Yrityksiin kohdistuva tiedonhankinta

Tiedonhankinta luvattomilla ja luvallisilla keinoilla

Turvallisuusjohtaminen koulutus TJK18

Lopputyöraportti

Petteri Korsow

Avarn Security Oy

Helsinki 5.3.2024

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Lopputyöni osana Aalto Pro -yliopiston Turvallisuusjohtamisen koulutusohjelmaa (TJK18) pureudun yrityksiin kohdistuvaan tiedonhankintaan, joka voi tapahtua sekä luvallisilla että luvattomilla keinoilla. Tutkimukseni keskittyy tiedonhankinnan moninaisiin toteutustapoihin, taustalla vaikuttaviin syihin, toiminnan tekijöihin sekä näiden motiiveihin. Lisäksi työssäni tarkastelen, kuinka yritykset voivat havaita ja torjua tällaista toimintaa tehokkaasti.

Erityisen tarkastelun kohteena ovat luvattomien keinojen, kuten yritysvakoilun, yrityssalaisuuksien rikkomisen ja väärinkäytön, muodot. Toisaalta luvallisten keinojen osalta syvennyn avoimen lähteiden tiedusteluun (OSINT, Open Source Intelligence), joka tarjoaa laillisen väylän tietojen keräämiseen.

Tärkeässä roolissa tiedonhankinnassa on ihmisten toiminta. Analysoin niin tarkoituksellista kuin tahatonta toimintaa, jossa ihmiset voivat tulla kolmannen osapuolen hyväksikäytön kohteeksi tiedonkeruussa. Työni kriittinen osaalue on sisäpiiririski, joka muodostaa merkittävän uhkan yrityksen tietoturvalle ja jonka hallinta on keskeinen osa nykyaikaista turvallisuusjohtamista.

Lopputyössäni määrittelen 'tiedonhankinnan' termiä laajasti, sisältäen sekä luvallisen että luvattoman tiedonkeruun. Tavoitteenani on tarjota kattava ymmärrys yrityksiin kohdistuvan tiedonhankinnan monimuotoisuudesta ja siihen liittyvistä riskeistä sekä keinoista, joilla näitä riskejä voidaan hallita ja minimoida.

Abstract

In my thesis, as part of the Aalto Pro University's Security Management training program (TJK18), I delve into the acquisition of information targeted at businesses, which can occur through both legitimate and illegitimate means. My research focuses on the various implementation methods of information gathering, the underlying reasons, the agents involved, and their motives. Additionally, my work examines how businesses can effectively detect and counteract such activities.

A particular focus is given to the forms of illegitimate methods, such as corporate espionage, breach of corporate secrets, and their misuse. On the other hand, regarding legitimate methods, I delve into open-source intelligence (OSINT), which offers a legal avenue for information collection.

The role of human action in information gathering is paramount. I analyze both deliberate and unintentional activities, where individuals can become targets of third-party exploitation in information collection. A critical area of my work is the insider threat, which poses a significant risk to a company's information security and whose management is a central part of modern security leadership.

In my thesis, I broadly define the term 'information gathering' to include both legitimate and illegitimate information collection. My aim is to provide a comprehensive understanding of the diversity of information gathering targeted at businesses, the associated risks, and the methods through which these risks can be managed and minimized.

Sisältö

1 Johdanto

Lopputyö on osa Aalto Pro -yliopiston Turvallisuusjohtamisen koulutusohjelman koulutuskokonaisuutta (TJK18). Työssä käsitellään yrityksiin kohdistuvaa tiedonhankintaa, joka tapahtuu luvallisilla sekä luvattomilla keinoilla, tarkastellen näiden toteutustapoja, syitä, tekijöitä, tekijöiden motiiveja sekä keinoja torjua ja havaita tällaista toimintaa.

Luvattomien keinojen osalta tutkitaan yritysvakoilua, yrityssalaisuuksien rikkomista ja niiden väärinkäyttöä. Luvallisten keinojen näkökulmasta syvennytään avoimen lähteiden tiedusteluun (OSINT, Open Source Intelligence).

Teknisten toteuttamiskeinojen lisäksi keskitytään erityisesti ihmisen rooliin tiedonhankinnassa, sekä luvallisessa että luvattomassa. Analysoimme tahallisen toiminnan ohella, kuinka ihmiset voivat tahattomasti tai tahtomattaan tulla kolmannen osapuolen hyväksikäytön kohteeksi tiedonkeruussa. Tähän liittyy olennaisena osana sisäpiiririski, jota käsitellään myös erillisenä kokonaisuutena.

Lopputyössä termi 'tiedonhankinta' määritellään kattamaan sekä luvallinen että luvaton tiedonhankinta, ja se sisältää pääsääntöisesti myös yritysvakoilun ja tiedustelun.

2 Taustaa yrityksiin kohdistuvalla luvattomalle tiedonhankinnalle

2.1 Tiedustelun ja vakoilun historia

Tiedon tarve on ikuista. Tietoa on aina tarvittu parempien päätösten tekemiseen, oli sitten kyse sotilaallisesta toiminnasta tai liiketoiminnasta. Ajantasainen ja riittävä tieto vastustajasta tai kilpailijasta mahdollistaa tekemään parempia päätöksiä ja pärjäämään paremmin kilpailussa tai sodankäynnissä. Mitä tarkempi tilannekuva, sitä parempi mahdollisuus onnistua päämäärien saavuttamisessa. Tilannekuva on tietoa, tieto on valtaa ja tietoa on saatava, välillä keinoja kaihtamatta.

2.2 Miksi luvatonta tiedonhankintaa tehdään?

Kuten aiemmin todettiin, oikea ja oikea-aikainen tieto, on osa strategista, taktista kuin operatiivista toimintaa myös yritysmaailmassa. Mitä tarkempi kuva kilpailijoiden toiminnasta, sitä paremmin ja tehokkaammin voidaan vastata markkinoiden vaatimiin muutoksiin. Tai toisinaan jopa luoda muutoksia, jotka ovat oman strategian mukaisia.

Vaikka tietoa on saatavilla julkisista ja täysin laillisista lähteistä ja keinoilla, niin yritysvakoilun tai muun luvattoman tiedonhankinnan merkitys ei ole vähentynyt. Aina on tahoja, jotka ovat valmiita ylittämään laillisuuden rajat saavuttaakseen taloudelliset tavoitteensa.

Rikollinen toiminta voi olla täysin suunnitelmista ja teollisella tasolla toteutettua tai siihen voidaan, yrityksen näkökulmasta, ajautua jopa vahingossa ilman johdon toiminnalle antamaa suoranaista hyväksyntää. Vaikka rikollinen toiminta harvoin voidaan katsoa tapahtuneet aidosti vahingossa, niin tilanteeseen voidaan ajautua ainakin osittain ilman suoranaista aikomusta.

3 Juridinen ulottuvuus

3.1 Suomen lainsäädäntö

Suomen lainsäädäntö kriminalisoi yritysvakoilun ja liikesalaisuuksien väärinkäytön rikoslaissa (30. luku). Yritys on myös säädetty rangaistavaksi kummassakin. Koska kummankin maksimirangaistus on kaksi vuotta vankeutta, voi poliisi käyttää laajempaa pakkokeinojen valikoimaa kuin useimmissa muissa maissa. Esimerkkejä näistä tutkinnan kannalta erittäin hyödyllisistä pakkokeinoista ovat takavarikoinnit ja kotietsinnät. Useissa maissa tällaisia pakkokeinoja ei ole poliisin käytettävissä, jolloin todistusaineiston kerääminen voi olla hyvinkin hankalaa, jos poliisi ei voi takavarikointien kautta esimerkiksi saada haltuunsa luvattomasti hankittua materiaalia tai dokumentteja.

Rikoslaissa on kolme eri kohtaa, jotka viittaavat aiheeseen:

1) Yritysvakoilu (rikoslaki luku 30, 4 §) jolla tarkoitetaan tapauksia, jossa tietoja on hankittu luvattomasti käyttäen keinoja… toiselle kuuluvasta yrityssalaisuudesta. Yritysvakoilun voidaan katsoa koskevan ulkopuolisen tekemää tekoa, ei esimerkiksi yrityssalaisuuden omaavan tahon työntekijää.
2) Yrityssalaisuuden rikkominen (rikoslaki luku 30, 5 §) taas tulee yleensä kysymykseen, kun rikkojalla ja yrityssalaisuuden haltijalla on jokin sopimusperäinen suhde.
3) Yrityssalaisuuden väärinkäyttö (rikoslaki luku 30, 6 §) voi tulla kysymykseen, jos hyödyntää elinkeinotoiminnassaan tai hankkiakseen itselleen tai toiselle taloudellista hyötyä 4§ tai 5§ mukaisilla teoilla saatua tietoa.

