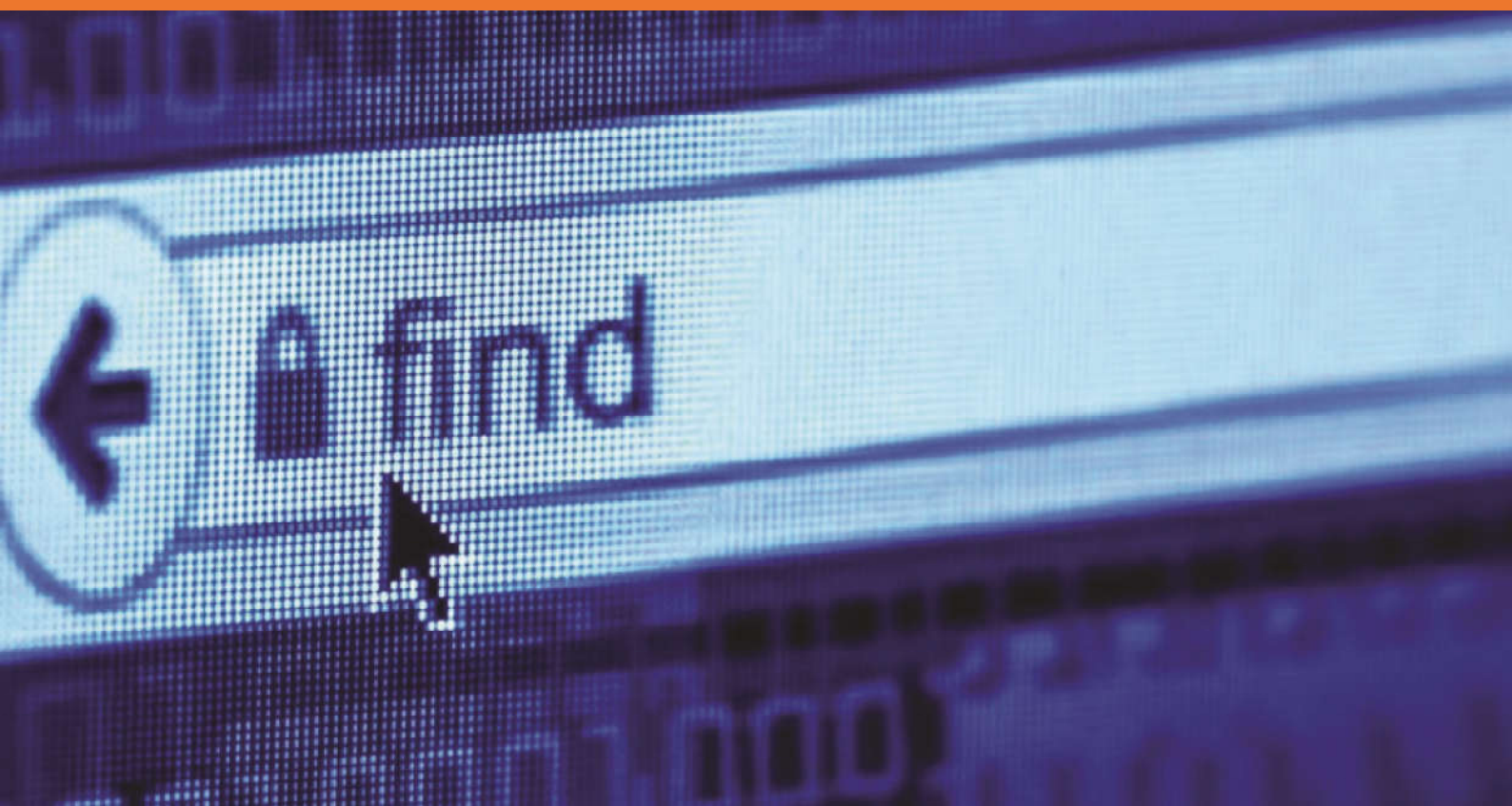
Kybervakoilu

– Mitä jokaisen yrityksen tulisi tietää?



Kybervakoilu – mitä jokaisen yrityksen tulisi tietää?

- ☑ **Kybervakoilu on kasvava haaste digitalisoituneelle yhteiskunnalle. Digitaalinen maailma mahdollistaa tietojen tehokkaan keräämisen ja analysoinnin. Yrityksiä ja ihmisiä voidaan profiloida erittäin kattavasti.**
- ☑ **Yritysvakoilun teho on parantunut merkittävästi ja sen tunnistaminen on entistä vaikeampaa kybermaailman luomien uusien mahdollisuuksien ansiosta.**
- ☑ **Yritysvakoilun kohteena ovat edelleen yrityssalaisuudet, käyttäjä- ja asiakastiedot, talous- ja markkinointitiedot. Vakoilu voidaan naamioida satunnaiseksi hakkeroinniksi tai haittaohjelmaksi.**
- ☑ **Valtiollisen vakoilun, tiedustelun ja hakkeroinnin raja on entistä häilyvämpi.**
- ☑ **Verkkosivuseuranta, sosiaalisen median palvelut ja älypuhelimet sovelluksineen tarjoavat ennennäkemättömät mahdollisuudet henkilöiden vakoiluun, seurantaan ja analysointiin.**
- ☑ **Kybervakoilulta suojautumisessa tärkeintä on tunnistaa uhat ja suojattavat kohteet.**
- ☑ **Henkilöihin liittyvät riski korostuvat ja uusia toimintatapoja tarvitaan (Insider threat).**
- ☑ **Tiedon eheyden seurannan merkitys korostuu.**

Sisällysluettelo

Kybervakoilu näkyy arjessamme

"Helsingin kaupungin tietojärjestelmässä oli laaja häiriö: terveysasemat sekaisin, metro- ja raitiovaunuliikenteessä ongelmia, lipunmyynti takkusi" YLE, 16.5.2018

Tuttu ja tavallinen uutinen meille, mutta tietolähde vakoilu- ja tiedusteluorganisaatioille?

