Helsingi linna vastu toime pandud andmemurre näitab, et andmemurded nõuavad uut lähenemist avaliku sektori valmisolekus, kommunikatsioonis ning andmemurrete ennetamises

Soome valitsus moodustas 2024. aasta juulis Õnnetuste Uurimiskeskuse (OTKES) juurde sõltumatu uurimisrühma, et selgitada 2024. aasta kevadel Helsingi linna vastu toime pandud andmemurdu. Andmemurru ohvreid on hinnanguliselt umbes 300 000, mis teeb sellest suurima andmeründe Soomes. Uurimisrühm on lõpetanud ohutuse uurimise ning uurimisaruanne anti üle valitsusele 17.06.2025.[1]

Küberkuritegevus on kasvav valdkond ning sellega kaasnevad kahjud on märkimisväärsed – eriti praeguses hübriidohtude olukorras. Avalik haldus pakub kurjategijatele huvi sinna talletatud andmete hulga ja olemuse tõttu. Avalikul sektoril on veel arenguruumi küberkuritegevuse ohtudele reageerimisel, sest rünnakute ja haavatavuste tuvastamise meetodid ei ole piisavalt laialdaselt kasutusel.

Avaliku halduse teabehaldust, küberturvalisust ja andmekaitset juhivad mitmed erinevad asutused. Ametiasutused juhivad seda iseseisvalt, lähtudes oma ülesannetest ja pädevusest. Teabehaldusüksuste juhtimine on killustatud ning seaduste ja juhiste rakendamine on praktikas ebaühtlane. Lisaks seisneb ametiasutuste tegevus peamiselt suunamises, kuid järelevalve tegutsejate üle on vähene. Kuid just teabe elutsükli haldamine on küberturvalisuse ja andmekaitse seisukohalt keskse tähtsusega. Avaliku sektori valmisolekut küberohtudele reageerimiseks saab tugevdada, arendades ja laiendades rünnakute ja haavatavuste tuvastamise meetodeid.

„Andmemurdetaolisteks juhtumiteks valmisolek ja nende tõrjumine seab meid mitmes mõttes uude olukorda: Soomes on traditsiooniliselt oldud harjunud ametiasutuste koostööga. Küberintsidentide puhul on tõrjemeetmed hajutatud. Samal ajal sõltub andmemurdejuhtumite uurimine ja juhtimine suuresti erasektori tegutsejate asjatundlikkusest ja kättesaadavusest. Näiteks SAR-tegevuse[2] sarnast koostöömehhanismi ei ole andmemurdejuhtumite jaoks määratletud. Palju jääb ka kannatanu enda õlule," märgib uurimisrühma juht Hanna Tiirinki.

„Samuti vajab kannatanu mõiste ümbermõtestamist. Kasutame peaaegu märkamatult igapäevaselt erinevaid andmebaase ja teenuseid. Kohalikul omavalitsusel on meie kohta mitmesuguseid isikuandmeid. Küberintsidentide puhul võib ründaja salvestada suures mahus andmeid hilisemaks kasutamiseks. Just andmete kombineerimine muudab kannatanud haavatavamaks. Andmemurrete korral tuleb alati arvestada riskiga, et andmeid võidakse hiljem kasutada pahatahtlikel eesmärkidel, näiteks identiteedivargusteks või pettusteks ning noored ei pruugi osata ette näha, mis nende andmetega juhtub, kui nad saavad täisealiseks," lisab Tiirinki.

Riiklik küberjulgeoleku seadus jõustus 08.04.2025. Euroopa Liidu võrgu- ja infoturbe direktiivi NIS2 siseriiklik rakendamine on küberjulgeoleku seaduse elluviimise osa. Soomes on aga omavalitsustel ulatuslik autonoomsus ning NIS2 küberturvalisuse direktiiv ei laiene kohalikele omavalitsustele ega linnadele.

„NIS2 direktiiv ei laiene Soomes kohaliku tasandi haldusüksustele. Uurimise käigus antud soovitustega püüame nüüd osaliselt seda lünka täita," lisab Tiirinki.