Liikesalaisuudesta itsessään taas säädetään Liikesalaisuuslaissa[i], jossa säädetään elinkeinotoimintaan liittyvien liikesalaisuuksien sekä teknisten ohjeiden suojasta. Liikesalaisuuksiin ja yrityssalaisuuksiin viitataan myös useissa muissa laeissa.

Työsuhteessa työntekijöillä sitoo hyvin voimakas salassapitovelvollisuus automaattisti, joka tulee työsopimuslaista.

Näitä keskeisiä lakeja verrattaessa tulee huomioida, että rikoslaki suojaa yrityssalaisuuksia ainoastaan kaksi vuotta työsuhteen päättymisen jälkeen. Tämä rajaus ei koske oikeudettomasti hankittuja tietoja. Lakien antamasta suojasta huolimatta tulisi työntekijän kanssa solmia erillinen salassapitositoumus, mikäli työntekijä käsittelee, tai hänellä on pääsy, yrityssalaisuuksiksi luokiteltuihin tietoihin.

Yrityssalaisuuden määritelmä ei ole yksiselitteinen, mutta sille voidaan ajatella muutamaa keskeistä kriteeriä, joiden kaikkien tulisi täyttyä, jotta voidaan puhua yrityssalaisuudesta.

1) Tieto ei ole yleisesti tunnettua tai helposti selville saatavissa kokonaisuutena tai osiensa yhdistelmänä.
2) Tiedolla pitää olla salassapitointressi, joka yleensä on tiedon taloudellinen merkittävyys. Jos kyseessä on vähäpätöinen, vähäarvoinen tai vanhentunut tieto, niin sitä ei yleensä voida luokitella yrityssalaisuudeksi.
3) Tiedon suojaamiseksi on ryhdytty kohtuullisiin toimenpiteisiin.

Näitä ehtoja tarkasteltaessa voidaan nopeasti huomata niin tulkinnan vaikeus. Taloudellisen arvon määrittäminen voi olla hyvinkin erilaista pienen yksinyrittäjän ja suuryrityksen kohdalla. Yksinyrittäjälle 500 € voi olla taloudellisti merkittävä summa, kun taas suuryritykselle 100 000 € voi olla vasta jossakin määrin merkittävä summa.

Vaikka liikesalaisuuden toisaalta pystyy helposti täyttämään ja perustelemaan, ei siihen tule kuitenkaan suhtautua ylimalkaisesti.

Tiedon salaamiseen ja salassa pitämiseen tuo nykyään oman lisähaasteensa pilvipalvelut ja näiden kohdalla erityisesti erilaiset yhteistyöalustat. Näiden käyttäminen on toki täysin perusteltavissa työn tehokkuuden kannalta, mutta näitä käytettäessä tulee oikeasti panostaa tietojen turvaamisen suunnitteluun sekä tarvittavien salassapitosopimusten laatimiseen. Ongelmallisuutta näiden suhteen lisää vielä nykyaikaiset pitkät alihankintaketjut, joihin kaikki samat rajaukset, velvollisuudet ja vastuut tulee ulottaa luotettavalla tavalla. Tiivis-

tettynä haaste tässä on se, että samalla kun tiedot pitäisi pitää salassa ulkopuolisilta, niin yhteystyön toimivuuden takia pääsy tietoihin pitää jakaa ulkopuolisille.

Yhteistyösopimusten päättyessä sopimukset, salassapitosopimukset erityisesti, vaativat toiselta osapuolelta saatujen luottamuksellisten tai salaisten tietoja palauttamista tai tuhoamista. Analogisessa maailmassa tämä tarkoittaisi silppuria tai vaikka polttamista. Digitaalisessa maailmassa taas tallennusvälineiden tuhoamista tai tietojen poistamista muuten tietojärjestelmistä. Yleensä tälle on asetettu jokin aikaraja sopimuksissa. Tätä vaatimusta voi olla käytännössä täysin mahdotonta toteuttaa teknisesti, jos ajatellaan vaikka varmuuskopioita. Todennäköisesti yksikään toimija ei pysty poistamaan luotettavasti vain tiettyjä tietoja yrityksen varmuuskopioista. Ongelmia tiedon luottamuksellisuuteen tämä voi aiheuttaa tilanteissa, joissa varmuuskopioita joudutaan palauttamaan. Tällöin jo kertaalleen poistettuja tietoja saattaa palautua saataville tai jos varmuuskopioiden tietoturva vaarantuu jollain tavalla ja ne joutuvat vääriin käsiin. Pilvipalvelut eivät tuo ainakaan helpotusta tähän ongelmaan. Tähän ongelmaan ei juurikaan koskaan näe puututtavan salassapitosopimusten sisällössä.

Liikesalaisuuden väärinkäytön kohdalla pitää muistaa myös siihen pätevät rajoitteet. Esimerkiksi entisen työntekijän ei voida olettaa unohtavansa kaikkia entisessä työssään oppimiaan asioita tai vaatia, että hän ei niitä enää loppuelämänsä aika käyttäisi. Työntekijällä, entiselläkin, on oikeus omaan ammattitaitoon. Vähän kärjistäen voi sanoa, että asiat, jotka työtekijä voi viedä mennessään päänsä sisällä, eivät yleensä loukkaa liikesalaisuutta vaan ne lasketaan ammattitaidoksi. Mutta jos työtekijä vie mennessään mitä tahansa konkreettista, voidaan jo hyvinkin helposti puhua liikesalaisuuden loukkaamisesta.

3.2 Tekijänoikeusrikos

Tekijänoikeusrikos määräytyy Suomen laissa tekijänoikeuksista (tekijänoikeuslaki 404/1961) ja erityisesti sen 49 §:ssä[ii] (Luettelon ja tietokannan valmistaja). Tekijänoikeusrikoksella tarkoitetaan tekijänoikeuden loukkaamista tavalla, joka on omiaan tuottamaan tekijälle tai muulle oikeudenhaltijalle taloudellista vahinkoa. Tämä voi tapahtua esimerkiksi kopioimalla, levittämällä tai julkaisemalla tekijänoikeudella suojattua ilman oikeuden haltijan lupaa.

Myös rikoslaista (39/1889) voidaan löytää tekijänoikeusrikoksiin soveltuvia säännöksiä sen osilta, jotka käsittelevät omaisuuden suojaa liittyviä rikkomuksia kuten varkautta ja petosta, mikäli ne liittyvät tekijänoikeuksien rikkomiseen. Luvattoman tiedonhankinnan kohdalla tekijänoikeuslain rikkominen vaatii toki sen, että luvattoman tiedonhankinnan kohteeksi joutunut tiedon on voitu katsoa muodostaneen teoksen.

Esimerkiksi tapaus Meyer Turussa tekijälle alun perin vaadittiin tuomiota tekijänoikeusrikoksesta yrityssalaisuuden väärinkäyttämisen lisäksi.

3.3 Toiminta Suomen ulkopuolella

Verkottunut digitalisaatio laajentaa lähes kaikkien yritysten toiminnan tai saavutettavuuden Suomen rajojen ulkopuolelle. Vaikka yritys itsessään onnistuisi pitämään kaiken liiketoimintasa rajojen sisäpuolella, se ei tällä kuitenkaan saa suojattua itseään globaaleita uhilta, sillä lähes kaikilla yrityksillä on jotain sellaista tietopääomaa mikä hyvinkin voi kiinnostaa rajojen ulkopuolella toimivaa luvattomaan tiedonhankintaan turvautuvaa toimijaa.

Mikäli liiketoiminta missään määrin sisältää yhteyksiä tai kumppanuuksia ulkomailla toimivien tahojen kanssa, tulee yrityksen muun muassa panostaa sopimusteknisesti suojaamaan omaa tietopääomaansa ja samalla pyrkiä mahdollisuuksien ja riskiarvioiden kautta ymmärtämään näiden maiden paikallista lainsäädäntöä, kansainvälistä lainsäädäntöä ja tapaoikeutta. Pienemmille ja pienillä resursseilla toimiville yrityksille tämän kaltainen toiminta voi olla, varsinkin laajasti ja syvällisemmin toteutettuna, liian vaativaa. Minimivaatimuksena voisi kuitenkin pitää laillisesti sitovien salassapitosopimusten solmimista. Salassapitosopimus olisi hyvä teetättää asiaan perehtyneellä juristilla, vaikka yleiskäyttöisiä sopimuspohjia löytyykin verkosta paljonkin.