Tapaus kuvaa potentiaalisen tiedustelutiedon muodostumisesta arkipäivän median välityksellä. Oletko ajatellut, että tietojen perusteella voidaan muodostaa ymmärrystä esimerkiksi kriittisten valokuituyhteyksien sijainnista, operaattoreista, vaikutusten laajuudesta, keskinäisriippuvuuksista sekä mahdollisesti palveluiden käyttämästä tekniikasta ja palveluntarjoajista. Vaikka yksittäinen tieto itsessään ei olisikaan kovin merkittävä, se voi sopivassa asiayhteydessä muodostaa hyvinkin arvokasta lisätietoa.

Tiedusteluorganisaatiot voivat käyttää avointa tietoa täydentämään omia analyysejaan tai niitä varmentavana tietona. Näin voidaan myös tiedostamatta tarjota tiedusteluorganisaatioille uusia kohteita, joihin tiedustelutoimintaa tulee kohdentaa.

Taktisella tasolla kiinnostavia tietoja voivat olla esimerkissä valokuituyhteydet ja niiden sijainnit.

Operatiivisella tasolla kiinnostavia voivat olla kaupungin toiminnassaan käyttämät palveluntarjoajat, heidän vasteaikansa, palvelujen mahdollisesti puutteellinen kahdennus, vian vaikutukset eri kaupungin palveluihin (kertoo taustalla olevista infrastruktuuriratkaisuista), kaupungin oman henkilöstön vasteajat, käytetyt kriisiviestinnän kanavat tai tavat minimoida ongelman vaikutuksia.

Strategisella tasolla puolestaan kiinnostavaa voisi olla tarkastella, missä kulkevat kaupunginjohdon, aluehallinnon, valtionhallinnon eri organisaatioiden puuttumiskynnykset ja miten asioihin puututaan, ketkä ovat keskeisiä toimijoita ja mitkä ovat vasteajat. Lisäksi pidemmällä aikavälillä voisi olla kiinnostavaa seurata, miten havaittuja ongelmia korjataan vai korjataanko ollenkaan. Tämä kertoisi myös kohteen riskitietoisuudesta. Kiinnostavaa olisi myös, miten palveluja tuottavat yritykset toimivat häiriötilanteissa ja mikä on niiden kriisinsietokyky.

Kybervakoilu haastaa koko yhteiskuntaa

Kybervakoilu on kasvava haaste digitalisoituneessa yhteiskunnassa. Meistä kerätään jatkuvasti valtavat määrät tietoa, halusimme sitä tai emme. Käytännössä kaikesta tekemisistämme verkossa jää ainakin jonkinlainen jälki. Tämä digitaalinen jalanjälki saattaa toimia kanavana kybervakoiluille, kohdennetuille tietoverkko-operaatioille tai sitä voidaan hyödyntää vaikkapa vaalituloksiin vaikuttamisen välineenä.

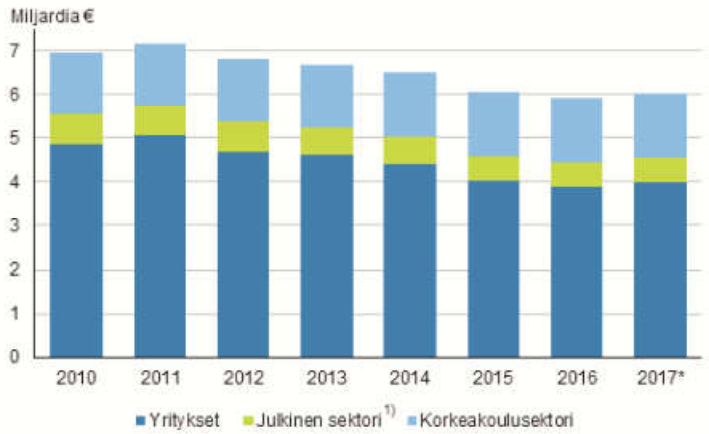
Kybervakoilu on vakava uhka suomalaiselle tietopääomalle. Jos tuotekehitystiedot varastetaan toiseen maahan, yritys voi menettää koko tulevaisuutensa, sanoo Suojelupoliisin päällikkö **Antti Pelttari.** Supo myös muistuttaa, että yritysten turvallisuuden merkitys yhteiskunnalle on kasvanut, sillä kriittinen infrastruktuuri on monin osin yksityisessä omistuksessa ja operoinnissa.

Yhdysvaltojen viranomaisten mukaan Yhdysvalloissa kyberhyökkäysten aiheuttamat menetykset maan taloudelle olivat vuonna 2016 57–109 miljardia dollaria eli 46–88 miljardia euroa.[1] Suomen valtion budjetti vuodelle 2018 on arviolta 55 miljardia. Suomi panostaa vuosittain T&K toimintaan noin kuusi miljardia euroa, josta yritysten osuus on noin neljä miljardia euroa.[2] Globaalien suuryritysten tutkimus-, tuotekehitys- ja innovaatiobudjetit ovat tähän verrattuna huimia. Esimerkiksi kiinalainen verkkokauppa Alibaba aikoo panostaa seuraavan kolmen vuoden aikana reilu 13 miljardia euroa tutkimukseen ja kehitykseen.[3]

Innovaatio-, tutkimus- ja kehittämistoiminta on tärkeä osa yrityksen uudistumista. Ilman kehitystyötä ja osaavaa henkilökuntaa yrityksellä ei ole eväitä kasvuun, joka mahdollistaa menestymisen myös tulevaisuudessa. Kuinka paljon tästä investoinnista valuu hukkaan erilaisten tietovuotojen ja yritysvakoilun vuoksi? Finnish Information Security Clusterin (FISC) arvion mukaan globaalin kyberrikollisuuden kustannukset maailman markkinoille ovat jo nyt biljoonan[4] dollarin luokkaa. Vuoteen 2021 mennessä lisääntyvän IoT-markkinan ja sen tarjoamien uusien mahdollisuuksien myötä kyberrikollisuuden kustannusten arvioidaan jopa kuusinkertaistuvan. Iso osa tästä on valtiollisen kybervakoilun ja järjestäytyneiden kyberrikollisten aiheuttamia kustannuksia.

