HAMK
Häme University
of Applied Sciences

Tämä on rinnakkaistallenne alkuperäisestä artikkelista /

This is a self-archived version of the original article.

Version: Accepted manuscript / Final draft

Käytä viittauksessa alkuperäistä lähdettä: /

To cite this article please use the original version:

Turve, I. (25.5.2023). Avointen lähteiden tiedustelua käyttävät rikollisetkin. *Itä-Häme*, 12.

Avointen lähteiden tiedustelua käyttävät rikollisetkin

Avointen lähteiden tiedustelulla (OSINT, Open Source Intelligence) tarkoitetaan tiedustelutiedon hankintaa, koostamista ja analysointia hyödyntäen sellaisia lähteitä, joihin on avoin tai kaupallisesti saatavilla oleva pääsy. Avoimia lähteitä ovat lehdet, kirjat, esitteet, mainokset, televisio- ja radio-ohjelmat, erityyppiset videot ja opinnäytetyöt sekä sosiaalisen median julkaisut. Avointen lähteiden tiedustelun idea on siinä, että yhdistelemällä monesta lähteestä saatua julkista aineistoa saattaa syntyä tietokokonaisuus, joka on salaista tai ei ole ainakaan tarkoitettu julkisuuteen.

Avointen lähteiden tiedustelu pohjautuu sotilastiedusteluun, mutta sitä käytetään laajasti muuallakin kuin puolustusvoimissa. Yritysmaailmassa avointen lähteiden tiedustelua pidetään yhtenä tärkeimpänä menetelmänä tiedonhankinnassa ja kilpailijoiden arvioinnissa koska avointen lähteiden käyttö on vapaata ja täysin laillista. Nykyisin myös rikolliset käyttävät avointen lähteiden tiedustelua entistä tehokkaammin hyödykseen.

Jokaisella internetissä toimivalla yrityksellä ja yksityisellä henkilöllä on digitaalinen jalanjälki, joka tarkoittaa kaikkea sitä, mitä me jätämme jälkeemme nettiin. Kaikki mitä me internetissä teemme, milloin teemme, missä me olemme, mitä me julkaisemme sekä myös mitä muut meistä julkaisemme, muodostavat digitaalisen jalanjälkemme, josta myös verkon rikolliset voivat olla kiinnostuneita. Rikolliset voivat olla kiinnostuneita esimerkiksi siitä missä me olemme, tai vaihtoehtoisesti myös siitä missä me emme ole. Jos meillä on jotain rikollista kiinnostavaa, rikollinen saattaa paikkatietoja hyödyntäen saada selville, että rikoksen kohde on ulkomaanmatkalla jolloin on hyvä aika noutaa haluttu tavara parempaan talteen.

Perinteisen rikollisuuden ohella myös valtiolliset toimijat voivat olla kiinnostuneita yksityisistä ihmisistä. Henkilötiedustelun keinoin voidaan lähteä lähestymään kiinnostavaa henkilöä. Aluksi selvitetään taustatietoja, selvitetään mistä henkilö on kiinnostunut, mitä henkilö tekee ja miten henkilöä voitaisiin lähestyä reaalimaailmassa. Jatkossa kohdetta saatetaan tiedustelun kautta saadun datan kautta kiristää tai vaihtoehtoisesti lahjoa tekemään jotain sellaista, mitä hän ei muuten tekisi.

Monesti kuulee sanottavan, että ei minussa ole mitään mielenkiintoista tai ei minulla ole mitään salattavaa. Harva kuitenkaan ei tiedä, missä on muutaman vuoden päästä. Työtehtävät saattaa muuttua koulutuksen kautta sellaisiksi, että ei enää halutakaan, että muut saavat selville missä henkilö asuu, minkälainen perhe on, tai missä lapset ovat koulussa.

On siis hyvä miettiä mitä tietoa itsestään verkkoon laittaa. On hyvä pohtia mitä henkilötietoja itsestä verkossa on. Sosiaalisessa mediassa olevien kuvien perusteellakin voidaan mahdollisesti selvittää henkilön asuinpaikka suhteellisen tarkasti. Lisäksi on hyvä tarkastaa välillä omien somepalveluiden yksityisyysasetukset, jääkö omat julkaisut vain kaveripiirin nähtäväksi, vai meneekö kaikki julkaisut julkisesti kaikkien nähtäville.

Ismo Turve

Kirjoittaja on kyberturvallisuus orientoitunut heinolalainen Tietojenkäsittelyn lehtori Hämeen ammattikorkeakoulusta.