Rajat ylittävässä toiminnassa on tärkeää huomioida ja ymmärtää, että jossakin tapauksissa sekä mikä Suomessa olevaan yritykseen kohdistuva toiminta on rikollista, saattaa, suomalaisesta näkökulmasta, rikollista toimintaa harjoittava taho toimia paikallisen lainsäädännön mukaisesti laillisesti. Yleensä tämä ristiriita tulee esille, kun puhutaan valtiollisista toimijoista tai näiden lukuun toimivista toimijoista.

3.4 Verkossa tapahtuva yritysvakoilut tai luvaton tiedonhankinta

Verkossa tapahtuvan rikollisuuden yksi hankaluus, myös yritysvakoilun suhteen, on rikospaikan määrittely. Suomen rikoslain mukaan verkkorikosten tapahtumapaikan määrittely voi olla haasteellista, koska nämä rikokset voivat käytännössä tapahtua useassa paikassa yhtäaikaisesti. Vaikkakin rikoksen tekopaikaksi yleensä katsotaan paikka, jossa rikoksen seuraamukset ilmenevät. Käytännössä tämä tarkoittanee, että jos verkossa tapahtuneen rikoksen vaikutukset ulottuvat Suomeen, Suomen lainsäädäntö voi tulla sovelletuksi. Tällöin siis katsotaan, että rikos on tapahtunut suomessa, vaikka tekijä olisi toiminut toisesta maasta käsin[iii].

4 Avoimiin lähteisiin perustuva tiedonhankinta (OSINT)

4.1 OSINT yleisesti

OSINT, eli Open Source Intelligence, suomalaisittain avointen lähteiden tiedustelu, on erityisesti viimeisen vajaan kymmenen vuoden aikana internetin ja sosiaalisen median räjähdysmäisen kasvun kautta suosiota kerännyt tapa ja tekniikka kerätä tietoja mielenkiinnon kohteesta niin, että kaikki tiedot kerätään periaatteessa kaikille avoinna olevista lähteistä. Tietoa kerätään kohteeseen koskematta, eli OSINT ei sellaisenaan sisällä esimerkiksi kohdetta kohtaan suoritettavaa tietomurtoa.

OSINT toimintaa voidaan yleensä suorittaa ilman erillisiä työkaluja, mutta tietojen keräämistä, organisointia ja analysointia voidaan tehostaa ja helpottaa käyttämällä näihin tarkoituksiin suunniteltuja ohjelmistoja, niin kaupallisia kuin vapaan lähdekoodin sovelluksia. Nykyään OSINT toiminta keskittyy etupäässä Internettiin, mutta käsitteellisesti se ei kuitenkaan rajoitu siihen ja se voi tapahtua, vaikka keräämällä tietoa perinteisistä medioista tai vaikka tarkkailemalla kohdetta luonnossa (huomioiden kuitenkin ”kohteeseen koskematon” periaatteen).

4.2 OSINT hyödyntäminen yrityksiin kohdistuvassa toiminnassa

Yritykset voivat käyttää OSINT tekniikoita ja taktiikoita muun muassa kilpailija-analyyseja tehdessään tai vaikkapa selvittäessään potentiaalisia markkinoita uusilla osa-alueilla. Käytännössä tämänkaltaisen toiminnan tulisi kuulua jokaisen yrityksen normaaliin toimitaan, eikä siinä sinänsä ole mitään moitittavaa. Yrityksissä ei vain aina käytetä tätä nimitystä tai osata suoraan mieltää käytettyjä tekniikoita tai taktiikoita tämän nimikkeen alle. On myös yrityksiä, jotka suoraan tarjoavat OSINT palveluja yritysten käyttöön eri tarkoituksiin. Tarkoitukset voivat olla niin perinteinen kilpailija-analyysi tai osana markkina-analyysia tai yritys voi myös tilata itseensä kohdistuvan

OSINT toimeksiannon, jolla se pyrkii selvittämään omaa OSINT näkyvyyttään. Tämän tyyppinen toiminta on yleensä turvallisuusnäkökulmasta toteutettu eikä niinkään suoraan liiketoimintaan suoraan liittyvä toimeksianto.

Itseensä kohdistuvassa OSINT toimeksiannossa on rajattava selvityksen laajuus tarkasti niin, että omien työntekijöiden yksityisyydensuojaa ei loukata. Materiaalia kerättäessä tulee muistaa mahdollinen kertymävaikutus ja arvioida sen vaikutusta niin turvallisuuden kuin yksityisyydensuojan kannalta.

4.3 Luvallisesta luvattomaan

Normaalisti OSINT toiminta ei ole lakien tai asetusten vastaista, eikä edes näiden harmaalle alueelle menevää toimintaa. OSINT toimeksiannossa tulee kuitenkin aina muistaa painottaa sitä, että käytettävät taktiikat ja tekniikat tulee valita ja toteuttaa niin, että ne eivät riko mitään lakeja tai asetuksia, eivätkä saa muutenkaan olla eettisesti arveluttavia. Huonosti suunnitellussa ja valvotussa OSINT toimeksiannossa on aina riski, että siinä mahdollisesti jopa tahattomasti liutaan vähintäänkin harmaalle alueelle.

Toisaalta yritysten tulee itse varautua itseensä kohdistuvaan OSINT toimintaan, myös mahdollisesti laillisuuden rajat ylittävään. Laillisuuden rajat rikkovassa toiminnassa ei kuitenkaan ole enää kyse OSINT toiminnasta, vaan saatetaan puhua jo jopa yritysvakoilusta tai sen yrityksestä.

Käytännössä kohteen on vaikea havaita itsensä kohdistuvaa OSINT toimintaa, oli toiminta sitten kaikkien lakien ja asetusten mukaista tai vastaista. Periaatteessa toiminta voidaan havaita vasta kun se on ylittänyt laillisuuden rajat.

OSINT taktiikoiden ja tekniikoiden käyttäminen voi toisaalta kuulua myös muuten laittomiin keinoihin turvautuvan toimijan keinovalikoimaan yksinkertaisesti sen tehokkuuden takia. Tehokkuudella tarkoitetaan tässä niin sen tuottamaan tietoa, kustannustehokkuutta ja ajasta ja paikasta riippumattomuutta. Lopputulosta voidaan käyttää joko varsinaisen hyökkäyspinta-alan kartoittamiseen tai laittomin keinoin saatujen tietojen rikastamiseen tai syventämiseen. OSINT näkyvyyden ymmärtäminen, hallinta ja tarvittaessa rajoittaminen saattaa olla joissakin tapauksissa tarpeellista myös henkilöturvallisuuden takia[ivv].

5 Luvaton tiedonhankinta

Luvattoman tiedonhankinnan alla käsitellään niin perinteistä yritysvakoilua kuin liikesalaisuuden väärinkäyttöä.

5.1 Sisäpiiri

Sisäpiiri muodostaa erityisen uhan mietittäessä yrityksiin kohdistuvaa yritysvakoilua ja liikesalaisuuksien väärinkäyttöä. Sisäpiiriuhkaa käsitellään laajemmin kappaleessa 9. Sisäpiiriuhka ja -toimijat.

5.2 Ulkopuolinen taho

Yritysmaailmassa keskeiset ulkopuoliset tahot ovat kilpailijat ja rikolliset toimijat, jotka hakevat taloudellista hyötyä. Kilpailijat suoraan itselleen ja rikolliset toimijat myydäkseen hankittuja tietoja.

5.3 Valtiollinen toimija

Vaikka valtiolliset toimijat eivät suoraan kuulu tämän lopputyön aihepiiriin, ei niitä voida kuitenkaan kokonaan ohittaa miettiessä yrityksiä ja niiden liikesalaisuuksien suojaamista. Lisäksi nykyaikaisessa ”harmaassa” toiminnassa ei aina voida täysin erottaa valtiollisia toimijoita ei valtiollisista toimioista. Valtiollinen toimija saattaa ulkoistaa yritysvakoilun ei valtiolliselle toimijalle salatakseen omat päämääränsä tai osallisuutensa tai vähintäänkin saadakseen mahdollisuuden kiistääkseen osallisuutensa. Eli yrityksellä on vastassaan tällöin jonkun valtiollisen tahon intressit, mutta ei valtiollisen tahon toiminta. Tämä toimii käytännössä samalla toimintalogiikalla kuin kybertoiminnalla vaikuttamisessa, esim. proxytoimijalle ulkoistetussa kyberhyökkäyksessä.