Viranomaisten mukaan vuoden 2017 aikana tuli esiin useita tapauksia, joissa oli ilmeistä, että yritykseen kohdistuvan vakoilun taustalla oli jokin valtiollinen toimija. Erityisiä kiinnostuksen kohteita ovat ulko- ja turvallisuuspolitiikkaan liittyvät salaiset tiedot sekä **suomalainen korkea teknologia ja tuotekehitys.** Verkottuneessa maailmassa hyökkäys on helppo toteuttaa mistä tahansa Suomen rajojen ulkopuolelta: näin on helppo hankkia suuri määrä tietoja kiinni jäämisen riskin jäädessä pieneksi.

TUTKIMUS- JA KEHITTÄMISTOIMINNAN MENOT SEKTOREITTAIN (stat.fi)



1 https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

2 https://www.stat.fi/til/tkke/2016/tkke_2016_2017-10-26_tie_001_fi.html

3 https://techcrunch.com/2017/10/10/alibaba-group-will-invest-15b-into-a-new-global-research-and-development-program/

4 Luku EU SI-järjestelmän mukainen biljoona (1012), joka vastaa lukua US triljoona (1012)

Mitä jokaisen yrityksen tulisi tietää kybervakoilusta?

Monilla kybermaailman tapahtumilla on myös vakoillullinen merkitys, sillä ne tuottavat aina uutta tietoa kohteesta, sen haavoittuvuuksista tai turvallisuuden tasosta. **Yritysten näkökulmasta on aina huolestuttavaa, kun tietoa katoaa tai yrityksen tietojärjestelmissä on jälkiä ulkopuolisen toiminnasta.** Yksittäinen tietovuoto tai hakkerointi on voitu naamioida näyttämään satunnaiselta kyberrikollisten toiminnalta, mutta kyseessä saattaa olla osa laajempaa kohdistettua vakoiluoperaatiota.

On hyvin todennäköistä, että yrityksesi joutuu vakoilijan kohteeksi mikäli:

- **Yrityksesi on potentiaalinen ostokohde**
- **Yrityksellläsi on syvää erityisosaamista**
- **Yrityksesi hallussa on turvallisuuskriittistä tietoa**
- **Yrityksesi toimii merkittävässä roolissa yhteiskunnan häiriöttömän toiminnan kannalta tai on tällaisen yrityksen tai viranomaisen yhteistyökumppani**

Vakoilu on ammattimaista ja läpitunkevaa. Yritysvakoilu on suunnitelmallista toimintaa. Se kattaa yrityksen koko liiketoiminnan aina julkisista tiedoista ulottuen tekniikkaan, tuotteisiin, prosesseihin, jakelukanaviin ja ihmisiin.[5] Kybervakoilu lisää yritysvakoilun keinovalikoimaa ja mahdollistaa, jopa kohteen reaaliaikaisen seurannan.

Yrityksissä voidaan ajatella, ettei kukaan ole kiinnostunut heidän yrityssalaisuuksistaan. Tämä puolestaan näkyy siinä, ettei kyberturvallisuuteen panosteta tai esimerkiksi tuotekehityksen turvaaminen ja valvonta jäävät heikoksi. Ei ole olemassa epäkiinnostavaa kohdetta kyberhyökkäyksille. Kaikki tieto voi olla haluttua. Erityisesti kiinnostaa se, jolla on kyberrikollisille jälleenmyyntiarvoa tai tieto, jolla on merkitystä globaalissa kilpailussa.

Minulla itselläni ole mitään salattavaa – vaarallinen ajatus! Hakkerit ja erityisesti valtiollisen tason toimijat ovat entistä ovelampia ja kyvykkäämpiä hyödyntämään ihmisten välinpitämättömyyttä ja heidän käyttämissään laitteistoissa olevia haavoittuvuuksia. Tämä heijastuu myös yritysten toimintaan erityisesti henkilöstön jokapäiväisen toiminnan kautta.

Älypuhelimet ja niiden sovellukset ovat erittäin suosittuja vakoilukohteita. Älypuhelinten seurantaa suorittavat useat eri tahot. Esimerkiksi Google on myöntänyt keränneensä kaikkien Android-puhelinten sijaintitiedot haltuunsa, vaikka tämä olisi estetty puhelimen asetuksista.[6] Joistakin puhelimista on löydetty myös tehdasasennettuja takaportteja[7]. Tämän lisäksi on lukematon määrä erilaisia sovelluksia, jotka mahdollistavat käyttäjien seuraamisen[8], salakuuntelun tai katselun. Sovellukset voivat jakaa tietoa puhelimen käytöstä ohjelmistovalmistajille tai muille kaupallisille toimijoille, mutta myös hakkereille tai jopa valtiollisille toimijoille[9].

Sosiaaliset verkostot ja vuorovaikutus kiinnostavat. Sosiaalisen median palvelut ja ihmisten keskinäinen viestintä ovat tärkeässä asemassa etsittäessä avainhenkilöitä tai väyliä heihin vaikuttamiseen. Myös pikaviestipalveluiden mobiilisovellutukset ovat tuoneet ennennäkemättömän helpon ja laajan kanavan henkilöiden kohdentamiseen ja seurantaan. Vaikka viestit ja viestiliikenne olisivat päästä päähän salattuja, paljastavat viestiliikenteen ns. metatiedot hyvin paljon vakoilun kannalta tärkeää tietoa (kuka, kenen kanssa, milloin, missä, kuinka usein, ketä muita on samassa paikassa tai keskusteluryhmässä, jne.).

Algoritmit voivat tuntea sinut paremmin kuin omat läheisesi. Verkkopalveluiden seuranta, hakupalveluiden historiatiedot, verkkokauppojen ostoskäyttäytyminen, sosiaalisen median profilointi täydentävät yhdessä digitaalista jalanjälkeä, jonka hyödyntäminen perustuu algoritmeihin.[10] Tietoa käytetään pääasiassa mainonnan ja viestinnän kohdentamiseen, mutta kannattaa muistaa, että tieto voi toimia kanavana myös kybervakoiluille.

