkoituksen vesittämällä turvallisuusjärjestelmien tehon.

Rikolliset ja kilpailijat ovat suurimmat uhat

Yritysten on arvioitava yritysturvallisuuden kokonaisuutta vakoiluriskien kautta. Yritysturvallisuuden monet osa-alueet kuten tietoturvallisuus, toimitilaturvallisuus, kouluttaminen, salassapitositoumukset ovat yritysten yleisesti käyttämiä varautumisen keinoja, mutta niitä tulisi arvioida riskienhallinnan keinoin erityisesti vakoiluriskien kulmasta. Yritykset pitävät rikollisia (65 %) ja kilpailijoita (47 %) suurimpina vakoiluriskeinä. Varautuminen vakoiluun – ulkoiseen tai sisäiseen uhkaan - vaatii yritysten toimenpiteiltä hieman enemmän kuin muihin riskeihin varautuminen.

Etätyö antaa vakoilijoille enemmän mahdollisuuksia – kohteena ihminen

Viimeisen vuoden aikana yrityselämä on tehnyt merkittävän digiloikan. Etätyöstä on tullut monen asiantuntijatyötä ja tietotyötä tekevän pääasiallinen työmuoto. Kaksi kolmasosaa vastaajayrityksistä oli siksi antanut erillisiä ohjeita tiedon suojaamisesta etätyössä. Kun työntekijä on fyysisesti yksin työnsä ääressä, hän on helpompi kohde työnsä osaaville vakoilijoille. Joka kymmenes yritys kertoi yrityssalaisen tiedon vaarantuneen etätyön seurauksena. Siksi työntekijöiden on tiedostettava turvallisuus aiempaa paremmin ja työnantajan on pidettävä työntekijät hereillä mahdollisten uhkien varalta.

LÄHTEITÄ JA LISÄTIETOA

ICC Finland ja Keskuskauppakamari (2016). Tietoturvaopas yrityksille. ICC Cyber security guide for business.

Helsingin seudun kauppakamari (2019, 2016 ja 2015). Yrityksiin kohdistuvat kyberuhat.

Helsingin seudun kauppakamari (2018) Elinkeinoelämä ja hybridivaikuttaminen.

Helsingin seudun kauppakamari (2020) Yritysten rikosturvallisuus 2020

Keskuskauppakamari ja Helsingin seudun kauppakamari (2017, 2012, 2008 ja 2005)
Yritysten rikosturvallisuus –riskit ja niiden hallinta -selvitykset.

Tilastokeskuksen sivuilta löytyy tilastotietoa esimerkiksi rikollisuudesta ja rikostenselvittämisprosenteista. Http://www.stat.fi/ .

Vapaavuori, Tom (2016). Yrityssalaisuudet, liikesalaisuudet ja salassapitosopimukset.

YRITYSVAKOILU 2021 – KYSYMYKSET

1. Yrityskoko
    a. 1-9
    b. 10-49
    c. 50-249
    d. 250-

2. Yrityksen toimiala
    a. Palvelut
    b. Kauppa
    c. Teollisuus
    d. Rakentaminen
    e. Jokin muu

3. Mitä toimia yrityksesi on tehnyt yritysvakoilun torjumiseksi? (Valitse kaikki sopivat)
    a. Väärinkäytösvihjekanavan luominen (Whistle blowing)
    b. Työntekijöiden taustatarkastusten parantaminen
    c. Salassapitosopimukset työntekijöille
    d. Kilpailukieltosopimukset työntekijöille
    e. Salassa pidettävän tiedon määrittäminen
    f. Salassa pidettävän tiedon tuhoaminen asianmukaisesti
    g. Tiedon parempi suojaus (salasanat, salaus, tietoverkonturvallisuuden hallinta…)
    h. Fyysisen turvallisuuden parempi hallinta (kulunvalvonta, lukitukset, vartiointi, kameravalvonta, hälytyslaitteet..)
    i. Työntekijöiden koulutus
    j. Oman toiminnan auditointi heikkouksien / riskien löytämiseksi ja toiminnan kehittämisekseksi
    k. Emme ole varautuneet millään tavalla
    l. Muu, mikä?

4. Onko työntekijöitä erikseen ohjeistettu suojaamaan yrityksen tietoa etätyössä?
    a. Kyllä
    b. Ei

5. Onko yrityksessänne yrityssalainen tieto vaarantunut työntekijöiden etätyöskentelyn seurauksena?
    a. Kyllä
    b. Ei

6. Tehdäänkö yrityksessäsi kybervakoiluun liittyvää riskienhallintaa?
    a. Kyllä, säännöllisesti ja määrämuotoisesti
    b. Kyllä, satunnaisesti
    c. Ei tehdä
    d. Muu, mikä?

7. Minkälaista tukea yrityksesi kaipaisi kybervakoilun havaitsemiseksi ja torjumiseksi?
    a. Tukea yrityksen kriittisen tietoaineiston tunnistamiseen
    b. Tukea teknisten kontrollien käyttöönottoon ja hyödyntämiseen
    c. Tukea hallinnollisten kontrollien käyttöönottoon ja hyödyntämiseen
    d. Tukea riskienhallinnan systemaattiseen toteuttamiseen
    e. Muu, mikä?

8. Ketkä seuraavista voisivat mielestäsi olla suurin uhka yritysvakoilijoina? (valitse kolme)
    a. Kilpailijat
    b. Urakoitsijat / alihankkijat
    c. Konsultit
    d. Omat työntekijät
    e. Entiset työntekijät
    f. Valtiot
    g. Rikolliset
    h. Muu?