Valtiollisen toimijan lukuun toimiva ei valtiollinen toimija toimii joko puhtaasti palkattuna tahona tai mahdollisesti myös ideologisista syistä.

Valtiollisen toimijan intressit eivät välttämättä ole taloudellisen hyödyn hakemista toisin kuin yritysten välisessä yritysvakoilussa yleensä. Valtiollinen toimija voi suorittaa yritysvakoilua taloudellisista syistä esimerkiksi toimittamalla kaappaamiaan yrityssalaisuuksia oman valtionsa kaupallisille toimijoille kilpailuedun saamiseksi. Toisaalta valtiollinen toimija voi toimia myös puhtaasti kansallisen turvallisuuden nimissä hankkimalla esimerkiksi tietoja toisen valtion kriittisestä infrastruktuurista tai vaikka aseteollisuudesta.

Puolustautuminen valtiollista toimijaa vastaa tapahtuu periaatteessa ja käytännössä samalla tavalla kuin muitakin toimijoita vastaan. Valtiollisia toimijoita miettiessä tulee kuitenkin huomioida, että näillä todennäköisesti on huomattavasti paremmat resurssit käytettävissään ja sen kautta puolustautumisesta tulee huomattavasti vaativampaa, kun yksityisiä toimijoita vastaan toimiessa. Resurssien lisäksi keinovalikoima saattaa olla huomattavasti laajempi.

6 Henkilötiedustelu (HUMINT)

Henkilöön kohdistuva tiedustelu (Human Intelligence) on tiedustelun muoto, jossa joku tai valittu joukko nimettyjä henkilöitä ovat tiedustelun kohteena niin, että näistä henkilöistä itsestään yritetään saada tietoa tai saada tietoja, joihin näillä henkilöillä on pääsy tai ovat näiden tiedossa.

Henkilö, joka joutuu HUMINT kohteeksi, ei aina välttämättä ole lopullinen kohde, vaan kyseistä henkilö saatetaan yrittää käyttää ainoastaan, jotta saataisiin pääsy varsinaiseen kohteeseen.

Internetin ja sosiaalisen median aikakaudella nämä kanavat ovat varmasti nousseet keskeisiksi kanaviksi HUMINT toiminnalla samoin kuin OSINT toiminnallekin. Tämä vaikkakin HUINT yleensä miellettään ihmisen tekemäksi ennemminkin kuin teknisin keinoin suoritetuksi toiminnaksi[vi].

Yritysturvallisuuden kannalta HUMINT voidaan nähdä joko suorana liikesalaisuuksiin kohdistuvana riskinä tai sitä voidaan myös OSINT tavoin käyttää kohteen hyökkäyspinta-alan kartoittamiseen.

Luonteensa vuoksi tämän kaltainen toiminta yleensä on vähintäänkin kohteen yksityisyydensuojaa loukkaavaa.

Näitä riskejä hallitakseen yritysten tulee antaa tunnistetuille henkilöille sellaista koulusta, joka antaa valmiudet toimia niin, että henkilö ei itse ainakaan liikaa myötävaikuta kohteeksi joutumistaan. Koulutuksen tulisi myös antaa valmiuksia tunnistaa HUMINT toimintaa. Henkilötiedustelun kohteeksi joutumisen riskin voidaan ajatella korostuvan matkustettaessa Suomen ulkopuolelle, varsinkin jos halutaan varautua valtiollisten toimijoiden harjoittaman yritysvakoilun suhteen.

Henkilötiedustelunkin kohdalla tulee muistaa, että suojaustoimien tulee olla sellaisia, että ne huomioivat myös inhimillisen puolen. Ihmisten kohdalla ei

voida ajatella yhtä selkeitä ja rajoittavia turvatoimia kuin teknisessä puolustuksessa. Onnistuminen vaatii ymmärtämään sen, että ihmisiä ei voi vaatia elämään täydellisessä suojatussa kuplassa. Tämänkaltaiseen ajatteluun perustuva ei voi pääsääntöisesti olla menestyksellistä.

Yritykselle olisi keskeistä yrittää tunnistaa ne työntekijät tai työtekijä ryhmät, jotka voivat olla erilaisten ominaisuuksiensa kautta alttiimpia HUMINT toiminnalle. Tätä kartoitusta tehdessä tulee kuitenkin muistaa tiukasti pitäytyä sellaisessa toiminnassa, joka ei loukkaa näiden henkilöiden yksityisyydensuojaa.

6.1 HUMINT digitalisoituvassa maailmassa

HUMINT ei terminä tai edes tekniikkana ota kantaa siihen missä domainissa se tapahtuu ja voidaan varmastikin olettaa sen siirtyneen digitaaliseen ulottuvuuteen maailman digitalisoituessa. Henkilön taustojen selvittäminen onnistuu helposti verkossa henkilöön koskematta muun muassa OSINT tekniikoilla, vaikka toiselta puolelta maailmaa. Tämä koskee myös luonnollisesti kohdehenkilöiden valitsemista.

Tiedonhankinnassa HUMINT ei itsessään ole päämäärä, vaan yksi työkalu pahantahtoisen toimijan valikoimassa, jonka kautta henkilöön päästään käsiksi pyrittäessä saamaan pääsy haluttuihin yritys- ja liikesalaisuuksiin.

7 Etiikka ja toimiminen harmaalla alueella

Yrityksiin kohdistuva vakoilu ja luvaton tiedonhankinta on itsessään hyvin monimutkainen kokonaisuus eikä siinä aina voida vetää selkeitä linjoja sen suhteen, milloin toiminta kestää eettistä tarkastelua tai milloin toiminta on mahdollisesti siirtynyt juridisesti harmaalle alueelle.

Kilpailevat yritykset ovat aina pyrkineet saamaan kilpailuetua hankkimalla tietoa toisistaan ja saamaan kilpailuetua hankittujen tietojen kautta. Tiedon olemassaolon ja tiedon hankkimisen tarve on luonut myös yritysvakoilun ympärille hyvin moniuloitteisia ja monimutkaisia toimintamalleja, jotka kaikki eivät aina kestä eettistä tarkastelua ja laillisuudenkin suhteen on saatettu siirrytty harmaalle alueelle.

Moni organisaatiossaan kilpailijaseurannasta vastaava henkilö saattaa löytää itsensä pohtimassa etiikan ja lain risteyksessä keinoja, miten täyttää tiedonhankinnalle asetetut vaatimukset ja tavoitteet.

Välttääkseen ongelmat, yrityksen tulee selkeästi omassa sisäisessä ohjeistuksessaan ja tiedonhankinnan toimeksiannoissaan ilmasta ehdoton vaatimus noudattaa eettistä ja selvästi laillisissa puitteissa tapahtuvaa tiedonkeruuta ja toimintamalleja. Käytettäessä ulkopuolisia toimijoita tiedonkeruun suorittamisessa, nämä vaatimukset tulee aina sisällyttää kirjalliseen toimeksiantoon.

Vaikka etiikka ja laki ovat yleensä yhteydessä toisiinsa, ne eivät aina ole täysin synkroniassa keskenään. Lait ovat yleensä enemmän konkreettisia ja antavat selkeämmin vastauksia siihen, mikä on sallittua ja mikä kiellettyä, etiikka taas muodostuu enemmän yhteiskunnan normien, kulttuuristen uskomusten ja yksilöllisten arvojen perusteella. Lisäksi etiikkaa saattaa reagoida ja muuttua nopeammin yhteiskunnallisiin muutoksiin kuin lainsäädäntö. Tämä toisinaan aiheuttaa sen, että jotkut asiat ovat laillisia mutta ne saatetaan nähdä epäeettisinä, ja päinvastoin.

Yritysten tulee myös miettiä omien vastatoimiensa eettisyyttä ja juridisia ulottuvuuksia suunnitellessaan ja toteuttaessaan siihen kohdistuvan yritysvakoilun torjuntataktiikoita ja –tekniikoita, jotta näissäkään ei liettäisi epäeettisiin saatikka laittomiin keinoihin. Tämä tulee luonnollisesti huomioida tämän kaltaisissa ulkoistuksissa ja tehtäväksi annoissa kirjallisesti ja sopimustasolla vaatimuksena.