5 https://www.defenseone.com/technology/2018/05/spies-are-going-after-us-supply-chains-intel-agencies-say/148264/
6 https://thehackernews.com/2017/11/android-location-tracking.html
7 https://www.engadget.com/2017/11/14/oneplus-leaves-backdoor-on-phones/
8 https://www.tivi.fi/Kaikki_uutiset/supersuosittu-sovellus-vakoilee-kayttajaa-paljastaa-tarkan-sijainnin-vaikka-toiminnon-kytkisi-pois-paalta-6670979
9 https://www.tivi.fi/Kaikki_uutiset/kiina-pakottaa-muslimivahemmiston-asentamaan-puhelimiinsa-vakoilusovelluksen-tottelemattomia-uhkaa-pidatys-6664507
10 https://yle.fi/uutiset/3-10097475

Tiedustelua, yritys- ja kybervakoilua vai markkina-analyysiä?

Tieto on yhä useammin yrityksen tärkeintä pääomaa. Olemassa olevaa tietoa on mahdollista jalostaa erilaisin työkaluin ja jopa tekoälyavusteisesti, jolloin voidaan synnyttää kokonaan uutta tietoa ja liiketoimintaa.

Avoin data[11] tarjoaa lisääntyvässä määrin julkisesti tietoa, jota aikaisemmin ei ollut saatavilla kuin vakoilun keinoin. Avoin data toimii perustana monille julkisille palveluille ja luo paljon uusia liiketoimintamahdollisuuksia. Valitettavasti avoin tieto toimii hyvänä tietokanavana myös rikollisiin tai vakoilutarkoituksiin.

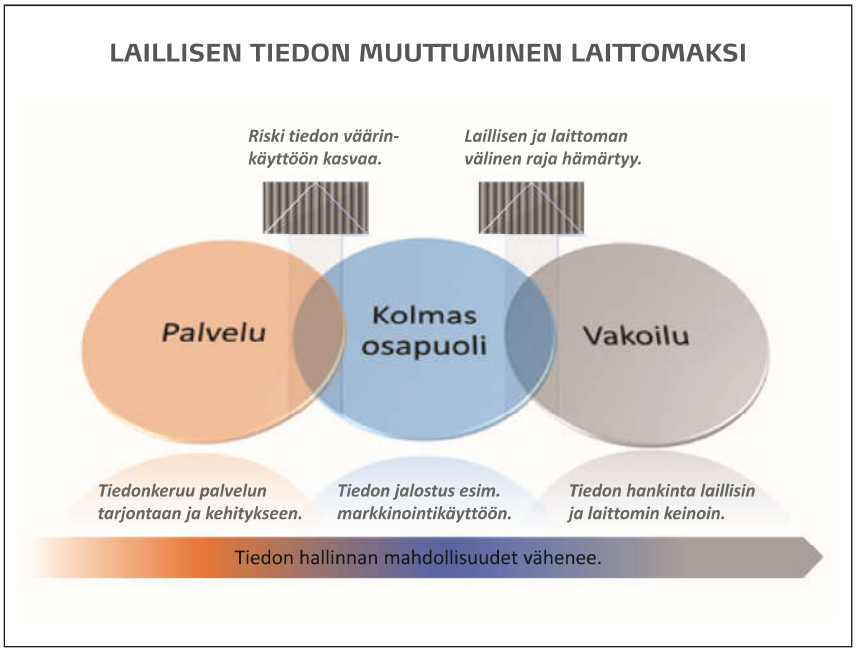
Yritysten julkiset tiedot kertovat paljon. Pelkästään yritysten julkisesti saatavilla olevista perustiedoista, taloudesta, henkilöistä, palveluista ja tuotteista saa varsin laajan ja tarkan yleiskuvan organisaatiosta ja sen tilanteesta. Yrityksen itse julkaisemia tietoja seuraamalla ja analysoimalla voi saada hyvin yksityiskohtaista tietoa yrityksestä, sen käyttämistä teknisistä ratkaisuista tai tulevaisuudensuunnitelmista. Esimerkiksi organisaation visio ja strategia yhdistettynä työpaikkailmoituksiin voi tuottaa vakoilijalle käyttökelpoista tietoa. Tämän lisäksi avoimet kaupalliset tutkimukset ja markkinointikatsaukset voivat tarjota arvokasta analyysiä yrityksen toimialasta, markkinoista tai itse yrityksestä. Näitä tietoja yhdistelemällä voidaan muodostaa varsin kattava kuva yrityksen toiminnasta, joka taas voidaan hyödyntää yritysvakoilussa tai sen valmistelussa.

Missä menee raja? Verkkopalveluiden kävijäseuranta ja analyysit sekä sosiaalisen median kautta saattavat tiedot ovat iso liiketoiminnan alue, joka mahdollistaa eri tietolähteiden yhdistämällä hyvin tarkkojen henkilö- ja yritysprofiloinnin muodostamisen.[12] Käytännössä joskus voi olla vaikea erottaa, missä kulkee kävijäanalyysin, kohdennetun markkina-analyysin, yritysanalyysin ja yritysvakoilun raja. Tällainen tietojenkeruu on vaikeasti määriteltävissä ja valvottavissa. Yhtä lailla jaottelu vakoilun ja tiedustelutoiminnan välillä on haastavaa. Yhden tiedustelutoiminta voi olla vastapuolelle rikollista vakoilua. **Oleellista kuitenkin on, käytetäänkö laillisia vai laittomia keinoja ja mikä on toiminnan tavoite.**

Oletko itse osa tiedustelun ekosysteemiä? Tuotatko tietämättäsi arvokasta vakoilutietoa rikollisille tai ulkomaisille valtiollisille toimijoille?

11 https://www.avoindata.fi/fi
https://www.europeandataportal.eu/data/en/organization

12 http://crackedlabs.org/en/corporate-surveillance/
https://yle.fi/uutiset/3-10097475



Markkina-analyysi, -kartoitus tai -tutkimus tarkoittaa yleisesti markkinan järjestelmällistä analysointia ja yritystä ymmärtää sitä. Haetaan siis kuluttajien preferenssejä, kulutustottumuksia, toiminnan ja käyttäytymisen motiiveja ja pyritään löytämään haluttuja kohderyhmiä, joihin markkinointitoimet kohdistetaan.

Yritysanalyysi pyrkii luomaan kattavan kuvan liiketoiminnan nykytilasta, tulevaisuuden suunnasta, mahdollisista strategiavaihtoehdoista ja kehittämismahdollisuuksista.

