

Järjestäytynyt kyberrikollisuus on miljardien arvoista globaalia liiketoimintaa

Tietoverkkorikollisuuden keskeinen elementti on **kansainvälisyys** ja niiden taustalla on enenevässä määrin **järjestäytynyttä rikollisuutta**.

Europolin uhka-arvioissa korostetaan, että perinteisten hierarkkisten rikollisryhmien ja verkostojen rinnalle on kehittynyt yksittäisten projektimaisesti toimivien rikollisten "yrittäjien" markkinapaikkana toimiva virtuaalinen alamaailma, erityinen **rikollinen palveluteollisuus** (Crime-as-a-Service, CaaS). Se koostuu erilaisista palveluntarjoajista ja monimutkaisista toimitusketjuista.

Yksittäinen tekijä kykenee teknologiaa hyödyntämällä tekoihin, joiden vaikutukset voivat välittömästi heijastua useisiin eri valtioihin ja miljooniin ihmisiin.

Rikosvahinko Suomessakin lasketaan sadoissa miljoonissa euroissa.

Vuosien 2009–2020 tietoverkkorikoksista annetut tuomiot ovat Suomessa olleet kasvussa.

Suurin osa tietoverkkorikollisuudesta on **piilorikollisuutta**. Tässä hyödynnetään myös psykologisia keinoja, kuten uhrien häpeän tunnetta.

Kyberrikollisten näkökulmasta terveydenhuollon organisaatiot ovat erityisen houkuttelevia kohteita (Medical Identity Theft, MID). Kansainvälisten tutkimusten mukaan noin **25 % kaikista tietomurroista** kohdennetaan terveydenhuoltoon.

Mitä datalla tehdään: Uhkaillaan, kiristetään, myydään, ostetaan (mm. lääkkeitä/huumeita/lääketieteellisiä laitteita tai hoitoja), haetaan korvauksia tai avustuksia, avataan tilejä, hankitaan työpaikka.

Päämotiivina on siis taloudellisen hyödyn tavoittelu, suoraan tai epäsuoraan.

Muita motiiveja:

Terrosistisen tai muun **rikollisen toiminnan rahoitus**

Tahallinen mainehaitta tai **epäluottamuksen aikaansaaminen** yhteiskunnan toimintaa kohtaan

Kilpaileva liiketoiminta

Kosto entiselle työnantajalle

Tahaton työntekijän huolimattomuus

Poliittiset, eettiset tai kulttuuriset motiivit ("haktivistit")

Julkisuuden henkilöiden kiristäminen uhreina

Huomiohakuisuus, jännityshakuisuus, älyllinen haaste

Mitä tekijöistä tiedetään?

Suuri osa tekijöistä on osa järjestäytyntä rikollista toimintaa (yli 60 %)

Verkkorikokset ovat monille **pääelinkeino**.

Diginatiivit jotka ovat tottuneet toimimaan digitaalisessa ympäristössä. Tyypillisesti nuorehko mieshenkilö jossa rikos tehdään **ryhmässä**. Vaativien verkkorikosten kohdalla kyseessä on ammattiatitoa vaativa projekti.

Persoonallisuus: impulsiivisia, epäsensitiivisiä, riskinottokykyisiä, vähäinen omien tekojen pitkäaikaisten seurausten vastuunottokyky.

Kansainvälisellä tasolla korostetaan potilastietojen anastamisen suurimman uhkan tulevan **organisaation sisältä; tahallisesti tai tahattomasti**. Tämä tarkoittaa organisaation työntekijöitä (mm. pääkäyttäjät ja loppukäyttäjät), entisiä työntekijöitä ja organisaatiossa väliaikaisesti työskenteleviä kolmansia tahoja (esim. projektiluontoisesti tai tilapäistyöntekijät).