Huolellisuusvelvollisuus näiden kohdalla korostuu varsinkin käytettäessä teknisiä välineitä, joissa olevat ominaisuudet saattavat mahdollistaa sellaisetkin toimenpiteet, jotka eivät ole sallittuja paikallisen sovellettavan lainsäädännön näkökulmasta. Esimerkkinä tällaisesta voisi olla muun muassa työtekijöiden viestinnän laajamittainen, pitkäkestoinen ja kohdennettu seuranta, jota ei voida tosiasiallisesti perustella rikosten- ja väärinkäytösten paljastamisella.

Yhteenvetona voidaan sanoa, että jokainen yritys on itse vastuussa oman toimintansa eettisyydestä ja siitä, että se ei lipsu liikaa laillisuuden harmaalle alueelle tai ainakaan sen laittomalle puolelle. Vaikka harmaalla alueella ei vielä varsinaisesti syyllistyttäisi suoranaisiin laittomuuksiin, tulee tässäkin kohtaa huomioida sen mahdolliset haitat, jotka voivat heijastua asiakkuus- ja kumppanuussuhteisiin sekä aiheuttaa negatiivista julkisuuskuvaa.

8 Yritysvakoilu palveluna (EaaS)

Teknologian nopea kehittyminen ja sen myötä kaiken kattava globalisaatio on avannut mahdollisuuden uudenlaisille rikollisuuden muodoille. Yksi näistä kyberrikollisuuden muodoista on palveluna tuotettava yritysvakoilut.

Kuten muissakin “aaS” palveluissa, EaaS tarjoaa yleensä modulaarisen, skaalautuvan palvelun, joka on saatavilla 247 ympäri maailman. Näiden palveluiden käyttäminen voi myös luoda tilaajalleen kiistettävyyden suojan kiinnijäämistilanteessa.

Erilaisia toimintamalleja voivat olla:

- Hankitaan materiaalia tai pääsyoikeuksia, joita sitten myydään jälkikäteen niistä kiinnostuneille.

- Otetaan vastaan toimeksiantoja kohdistettuihin yritysvakoilutoimeksiantoihin, jossa tilaaja valitsee kohteen.

- Myydään muissa tietomurroissa ja tietovuodoissa julkaistua materiaalia, jota on ehkä pystytty jalostamaan helpommin hyödynnettävään muotoon.

- Valtiollisilla toimijoilla on käytettävissään vielä huomattavasti kehittyneempiä ja paremmin organisoituja taktiikoita ja tekniikoita.

EaaS toimijat vaihtelevat yksittäisistä hakkeriryhmistä tai -henkilöisät aina hyvin organisoituihin järjestäytyneen rikollisuuden toimijoihin. Näiden toimijoiden motiivit voivat olla taloudellisia, poliittisia tai ideologisia. Taustalla voi olla myös valtiollisia toimijoita tai tahoja, joille valtiollinen toimija on toiminnan ulkoistanut (vrt. APT).

Hyvän saatavuuden takia näiden palveluiden käyttäjät eivät rajoittune ainoastaan suuriin tai varakkaisiin yrityksiin, vaan käyttäjinä saattaa myös olla

pienempiä tai startup yrityksiä, jotka yrittävät saada liiketoimintahyötyä näiden palveluiden kautta.

EaaS toimijat voivat käyttää toiminnassaan huipputeknologisia työkaluja ja menetelmiä, mutta ne voivat myös perustaa toimintansa myös sen ympärille, “mitä on saatavilla”. Jälkimmäisestä esimerkkinä voisi toimia perinteiset kalasteluviestien kautta saadut jalansijat tai vaikka yleiset salasanavuodot, joita voidaan yrittää myydä sellaisenaan tai murrettuna (ts. Salasanavuoto on sisältänyt salasanojen tiivisteet ja osa näistä on pystytty purkamaan).

Suojautuminen näitä vastaan tapahtuu etupäässä samoin keinoin kuin mitä tahansa kyberuhkaa vastaan.

9 Sisäpiiriuhka ja -toimijat

9.1 Sisäpiiri - erityinen uhka yritys- ja liikesalaisuuksille

Sisäpiirillä viitataan yleensä sellaisiin henkilöihin, joilla on pääsy yrityksen sisäisiin luottamuksellisiin tietoihin, muun muassa yritys- ja liikesalaisuudet ja muut arkaluonteiset ja salassa pidettävät tiedot. Näillä henkilöillä voi olla työnsä puolesta sallittu käyttöoikeus näihin tietoihin tai henkilö voi saada näitä tietoja tietoonsa luvattomilla keinoilla hyödyntäen luvallisia pääsyoikeuksiaan. Yleisellä tasolla sisäpiiriuhaksi voidaan katsoa myös osittain toimitusketjuun kuuluvat tahot, esimerkiksi alihankkijat ja ulkoistuskumppanit.

Sisäpiiriuhaksi voi luokitella henkilöt jotka:

1. Työskentelevät yrityksessä tai kuuluvat toimitusketjuun, jolla on samansuuntaiset pääsyoikeudet suojeltavaan tietoon kuin yrityksessä työskentelevillä.
2. Saavat tietoonsa yrityksen salaisia ja luokiteltuja tietoja joko työnsä puolesta luvallisesti tai luvattomia keinoja käyttäen.
3. Hyödyntävät näin saamiaan tietoja yrityksen ulkopuolella henkilökohtaiseen hyötyyn tai antavat sen kilpailijoille tai muille tahoille.

Edellä mainitun kuvauksen lisäksi tulee huomioida mahdollisuus valtiollisiin toimijoihin, vaikka ne eivät sisälly tämän lopputyön piiriin.

Sisäpiiriuhkein torjumiseksi tulee ymmärtää seuraavat uhat ja niihin liittyvät perusasiat:

4. Motiivit. Sisäpiirin väärinkäytöksien motiivit voivat olla moninaiset. Motiivit voivat syntyä tyytymättömyydestä työnantajaa kohtaan ja toimia kostona koetuista vääryyksistä. Toisia taas saattaa ajaa henkilökohtainen taloudellinen motivaatio rahallisen hyödyn tavoittelun kautta. Taloudellisen motivaation takana saattaa myös olla henkilökohtaiset raha- ja talousvaikeudet. Toisaalta motiivina voi toimia

myös ajatus paremmasta urakehityksestä toisen työnantajan palveluksessa.

5. Helppo pääsy tietoon. Koska sisäpiirissä olevalla henkilöllä on jo työnsä puolesta pääsy tietoon tai pääsyn hankkiminen voi onnistua helposti, voi kynnys väärinkäyttää luottamusta madaltua varsinkin, jos yrityksessä ei noudateta kunnollisia kontrolleja tiedon pääsyn suhteen.
6. Havaitsemisen vaikeus. Tietojen väärinkäyttöä voi olla erittäin hankala havaita ja tietojen väärinkäyttö voi tämän takia jatkuva vuosia tai jopa vuosikymmeniä. Pieni kiinnijäämisriksi voi toimia lisämotivaationa kahden vaiheilla olevalle henkilölle.
7. Tiedon ymmärtäminen. Sisäpiiriläinen yleensä pystyy ulkopuolista paremmin arvioimaan mikä tieto on arvokasta ja mikä vähemmän arvokasta ja tämän kautta keskittymään paremmin arvokkaampaan tai paremmin hyödynnettävään tietoon. Tämä lisää vahinkojen määrä ja myös nopeutta millä tilanne voi kehittyä.
8. Yhteistyö ulkopuolisten kanssa omasta tahdosta tai tahdonvastaisesti. On syytä muistaa, että sisäpiiriuhan muodostava henkilö saattaa olla värvätty suorittamaan tehtävää joko oman tahdon mukaisesti tai oman tahtonsa vastaisesti esimerkiksi kiristyksen kautta. Kummatkin tilanteet voivat muodostua niin työsuhteen aikana, kuin enne työsuhdettakin. Toisin sanoen henkilö voi rekrytoitua sellaiseen työtehtävään, jossa saa pääsyn haluamansalaiseen tietoon.

9.2 Sisäpiiriuhan havainnointi ja torjunta

Sisäpiirin luoman uhan erityisen luonteen vuoksi sen havainnointi ja torjunta on pääsääntöisesti hankalampaa kuin ulkoisten uhkien havainnointi ja torjunta. Osa näistä hallintakeinoista pätee yhtä lailla myös ulkoisiin uhkiin:

9. Käyttäjien käyttäytymisen analysointi (UBA, User Behaviour Analysis). Erityisesti tähän käyttöön suunniteltuja valvontajärjestelmiä ja ohjelmistoja, jotka seuraavat hyvinkin yksityiskohtaiesti käyttäjän toimintaa tietojärjestelmissä ja etsivät siitä poikkeavaa toimintaa nostaen siitä tarvittaessa hälytyksen. Kehittyneissä UBA järjestelmissä voidaan myös hyödyntää automatiikkaa käynnistämään mahdolliset vastatoimet automaattisesti. UBA:n käytössä tulee huomioida paikallinen lainsäädäntö ja yksityisyydensuoja.