Yritysvakoilulla tarkoitetaan tarkoitushakuista, laillista ja laillisen toiminnan harmaalle alueelle ulottuvaa sekä usein myös laittomia tiedonhankintakeinoja hyväksikäyttävää toimintaa. Kyberulottuvuuden kehittymisen myötä vakoilun keinovalikoimat ovat lisääntyneet ja yritysvakoilu on muuttanut luonnettaan pitkäkestoisista projekteista jatkuvaksi, jopa reaaliaikaiseksi seurannaksi.

Kybervakoilulle ei ole olemassa kansainvälisesti hyväksyttyä määritelmää. Toiminnallisesti tarkasteltuna ja noudattaen yleisiä tiedustelumaailman periaatteita se voidaan määritellä seuraavasti: hankitaan ei-julkisia ja salaisia tietoja yksityisiltä ihmisiltä, kilpailijoilta, ryhmiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen laillisia tai laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa, sosiaalisessa mediassa tai laitteissa. Samalla myös julkisille tiedoille voidaan saada varmistuksia tai rikastaa aiemmin kerättyä tietomassaa uusilla tiedoilla, jotka eivät itsessään välttämättä ole mitenkään salaisia. Niiden yhdistelmät huolellisesti analysoituina kuitenkin voivat tuottaa merkittävää lisäarvoa tiedustelua suorittavalle toimijalle – tai joskus jopa tahallista merkittävää vahinkoa kohteeksi joutuneelle taholle. Monet valtiot pitävät kybervakoilua itsessään jo kyberhyökkäyksenä, johon on vastattava aktiivisilla toimilla. Kansainvälinen asenne kyberhyökkäyksiä kohtaan on tiukentumassa.

Kybertiedustelu on julkisiin ja ei-julkisiin lähteisiin kohdistuvaa tiedonhankintaa, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhista, riskeistä ja muutoksista niin maan sisällä kuin rajojen ulkopuolella. Tiedustelutoiminnan tavoitteena on tuottaa varhaisvaiheen tietoa, joka mahdollistaa uhkiin, riskeihin ja muutoksiin vaikuttamisen ja varautumisen. Tiedusteluun kuuluu tiedon analysointi, jonka avulla erilaisia turvallisuusympäristön epävarmuustekijöitä pyritään jäsentämään.

Valtioiden tiedustelutoiminnan tulisi noudattaa kansallista lainsäädäntöä ja toiminnalla on usein myös poliittisen johdon hyväksyntä. Se mikä meille on laitonta ja poliittisesti tuomittavaa, voi hyvin olla toisessa maassa täysin laillista ja poliittisesti perusteltua toimintaa. Tästä syystä erot kansallisessa lainsäädännössä ja poliittisessa tahtotilassa asettavat valtiot ja niissä toimivat yritykset keskenään erilaiseen asemaan. Siksi monet valtiolliset toimijat ovatkin ulottaneet kybervakoilun kaupallisten toimijoiden keräämiin ja analysoimiin tietomassoihin. Tästä viimeisimpänä esimerkkinä on ns. Cambridge Analytica tapaus.[13]

Kyberrikollisten ensisijainen tavoite on kerätä tietoja, jotka ovat myytävissä tai käytettävissä hyväksi varsinaisissa kyberhyökkäyksissä. Monet valtiolliset toimijat käyttävät hyväksi kyberrikollisten tuottamia kybervakoilupalveluja tai hakkeriryhmiä tekemään operatiivisia hyökkäyksiä, vaikka tätä on hyvin vaikea näyttää toteen. Tässä toiminnan tavoitteella on suuri merkitys. Usein vakoilun, kehittyneen kyberhyökkäyksen ja tavanomaisen kyberrikoksen alkuvaiheet muistuttavat toisiaan, jolloin puolustajan on hankala arvioida, onko vastapuoli keräämässä tietoja vai valmistelemassa mekanismeja tulevaa kyberoperaatiota varten. Kyberrikollisuus on nykyisin kietoutunut tiiviisti muuhun kansainväliseen järjestäytyneeseen rikollisuuteen.

13 https://www.theguardian.com/news/series/cambridge-analytica-files

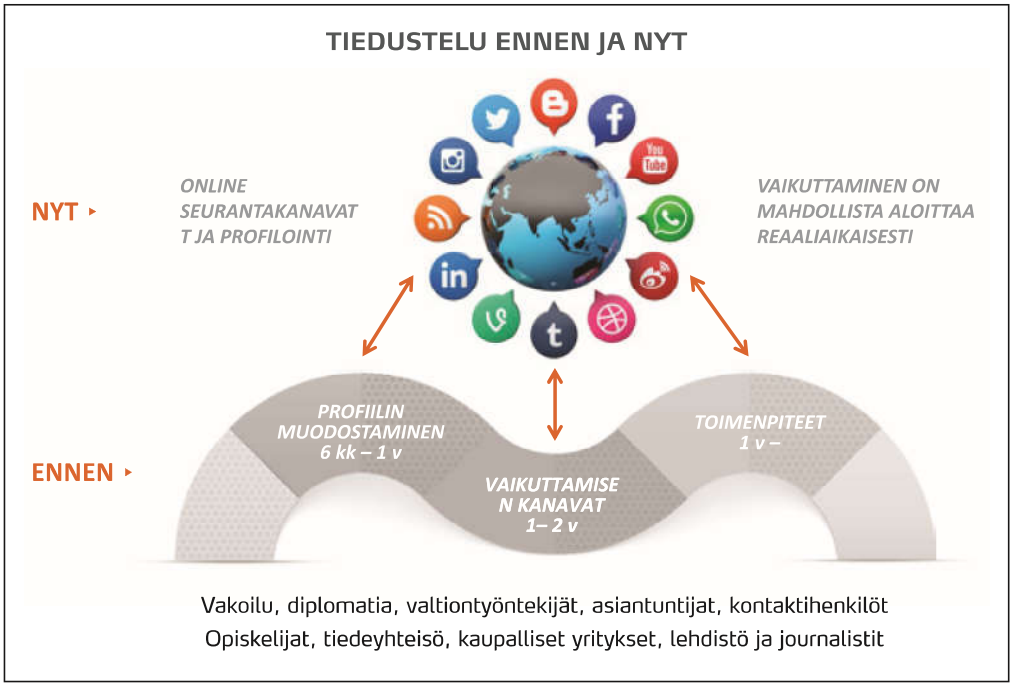
Kybervakoilun menetelmät

Tiedustelu voidaan nykyisin jakaa karkeasti perinteiseen tiedusteluun ja kybertiedusteluun. Perinteinen tiedustelu pitää sisällään henkilötiedustelun (HUMINT, Human Intelligence), julkisiin lähteisiin perustuvan tiedustelun (OSINT, Open Source Intelligence) sekä signaalitiedustelun (SIGINT, Signal Intelligence).