9. Mitkä kolme seuraavista ovat yleisimmät tavat vakoilla yrityksiä? (Valitse kolme merkittävintä tapaa)
    a. ”Lojaali” työntekijä, joka myy luottamuksellisia tietoja työnantajansa kilpailijoille
    b. Tekijä lähettää tai värvää tiedonurkkijan (istuttaa myyrän) kilpailijan palvelukseen
    c. Tekijä käyttää laittomia palveluntarjoajia arkaluonteisten tietojen saamiseksi kilpailijalta laittomin keinoin
    d. Sosiaalisen median keskustelujen hyödyntäminen
    e. Tekninen vakoilu (piilotetut mikrofonit tai kamerat)
    f. Viestinnän laiton sieppaus (puhelut, sähköpostit, muut viestit)
    g. Tiedonkerääminen liikuttaessa toimitiloissa luvallisesti tai luvattomasti
    h. Valetyöhaastattelukutsut, kanavana esimerkiksi LinkedIn, pyrkimyksenä kerätä tietoa nykyisestä työnantajasta
    i. Kybervakoilu tietoverkon kautta
    j. Työntekijä/t keräävät tarkoituksella luottamuksellisia tietoja, joihin heillä ei ole oikeuksia ja lähtevät yrityksestä perustaen kilpailevan yrityksen hyödyntäen näitä laittomasti haltuunsa saamiaan entisen työnantajansa luottamuksellisia tietoja
    k. Muu, mikä

10. Millaisiin tietoihin yritysvakoilua mielestäsi kohdistetaan? (Valitse kolme merkittävintä)
    a. Yrityksen luottamukselliset kaupalliset tiedot (asiakasrekisterit, sisäiset tuotetiedot, valmistushinnat…)
    b. Tuotantomenetelmät
    c. Tutkimus- ja kehitysprosessit
    d. Lanseerattavien tuotteiden tiedot (markkinointimateriaalit, kehitystiedot, hinnoittelu…)
    e. Palveluntarjoajan hallussa oleva yrityksen luottamuksellinen tieto (Oma asianajotoimisto, mainostoimisto, insinööritoimisto, patenttitoimisto, kirjanpitotoimisto, alihankkija…)
    f. Luottamuksellinen tieto työntekijöistä, asiakkaista, yhteistyökumppaneista tai alihankkijoista
    g. Muu, mikä

11. Onko jokin viranomainen toimittanut yrityksellesi tai alallesi tietoa tai ohjeita yritysvakoilun vaaroista ja riskeistä tai apua sen torjunnassa?
    a. Kyllä
    b. Ei

12. Yritysten luottamuksellinen tieto on merkityksellistä kansantaloudelle. Mitä viranomaisten mielestäsi pitäisi tehdä tulevaisuudessa yritysvakoilun torjumisen kehittämiseksi?

13. Mikä on suurin este yritysvakoilun torjunnan kehittämiselle yrityksessäsi?
    a. Rikosoikeudelliset seuraamukset riittämättömiä ja todennäköisyys vähäinen, varautuminen siksi hyödytöntä
    b. Tiedonsaanti yritysvakoilusta ja sen torjumisesta
    c. Työntekijät eivät osaa tunnistaa tilanteita, joissa heihin kohdistetaan yritysvakoilua
    d. Viranomaiset resurssit
    e. Omat resurssit
    f. Johdon asenne vähättelevä
    g. Emme tunnista yrityksemme olevan potentiaalinen kohde yritysvakoilulle
    h. Muu, mikä?

14. Oletteko joskus havainneet, että kilpaileva yritys, maa tai muu taho on julkistanut tuotteen, joka vastaa yrityksen kehitysvaiheen loppusuoralla olevaa tuotetta tai palvelua?
    a. Kyllä,
        i. minkä maalainen yritys on julkaissut sen?
    b. Ei

15. Onko nykyinen yrityksesi / työnantajasi tai jokin aiempi työnantajasi ollut yritysvakoilun kohteena?
    a. Ei, siirtyminen viimeiseen kysymykseen
    b. Kyllä

16. Miten yritysvakoilu tai -tapaukset tunnistettiin tai havaittiin?

17. Jos teon toimeksiantaja / hyötyjä selvisi, oliko kyseessä:
    a. Ulkomainen yritys
    b. Kotimainen yritys

18. Millaiseen tietoon yritysvakoilu kohdistui?

19. Ilmoititteko yritysvakoilutapauksen viranomaisille?
    a. Rikosilmoitus
    b. Kerrottu tiedoksi viranomaiselle
    c. Emme ilmoittaneet viranomaisille

20. Anna arvio yrityksesi kärsimän vahingon tai vahingon suuruudesta?
    a. 0–100 000 euroa
    b. 100 001–1 000 000 euroa
    c. 1 000 001–10 000 000 euroa
    d. Yli 10 000 000 euroa

21. Onko muutoin tiedossasi epäiltyä yritysvakoilutapausta, millainen se oli?

22. Luuletko yrityksesi ja / tai toimialasi olevan potentiaalinen kohde yritysvakoilulle?
    a. Ei, miksi?
    b. Kyllä, selitä miksi?

SELVITYS
YRITYSVAKOILU 2021

Helsingin seudun kauppakamari
Kalevankatu 12, 00100 HELSINKI
puh. 09 228 601, www.helsinki.chamber.fi