10. Vähimpien oikeuksien periaate. Käyttäjille annetaan vain ne käyttöoikeudet vain siihen tietoon ja tietojärjestelmiin mitä käyttäjä työssään tarvitsee. Lisäksi työtehtävien muuttuessa oikeudet pitää joka kerta muistaa päivittää uutta työtehtävää vastaavaksi.
11. Lokit ja seuranta. Järjestelmien, jotka sisältävät suojeltavaa tietoa, tulee pitää kirjaa tietojen käytöstä vähintään sillä tasolla, että voidaan selvittää kuka, milloin, mistä ja mitä tietoa on käsitelty. Lokitiedot tulee säilyttää tarpeeksi kauan, yleensä arvioidaan, että kolmen vuoden säilytysaika olisi toiminnallisesti järkevä minimi. Lisäksi seurantaa tulisi suorittaa vähintäänkin säännöllisillä pistokokeilla, jos jatkuvaa seurantaa ei teknisesti tai muista syistä voida järjestää. Seurannassa on syytä huomioida kertymävaikutus, joilla voidaan havaita tietojen hidasta varastamista.
12. Tietojen salaus. Sisäpiiriuhan kohdalla tietojen salaus ei välttämättä ole yhtä tehokas suojauskeino, kun ulkoista uhkaa kohden, mutta sitä voidaan erilaisilla sovellutuksilla hyödyntää myös sisäpiiriuhan yhteydessä. Esimerkiksi käytetään dokumenttien luokittelun kautta toimivaa käytön rajaamista ja tiedoston salaamista.
13. Järjestelmien ja verkkojen segmentointi. Segmentointi on enemmän ulkoisen uhan sivuttaista liikettä rajoittava toimi, mutta toimii myös jossakin määrin sisäpiiriuhkaa vastaan luomalla lisäesteitä tiedon luvattomalle käyttämiselle.
14. Siirrettävien tietovälineiden hallinta. Ulkoisten tallennusvälineiden käytön estäminen, rajoittaminen ja valvonta. Pyritään estämään ja havaitsemaan tilanteita, jossa tietoja pyritään siirtämään yrityksestä ulos ulkoista tietovälinettä käyttäen. Ulkoisia tallennusvälineitä voidaan käyttää, kun yritetään välttää esimerkiksi epäilyttävän verkkoliikenteen syntymistä yrityksestä ulospäin.
15. Koulutus. Koulutuksella tässä yhteydessä voidaan tarkoittaa sellaista koulutusta, jossa pyritään tuomaan esille tapoja arvioida oman toimintansa laillisuutta sekä tunnistamaan mahdollisia poikkeamia muiden toiminnassa. Ensimmäiseen kohtaan voidaan sisällyttää myös tapahtumien ketjuuntuminen, esimerkiksi luottamuksellisia asiakirjoja viedään ohjeiden vastaisesti kotiin, jossa ne sitten saattavat altistua ulkopuolisten saataville.
16. Asiakirjojen luokitteleminen. Asiakirjojen luokitteleminen on yksi keskeisimmistä tavoista suojata tietoa. Asiakirjojen luokittelematta

jättäminen, varsinkin jos se on ohjeistettu esimerkiksi tietoturvapolitiikassa, voi johtaa hankaliin juridisiin ongelmiin. Asiakirjoja voidaan luokitella joku manuaalisesti kirjoittamalla niihin niiden luokittelu, tai käyttämällä erityistä järjestelmää sitä varten (esimerkiksi suositussa M365 ympäristössä olevaa Purview labeling ominaisuutta).

17. Arvioinnit ja auditoinnit. Toimintaa ja ohjeiden noudattamista tulee arvioida ja auditoida säännöllisesti ja nämä tulee aina dokumentoida.

9.3 Erityiset riskiryhmät

Yrityksen tulee pyrkiä tunnistamaan omasta organisaatiostaan mahdolliset riksiryhmät, varsinkin korkeariskiset ryhmät ja toimenkuvat. Kartoitus ei saa rajoittua pelkästään kaikista selvimpiin tapauksiin, vaan tätä pitää lähestyä huomattavasti laajemmassa mielessä ja ottaa huomioon ne ryhmät, joilla pääsy tietoihin saattaa perustua muuhun kuin kyseisen tiedon nimenomaiseen käsittelyyn. Esimerkkinä tällaisesta ryhmästä on yrityksen IT osasto, jolla todennäköisesti pääsy kaikkeen yrityksen tietoon, käyttäjätileihin, käyttöoikeuksien muuttamiseen. Näiden lisäksi IT-osastolla työskentelevällä saattaa olla mahdollisuus päästä käsiksi lokitietoihin sekä muuttaa tai poistaa niitä.

Kuten aikaisemminkin mainittu, näitä erityisiä riskiryhmiä kartoitettaessa ja valvottaessa tulee ehdottomasti huomioida kohdehenkilöiden yksityisyydensuoja.

Vaikka nämä tekniset toimenpiteet voivat tarjota suojaa sisäpiirin uhkaa vastaan, on tärkeää myös vahvistaa organisaation turvallisuuskulttuuria, joka tähtää siihen, että kaikki työntekijät ottavat omistajuutta ja toimivat tietoisesti osaamisen ja ymmärtämisen kautta yhtiön edun mukaisesti. Yrityksen pitää myös olla valmiina vastaamaan nopeasti toimintaympäristössä tapahtuviin muutoksiin, joilla saattaa olla vaikutusta sisäpiiriuhkaan.

10 Ei vain kilpailijoiden kesken

On syytä muistaa, että yritysvakoilu ei kohdistu ainoastaan kilpailijoihin tai yrityssalaisuuksien luvatonta hyödyntämistä ei tehdä ainoastaan kilpailijan lukuun. Tätä toimintaa voidaan suorittaa myös toimittaja – asiakassuhteessa, kummastakin suunnasta. Kyseessä saattaa olla suoraan hintoihin ja hinnoitteluun liittyvien tietojen kerääminen tai sellaisen strategisen tai taktisen tiedon kerääminen, jolla pyritään saada etua kaupallisessa toiminnassa.

Asiakkaaseen kohdistuvalla luvattomalla tiedonhankinnalla saatetaan hakea parempaa taloudellista asemaa liikesuhteen optimoimiseksi. Toimittajaa saattaa esimerkiksi kiinnostaa asiakkaan käytettävissä oleva hankintoihin varattu budjetti tai saada selville kilpailijoiden hinnoittelua saadakseen etulyöntiaseman näihin verrattuna.

Yhtä lailla asiakas saattaa haluta kohdistaa luvatonta tiedonhankintaa toimittajaansa kohtaan.

11 Teknologiset trendit ja tulevaisuuden näkymät

Teknologinen muutos, muutoksen nopeus ja teknologinen monimutkaistuminen tuo omat haasteensa tulevaisuudessa yrityksiin kohdistuvassa luvattomassa tiedonhankinnassa ja sitä vastaan taistelemisessa. Tekoälyn, koneoppimisen ja big datan hyödyntäminen tiedonkeruussa luo uusia haasteita, mutta tarjoaa myös mahdollisuuksia parantaa tietoturvaa. Esimerkiksi tekoälyn käyttö käyttäytymisanalyysissä voi auttaa tunnistamaan epätavalliset toimintamallit, jotka viittaavat luvattomaan tiedonhankintaan. Lisäksi blockchain-teknologian[vii] soveltaminen voi lisätä tietojen läpinäkyvyyttä ja turvallisuutta.

Kyberturvallisuuden alueella tulevaisuuden teknologiat, kuten tekoäly ja koneoppiminen, tarjoavat merkittäviä parannuksia. Ne voivat automatisoida uhkien tunnistamista ja vastaamista, mikä tekee suojausjärjestelmistä nopeampia ja tehokkaampia. Toisaalta näitä teknologioita voidaan käyttää myös luvattoman tiedonhankinnan työkaluina, mikä luo uudenlaisia haasteita turvallisuuden ylläpitämiselle.