Useiden maiden tiedustelujärjestelmässä kybervakoilusta on tullut perustyökalu, joka on muuttanut muiden tiedustelumenetelmien roolia. Kybervakoilun avulla pystytään keräämään suuri määrä tietoa, jonka hankkiminen vaati aiemmin paljon enemmän työtä. Samoin henkilö- ja avointen lähteiden tiedustelu voidaan kohdistaa paremmin ja nopeammin haluttuihin kohteisiin.

Voidaankin sanoa, että kybervakoilun tarjoamien mahdollisuuksien avulla valtioiden tiedustelun teho ja nopeus ovat parantuneet huomattavasti. Pitkäjänteisen perinteisen operaatiosuunnittelun rinnalle on muodostunut kybertoimintaympäristö, joka mahdollistaa välittömät ja aktiiviset vaikuttamistoimet tilanteen vaatiessa. Hyökkäysprosessin suunnitteluun kuluva aika on lyhentynyt merkittävästi. Oikealla tiedustelutiedolla – oikeaan aikaan ja oikein käytettynä – on merkittävä vaikutus siihen, miten sotilaallisia, taloudellisia, poliittisia tai henkilöön kohdistuvia operaatioita kannattaa ja voidaan toteuttaa. Lisäksi muita elektronisen tiedustelun eri menetelmiä voidaan käyttää entistä joustavammin ja täsmällisemmin. Myös avoimien lähteiden tai henkilötiedustelun kautta voidaan tunnistaa tietotarpeita, joiden pohjalta käytettäväksi menetelmäksi voidaan valikoida esimerkiksi hakkerointia tai informaatiovaikuttamista.

Kybervakoilulle on ominaista sen pitkäkestoisuus. Operaatioilla pyritään tunkeutumaan haluttuihin kohteisiin ja pysymään mahdollisimman pitkään salassa. Näin voidaan kerätä jopa vuosien ajan tietoja kohteen tietämättä. Erityisen haluttua tietoa on haavoittuvuudet teknisissä ratkaisuissa, ihmisten toiminnassa sekä yritysten ja organisaatioiden avaintoiminnoissa ja -prosesseissa.

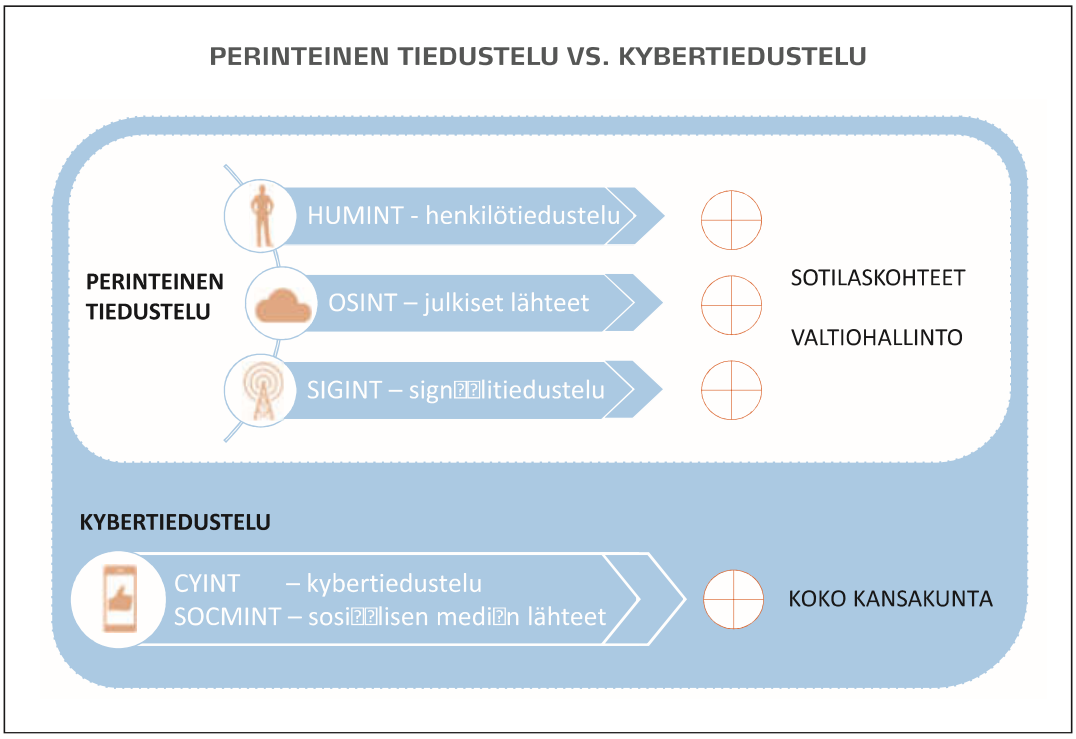


Myös henkilötiedustelu on siirtynyt tietoverkkoihin. Se on saanut rinnalleen uuden ulottuvuuden, **sosiaalisen median tiedustelun** (SOCMINT, Social Media Intelligence), jonka avulla voidaan kerätä tietoa sosiaalisista medioista havainnoista, uskomuksista sekä mahdollisesti tulevista tai jo menneistä tapahtumista. Tämän avulla voidaan lisäksi etsiä rikollista tai terroristista toimintaa, tuotekehitystietoa, yhteiskunnan kriittisissä toiminnoissa olevia haavoittuvuuksia, sekä henkilöiden inhimillisiä heikkouksia. SOCMINT tarjoaa kohdehenkilöistä luotettavia henkilöprofiileja lähes reaaliajassa.

Tiedusteluorganisaatiot ovat kiinnostuneita löytämään epäilyttäviä ja muutoin kiinnostavia ihmisiä, jotka eivät vielä ole vielä heidän kohteinaan. Samalla tiedustelumarkkinoille on tullut myös kaupallisia toimijoita, kyberrikollisten verkostoja ja yksittäisiä tai pienissä ryhmissä toimivia hakkereita. Sosiaalisen median ja erilaisten sovellusten keräämä tieto on helposti saatavilla ja analysoitavissa. Paradigman muutos on siis melkoinen.

Valtiollisten toimijoiden erityisen mielenkiinnon kohteena on usein poliittisten päätösten valmistelu ja toteuttaminen. Tavoitteena on saada tietoa siitä, miten poliittiseen päätöksentekoon voidaan vaikuttaa. Tämä liittyy monesti myös kiinteästi informaatiovaikuttamiseen ja jopa tiedon sabotointiin tai manipulointiin.[14] Kybervakoilulla voidaan luoda edellytykset tehokkaalle informaatiovaikuttamiselle keräämällä tarvittavat tiedot ja tyypilliset vaikuttamispisteet, joihin pyritään iskemään räätälöidyin tarkasti kohdennetuin viestein. Toiminnalla voidaan myös pyrkiä aktivoimaan tai vaihtoehtoisesti passivoimaan ryhmiä riippuen tavoitteista.

Raja hakkeroinnin, kyberrikollisuuden ja valtiollisen tiedustelun välillä on häilyvä. Valtiolliset tahot saattavat käyttää hakkereita toteuttamaan kyberoperaatioitaan. Samalla ne tuottavat tietoa rikolliseen toimintaan sekä valtiollisten tiedustelupalveluiden käyttöön. Myös rikolliset voivat rekrytoida hakkeriyhteisöjen osaajia käyttöönsä.



14 https://www.usatoday.com/story/news/2018/05/11/what-we-found-facebook-ads-russians-accused-election-meddling/602319002/

Miten suojautua kybervakoilulta?

Nopeasti digitalisoituva liiketoimintaympäristö vaatii ketteryyttä strategiseen johtamiseen ja liiketoimintaprosesseihin. **Kyberuhilta ja yritysvakoilulta suojautuminen tulee siksi nähdä ensisijaisesti johdon haasteena.** Kyse on kokonaisvaltaisesta hyvään tilanneymmärrykseen perustuvasta jatkuvuuden suunnittelusta, tärkeimpien kohteiden tunnistamisesta ja suojaamisesta sekä niihin kohdistuvien uhkien ja riskien hyvästä hallinnasta.

Mittava osa tietovuodoista ja liiketoimintaa uhkaavista tilanteista johtuu edelleen henkilökunnan toiminnasta, ns. insider-riskistä.[15] Henkilökunnan säännöllinen kouluttaminen ja turvallisuustietoisuuden lisääminen ovat siksi avainasemassa. Jokaisen on oltava tietoinen heihin itseensä ja yritykseen kohdistuvista kyberuhista sekä toimintamalleista, joita tulee noudattaa havaittuaan epäilyttävää toimintaa tietojärjestelmissä, prosesseissa tai ihmisten toiminnassa. Hyvällä henkilöstöjohtamisella voikin merkittävästi parantaa yrityksen kykyä vastata kyberturvallisuuden haasteisiin.

Tekniset ratkaisut ja laitteistot tulee arvioida ja suojata koko ekosysteemin osalta sekä huolehtia säännönmukaisista ohjelmisto- ja tietoturvapäivityksistä. Riskiympäristöissä paljon matkustavien ja niissä julkisissa paikoissa langattomia verkkoja käyttävien henkilöiden olisi mahdollisuuksien mukaan hyvä käyttää erillisiä, vain matkakäyttöön varattuja laitteita. Tiedon eheyden seuraamiseen on tarjolla hyviä suomalaisia ratkaisuja, jotka paljastavat ja havaitsevat nopeasti muutoksia, jotka voivat johtua erilaisista kyberoperaatioista.

Sosiaalisen median palveluihin kannattaa sopia yrityksen yhteiset käytänteet ja antaa suosituksia ja ohjeistuksia myös vapaa-ajan käyttöön. Perusperiaatteena sen tiedostaminen, että ihminen on haavoittuvainen, vaikutuksille altis ja tarvittaessa manipuloitavissa. Esimerkiksi horjuva henkilökohtainen taloudellinen tilanne, halu kostaa työnantajalle, kiristyksen kohteeksi joutuminen tai halu toimia oman elämän "salaisena agenttina", voi johtaa epätoivoisiin tai tarkoituksellisiin tekoihin.[16] Tällöin tiedusteluorganisaatiot voivat käyttää henkilöä hyväkseen ja korvausta vastaan vaatia tekemään vaikkapa ohjelmakoodiin virheitä tai luovuttamaan salausavaimia[17].

MITEN SUOJAUTUA KYBERVAKOILULTA?

- ☑ **Ketteryyttä strategiseen johtamisen ja liiketoimintaprosesseihin kyberympäristössä.**
- ☑ **Paranna kykyä tapahtumien ja poikkeamien havaitsemiseen sekä seurannaisvaikutuksien hallintaan.**
- ☑ **Suojattavien kohteiden, tiedon ja henkilöiden tunnistaminen.**
- ☑ **Oman toimialan turvallisuusuhkien jatkuva seuraaminen.**
- ☑ **Turvallisuuskyvykkyyden ja -tietoisuuden nostaminen koulutuksin, tietoiskuin ja harjoituksin.**
- ☑ **Hyvät turvallisuuskäytänteet ja turvallisuuskulttuurin rakentaminen.**
- ☑ **Henkilöstön ja yhteistyöyritysten taustan selvittäminen.**
- ☑ **Tekniset perusasiat kuntoon: tietoturvapäivitykset, palomuurit, virustorjunta, VPN-yhteyksien käyttö, turvalliset salasanakäytänteet (myös mobiililaitteissa).**
- ☑ **Lokitietojen taltiointi, seurantaprosessit ja suojaus.**

15 http://www.supo.fi/fi/ajankohtaista_supo/1/0/insider-teot_uhka_yrityksen_toiminnalle_75508
16 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf
17 Järvinen, P. (2014). NSA - Näin meitä seurataan (Docendo). Saarijärvi: Saarijärven Offset Oy

Uhkista huolimatta eteenpäin!