Blockchain-teknologia, tunnettu parhaiten kryptovaluuttojen yhteydessä, tarjoaa mahdollisuuksia tietojen suojaamiseen. Sen avulla voidaan varmistaa tietojen eheys ja autenttisuus, mikä on erityisen tärkeää arkaluonteisen yritystiedon kohdalla. Blockchainin hajautettu ja läpinäkyvä luonne voi auttaa estämään ja havaitsemaan luvattoman pääsyn tietoihin[viii].

Lisäksi pilvipalvelut ja niiden kehittyvät tietoturvaominaisuudet ovat keskeisessä roolissa yritysten tietoturvassa. Pilvipohjaiset ratkaisut mahdollistavat joustavamman ja skaalautuvamman tietoturvan, mutta ne tuovat mukanaan myös uusia haasteita, kuten tietojen suojaamisen pilvipalveluiden monimutkaisessa ja dynaamisessa ympäristössä.

Näiden teknologioiden rinnalla on tärkeää kehittää myös inhimillisiä tekijöitä: koulutusta, tietoisuuden lisäämistä ja organisaation tietoturvakulttuuria. Teknologia on vain yksi osa kokonaisvaltaista tietoturvaa, ja inhimilliset tekijät ovat yhtä tärkeitä onnistuneessa tietoturvan ylläpidossa.

Yhteenvetona voidaan sanoa, että teknologian nopea kehitys tuo mukanaan sekä mahdollisuuksia että haasteita yritysten tietoturvalle ja sen kautta yritysvakoilun tai luvattoman tiedonhankinnan kohteeksi joutumiselle. Tulevaisuuden näkymät ovat sekä jännittäviä että vaativia, ja yritysten on pysyttävä ajan tasalla sekä teknologian että tietoturvakäytäntöjen osalta, jotta ne voivat suojautua tehokkaasti luvattomalta tiedonhankinnalta.

12 Tapausesimerkki – Meyer Turku

Meyer Turun telakkayhtiöön liittyvä yritysvakoilutapaus[ix] on merkittävä esimerkki liikesalaisuuksien varastamisen vaikutuksista yrityksille. Tämä tapaus alkoi, kun Meyer Turku -telakkayhtiössä työskennellyt mies alkoi varastaa yhtiön liikesalaisuuksia käyttämällä hyväkseen pääsyään yhtiön ja myöhemmin Royal Caribbean -varustamon suojattuihin tietoihin ja tiedostonhallintaohjelmiin. Hänen epäillään kopioineen keskeisiä liikesalaisuuksia ja muita luottamuksellisia tietoja, jotka hän kopio omistamalleen konsulttiyhtiölle, mikä johti oikeudettoman hyödyn saamiseen.

Tämä tapaus herätti huolta yritysvakoilun seurauksista ja tietojen suojaamisen tärkeydestä. Se on esimerkki siitä, kuinka yksittäinen henkilö, jolla on pääsy arkaluonteiseen ja arvokkaaseen tietoon, voi vaikuttaa merkittävästi yrityksen toimintaan ja sen kilpailuasemaan.

Kun tapaus tuli ilmi, Meyer Turku ryhtyi oikeustoimiin vahingonkorvauksien saamiseksi. He vaativat viiden miljoonan euron hyvitystä ja vajaan sadan tuhannen euron vahingonkorvauksia viivästyskorkoineen vuodesta 2017 alkaen sekä oikeudenkäyntikulujen korvaamista. Tämä korostaa, kuinka suuria taloudellisia seurauksia liike- ja yrityssalaisuuksien menettämisellä voi olla.

Valitettavasti syytetty menehtyi tutkinnan aikana, minkä vuoksi oikeudenkäynti keskittyi hänen kuolinpesäänsä ja omistamaansa yritykseen kohdistettuihin vaatimuksiin.

Käräjäoikeuden käsittelyssä oli keskeinen kysymys siitä, olivatko kopioidut tiedostot luonteeltaan liikesalaisuuksia. Tämä herättää laajempia kysymyksiä siitä, miten liikesalaisuuksia määritellään ja suojataan, ja kuinka yritykset voivat varmistaa tietojensa turvallisuuden nykyisessä digitaalisessa ja verkottuneessa liiketoimintaympäristössä. Alun perin syyttäjä olikin vaatinut tuomiota tekijänoikeusrikoksesta ja liikesalaisuuden väärinkäytöstä. Vasta myöhemmin syyteisiin yritysvakoilu.

Oikeudenkäynnille varattiin seitsemän päivää lopussa, mikä osoittaa tapauksen monimutkaisuutta ja sen merkitystä laajemminkin. Meyer Turun tapaus on näyttänyt yrityksille sen, kuinka tärkeää on suojata liikesalaisuudet ja olla valppaana mahdollisten sisäisten uhkien suhteen. Tämän lisäksi tässä tapauksessa on korostunut myös sisäpiiriuhan merkittävyys.

13 Johtopäätös

Riskienhallinta ja -tiedostaminen on keskeinen lähtökohta kamppailtaessa yritysvakoilua vastaan. Sen huomioimisen tulee olla kiinteä ja pysyvä osa yrityksen riskienhallintaa. Sille täytyy osata ja uskaltaa laske vaikuttavuus ja todennäköisyydet aivan samalla tavalla kuin muillekin riskeille. Yritysvakoilu ja varsinkin yrityssalaisuuksien väärinkäyttäminen on todellisuutta, jota tapahtuu jatkuvasti.

Kaiken luvattoman tiedonhankinnan estäminen saattaa käytännössä olla mahdotonta, joten senkin kohdalla olisi syytä harkita painopisteen siirtämistä kyberturvallisuuden oppien mukaisesti havaitsemiseen ja toipumiseen ja näiden kautta rajata niiden vaikutusta mahdollisimman pieneen.

Suomessa on useita tahoja, jotka kouluttavat ja antavat tietoa yritysvakoilusta, esimerkiksi Kauppakamarit, joilta on saatavilla niin ohjeita[x] kuin tutkimustuloksia.

Koska ihmisen rooli on kiistatta edelleenkin keskeinen luvattoman tiedonhankinnan ja yritysvakoilun torjumisessa, tulee siihen suhtautua myös sen mukaisesti. Yhtenä osana tätä on henkilökunnan, kumppaneiden, asiakkaiden ja muiden sidosryhmien tietoisuuden lisääminen aiheesta yleisellä tasolla ja varsinkin kohdennetusti. Jos toimijalla on tiedossa selkeitä kohonneita riskitekijäitä, tulee nämä tuoda mahdollisimman avoimesti esille koulutuksissa ja ohjeistuksessa.

Ongelmana tietoisuuden lisäämisessä saattaa olla se, että tuomalla esille mahdollisia tunnistettuja ongelmakohteita, saatetaan tällä antaa mahdolliselle vihamieliselle toimijalle arvokasta tietoa oman vakoilu- ja tiedonhankintatoimintansa tueksi. Eli tässäkin tulee tasapainotella hyötyjen ja riskien välillä. Tietoisuuden lisäämisen tulee perustua selkeisiin konkreettisiin ja kohderyhmän todelliseen tekemiseen ja aihepiireihin liittyviin asioihin, mutta sen tulee

toisaalta pystyä muotoilemaan niin, että se toimi suoranaisena ohjekirjana laitonta toimintaa harjoittavalle taholle.

Ongelma ei ole puhtaasti tekninen, eikä puhtaasti inhimilliseen puoleen liittyvä, eikä se myöskään ole enää nykyään sidottu aikaan eikä paikkaan. Ongelma itsessään pitää sisällään ”tuntemattomia tuntemattomia” tekijöitä ja pakottaa riskeiltä suojautujan huomioimaan niin teknologisen kehityksen nopeuden ja arvaamattomuuden kuin rajut muutokset geopolitiikassa ja pandemioiden luomat mustat joutsenet.

Onko ongelma ratkaistavissa? Todennäköisesti ei, mutta sen vaikutusta voidaan rajata päättäväisellä ja jatkuvasti kehitettävillä taktiikoilla ja tekniikoilla. Taktiikoiden ja tekniikoiden lisäksi yritysvakoilun ja luvattoman tiedonhankinnan torjuminen pitäisi edes jollakin tasolla sisältyä yhtiön strategiaan, jos yrityksellä on missään määrin sellaista informaatio-omaisuutta tai -pääomaa, joka voisi kiinnostaa luvatonta tiedonhankintaa toimintamallinaan käyttävää tahoa. Vaikka yrityksen strategiassa ei suoraan otettaisikaan kantaa tähän aiheeseen, tulee sen sisältyä yrityksen turvallisuusstrategiaan.