Maailma ja ihmiset ovat verkottuneet nopeasti ja kehitys on kiihtyvää. Samalla tiedon hyödyntämisen mahdollisuudet tekoälyn ja esineiden internetin myötä jatkavat kasvuaan. Meistä kaikista on olemassa – ja tulee olemaan – merkittävä määrä tietoa saatavilla. Tietoa voidaan käyttää myös meitä vastaan. Kyberturvallisuudella ja digitaalisella jalanjäljellä on kasvava rooli jokaisen ihmisen osalta.

Kyberturvallisuuden tulisi olla osa liiketoimintastrategiaa. Ymmärrys kybermaailman realiteeteista, niiden vaikutuksista ja kyky kehittää omaa toimintaa ovat fundamentaalisen tärkeitä yrityksen koko olemassaololle. Yrityksen ylimmän johdon sitoutuminen ja ymmärrys ovat tässä avainroolissa.

Se kuinka osaamme ja uskallamme hyödyntää uusia mahdollisuuksia määrittää myös kuinka hyvin pärjäämme digitalisen kehityksen keskellä. Yhä tärkeämpää tulee olemaan myös kyky toipua mitä erilaisimmista kybertapahtumista ja -hyökkäyksistä. Tulevaisuus on mahdollisuus – siksi digitalisaatiota ja kyberturvallisuutta on rakennettava käsi kädessä.

Lähteet ja lisätietoja

Elinkeinoelämän keskusliitto EK

Johtava asiantuntija
Mika Susi
Puh. 09 4202 2287
mika.susi@ek.fi

PL 30 (Eteläranta 10), 00131 Helsinki
Puh. 09 420 20 ▪ www.ek.fi

Raportti internetissä: www.ek.fi

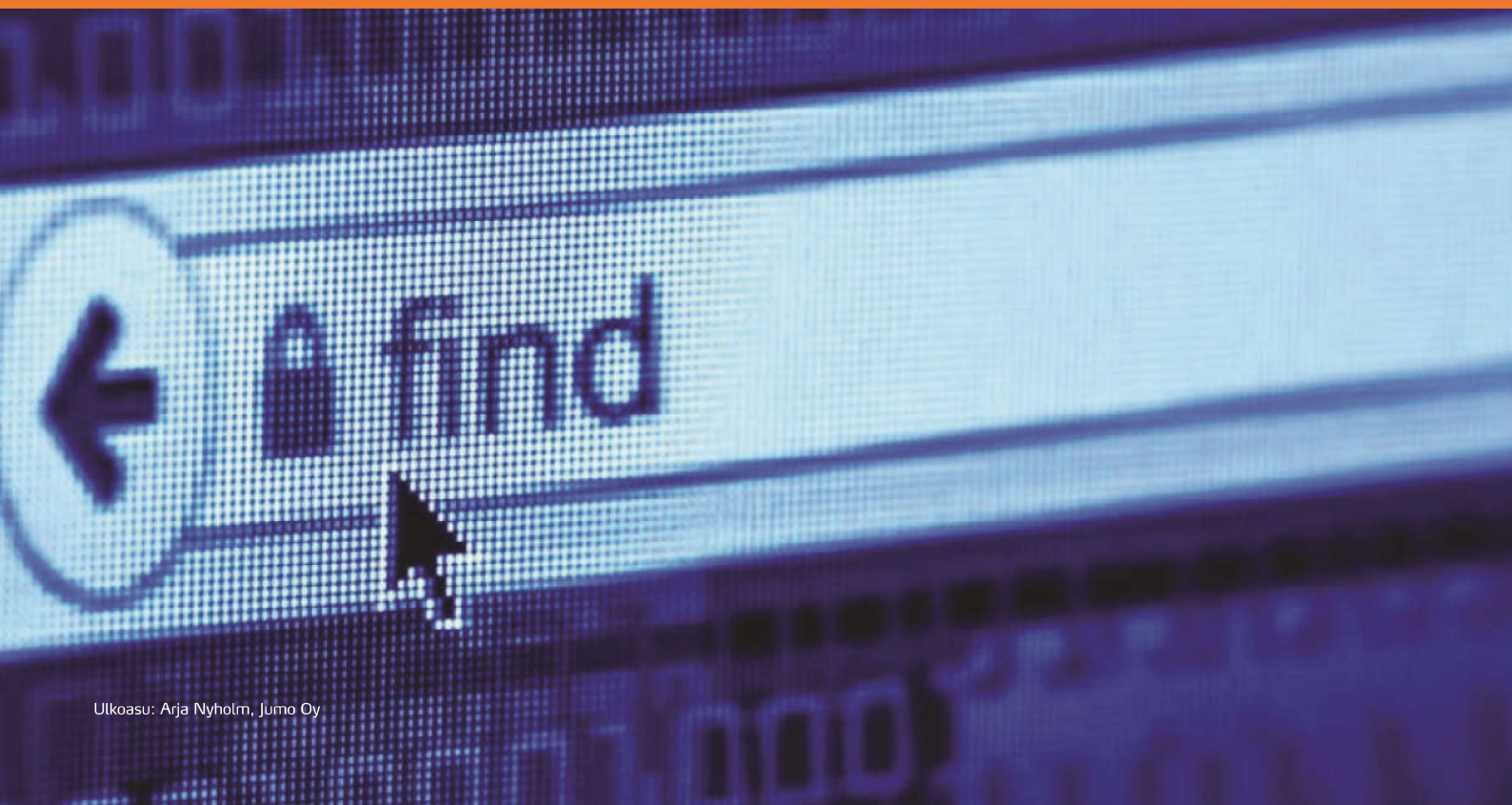
EK 2018

Cyberwatch Finland

CEO and Co-Founder
Aapo Cederberg
Puh. 0400 246 746
aapo.cederberg@cyberwatch.fi

Chief Analyst
Kim Waltzer
Puh. 040 771 4737
kim.waltzer@cyberwatch.fi

www.cyberwatch.fi



Ulkoasu: Arja Nyholm, Jumo Oy