14 Pohdintoja

Vakoilu ja sen kautta yritysvakoilu on ikiaikainen ongelma ja ilmiö joka ponnisteluista huolimatta ei osoita vähenemisen merkkejä. Päinvastoin voisi enneminkin sanoa, että vakoilu on tietoyhteiskunnassa entistäkin keskeisemmässä roolissa niin sitä suorittavien ja siitä hyötyvien kannalta kuin siltä puolustautuvienkin kannalta. Internetin tuoma 247 globaalius luo sille otollisen alustan.

Samalla toki tulee pitää mielessä, että yritysvakoilu voi edelleen tapahtua myös fyysisessä maailmassa tai vähintäänkin hybridimallina, joka hyödyntää sekä digitaalisuutta että fyysistä maailmaa.

Covidin jälkeinen etätyömaailma luo lisäksi omat haasteensa, kun luottamuksellistakin tietoa on pakko sallia käsiteltäväksi muuallakin kuin perinteisellä toimistolla. Tämä luo uudenlaisia uhkamalleja, tai korostaa vanhoja uudella tavalla. Käsitelläänkö luottamuksellista materiaalia kotokonttorilla käyttäen riittäviä toimintamalleja ja kontrolleja vai voiko materiaali päätyä muiden perheenjäsenten, tuttujen tai vaikka asunnossa vierailevan huoltomiehen saataville tahattomasti luoden näin ”tilaisuus luo varkaan” tilanteen. Tai vakavimmissa tapauksissa, voidaanko ulkopuolisen toimijan taholta helpommin kohdistaa toimenpiteitä kotikonttoria vastaan?

Luvattomaan tiedonhankintaan tulee varautua kuten muihinkin riskeihin, myös sisäpiirin kautta tulevaan riskiin, vaikka se ehkä saattaa tuntua organisaation sisällä kiusalliselta aiheelta. Tähän liittyvät riskit tulee kartoittaa ja käydä läpi säännöllisesti muun riskienhallinnan yhteydessä.

Geopoliittinen jännittyneisyys lännen ja idän välillä ja sen luoma polarisaatio on syventynyt viime vuosina, ja tämä kehitys on saanut uusia ulottuvuuksia COVID-19-pandemian ja Venäjän Ukrainaan kohdistaman täysimittaisen hyökkäyssodan myötä. Näiden tapahtumien aiheuttamat globaalit muutokset ovat luoneet otollisen maaperän yritysvakoilun uusille muodoille, joissa perinteiset geopoliittiset linjaukset ja lojaliteetit ovat entistä kovemmassa myllerryksessä ja sitä kautta myös merkittävämmässä roolissa.

Intian ja Venäjän välisen suhteen tiivistyminen on yksi esimerkki geopoliittisesta liikkeestä, joka herättää huolta länsimaissa. Intian kasvava taloudellinen ja sotilaallinen yhteistyö Venäjän kanssa voi johtaa uusiin turvallisuusuhkiin, jotka ovat "tuntemattomia tuntemattomia" länsimaiden kannalta. Tämä tarkoittaa, että mahdolliset uhat eivät ole pelkästään ennakoimattomia vaan saattavat ilmetä täysin odottamattomilla tavoilla, esimerkiksi kyberturvallisuuden alueella tai kansainvälisen kaupan mekanismeissa. Ottaen huomioon kuinka iso osa länsimaiden IT- järjestelmistä on riippuvaisia intialaisten yritysten tuottamista kehitys- ja ulkoistuspalveluista, tulee länsimaisten yritysten herätä tähän riskiin myös yritysturvallisuuden näkökulmasta mukaan lukien luvaton tiedonhankinta.

Tällainen epävarmuus ja arvaamattomuus vaativat yrityksiltä ja hallituksilta uudenlaista valppautta ja joustavuutta. Kun idän ja lännen väliset jännitteet kärjistyvät, yritykset, jotka toimivat globaalisti, voivat joutua yhä monimutkaisempien vakoiluoperaatioiden kohteiksi.

Lisäksi Intian ja Venäjän lähentyminen voi rohkaista muita valtioita muodostamaan uudenlaisia liittoutumia, mikä entisestään monimutkaistaa kansainvälistä turvallisuusympäristöä. Tämä geopoliittinen kehitys voi luoda uusia haasteita tiedonvaihdolle ja yhteistyölle turvallisuuskysymyksissä, kun luottamus perinteisten liittolaisten välillä joutuu koetukselle.

Yritysten on tässä ympäristössä elettävä jatkuvassa muutoksen tilassa, jossa kyky ennakoida ja reagoida nopeasti uusiin uhkiin nousee kriittiseksi menestystekijäksi. Tämä vaatii syvällistä ymmärrystä paitsi teknologisista ja operatiivisista riskeistä myös laajemmasta geopoliittisesta kontekstista. Yritysten turvallisuusstrategioiden on nyt enemmän kuin koskaan oltava dynaamisia ja mukautuvia, pystyen vastaamaan nopeasti ja tehokkaasti sekä tunnettuihin että tuntemattomiin turvallisuusuhkiin.

Näiden kehityskulkujen valossa on selvää, että yritysten ja valtioiden on yhä tärkeämpää tehdä yhteistyötä sekä keskenään että kansainvälisten kumppaneiden kanssa. Tämä yhteistyö voi auttaa luomaan kattavampaa tilannekuvaa ja parantamaan valmiuksia vastata monenlaisiin turvallisuushaasteisiin, jotka ilmenevät tässä jatkuvasti muuttuvassa ja polarisoituneessa maailmassa.

15 Viitteet

Finlex, KKO ennakkopäätös Yritysvakoilu Yrityssalaisuuden rikkominen Rikoksen yritys, 2013, https://finlex.fi/fi/oikeus/kko/kko/2013/20130020

Andrew Crane, In the company of spies: When competitive intelligence gathering becomes industrial espionage, 2005, https://www.sciencedirect.com/science/article/abs/pii/S0007681304001302?via%3Dihub

D. Zatonatskiy, V. Marhasova, and N. Korogod, “INSIDER THREAT MANAGEMENT AS AN ELEMENT OF THE CORPORATE ECONOMIC SECURITY”, ФКДПТП, vol. 1, no. 36, pp. 149–158, Feb. 2021.

I. Hilmi Elifoglu, Ivan Abel, Özlem Tasseven, Minimizing Insider Threat Risk with Behavioral Monitoring, 2018, S. 61-73, https://www.stjohns.edu/sites/default/files/uploads/review-of-business-382-june_2018.pdf

Hakonen Petri, Detecting Insider Threats Using User and Entity Behavior Analytics, 2022, S. 29, https://www.theseus.fi/bitstream/handle/10024/786079/Thesis_Hakonen_Petri_YTC21S1.pdf?sequence=2&isAllowed=y

Tara Seals, Threatlist: Targeted Espionage-as-a-Service Takes Hold on the Dark Web, 2019, https://threatpost.com/espionage-as-a-service-dark-web/145464/

Trend Micro, Espionage as a Service Cybercrime-as-a-Service Series, 2016, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/espionage-as-a-service-a-means-to-instigate-economic-espionage

Laki, Luettelon ja tietokannan valmistaja, https://www.finlex.fi/fi/laki/ajantasa/1961/19610404#L5P49

Minilex, Rikoksen tekopaikka voi olla siellä missä seuraus ilmeni, https://www.minilex.fi/a/rikoksen-tekopaikka-voi-olla-siell%C3%A4-miss%C3%A4-seuraus-ilmeni

EY McCavitt, Wolfe, How OSINT is valuable to threth monitoring and investication, 2023, https://www.ey.com/en_us/forensic-integrity-services/value-of-osint-to-threat-monitoring-and-investigations

SC Media, Levy, Corporate data breach detection through an OSINT lens, 2023, https://www.scmagazine.com/perspective/corporate-data-breach-detection-through-an-osint-lens

US Naval War College, Intelligence Studies: Human Intelligence (HUMINT), https://usnwc.libguides.com/c.php?g=494120&p=3381553#:~:text=Human%20Intelligence%20(HUMINT)%20is%20intelligence,(NATO%20Glossary%20of%20Terms)

Panu Vesterinen, Estä yritysvakoilu – uusi ohje yrityksille urkinnan estämiseen, 2021, https://helsinki.chamber.fi/esta-yritysvakoilu-uusi-ohje-yrityksille-urkinnan-estamiseen/

Helsingin seudun kauppakamari, Yritysvakoiluselvitys 2021, 2021, https://helsinki.chamber.fi/wp-content/uploads/2021/05/yritysvakoiluselvitys_kevat2021.pdf