NIS2 kehtestab organisatsioonidele 24-tunnise teavitamiskohustuse. Andmemurdejuhtumite puhul on teavitamine kaitsetegevuse oluline osa. Kommunikatsioon vähendab ebakindlust, aitab vältida

---

[1] Erakordse sündmuse uurimine võib seaduse kohaselt käsitleda juhtumit, mis ei ole õnnetus, kuid mis on olnud äärmiselt raske, põhjustanud surma või ohustanud tõsiselt ühiskonna põhifunktsioone või neid oluliselt kahjustanud (Ohutuse uurimise seadus 525/2011).

[2] Search and Rescue, otsing ja päästetööd

valeinfo levikut ning tagab, et kannatanud saavad vajaliku toe. Kommunikatsiooni kättesaadavus, ulatuslikkus ja arusaadavus on ülimalt oluline.

„Näiteks ka laste ja noortega ning nende eakohase teavitamisega tuleb arvestada. Kriisi- ja hädaolukorra kommunikatsiooni põhiolemus seisneb sageli selles, et tuleb alustada tegutsemist ebatäieliku infoga, sest tervikpilt olukorrast täieneb pidevalt. Algse info puudulikkus ei tohi olla takistuseks teavitamisele," rõhutab Tiirinki.

„Olgu veel öeldud, et kohaliku tasandi tegutsejad on väga erinevad ega ole ühtviisi võrreldavad. Osadel on valmisolek juba väga heal tasemel, teistel on aga veel arenguruumi. Soome on rahvusvahelises võrdluses valmisoleku osas parimate hulgas. Peale toimunud andmemurde on meil probleemi märgatud ning sellega on hakatud tegelema. Teisisõnu – juba praegu tehakse palju andmemurdetaoliste juhtumite ennetamiseks ja tõrjumiseks," rõhutab Tiirinki.

Uurimise käigus anti neli soovitust. Need on suunatud peamiselt Finantsministeeriumile, kes vastutab nende elluviimise eest koostöös Justiitsministeeriumi, Majandus- ja kommunikatsiooniministeeriumi, Haridusministeeriumi ja Omavalitsusliiduga. Lisaks kommunikatsiooni juhiste arendamisele hõlmavad soovitused ka teabehalduse koordineerimist, selle järelevalvet ja juhiseid. Samuti hõlmavad soovitused avaliku halduse infoturbe puuduste tuvastamise tõhustamist ning võimekuse suurendamist nende puuduste märkamiseks ja kõrvaldamiseks.

Riikliku küberturvalisuse ameti kommentaar:

Küberturvalisuse Keskus (KTK) *„Riikliku küberturvalisuse asutusena aitame ja nõustame ettevõtteid, ametiasutusi ja kodanikke, et nad oleksid valmis tuvastama praegusi ja tulevasi küberohte. Traficomi juurde kuuluv Küberturvalisuse Keskus on pakkunud Helsingi linnale igakülgset tuge alates andmemurde avastamisest ning me jätkame koostööd linna ja teenusepakkujatega,"* ütles *Traficomi Küberturvalisuse Keskuse juht Samuli Bergström. „Küberrünnaku korral tõuseb kommunikatsiooni olulisus esile. Traficomi 2025. aasta kevadel koostatud kriisikommunikatsiooni juhendis Kuidas teavitada küberrünnakutest käsitletakse erinevat tüüpi küberrünnakuid ning kurjategijate kasutatavaid meetodeid ja võtteid. Lisaks annab juhend soovitusi suhtlusalaseks valmisolekuks ning juhiseid suhtlemiseks küberrünnaku ajal ja pärast seda,"* lisab Bergström.

Muud uurimised seoses Helsingi linna andmemurdega:

Keskkriminaalpolitsei (KRP): Helsingi linna andmemurde eeluurimise eest vastutab Keskkriminaalpolitsei. Juhtumit uuritakse kui rasket andmemurret. Lisaks uurib Keskkriminaalpolitsei eraldi eeluurimises, kas linn on kaitsnud andmeid nõuetekohaselt. Selles uurimises on kuriteokahtluseks andmekaitserikkumine.

Soome Andmekaitseinspektsioon (TSV) uurib isikuandmetega seotud infoturbeintsidenti andmekaitsealaste õigusnormide järgimise vaatenurgast. Uurimise käigus hinnatakse eelkõige, kas Helsingi linnal olid kasutusel piisavad kaitsemeetmed ning kas linn on taganud rikkumise ohvriks langenud isikute õiguste kaitse. Juhtumi uurimine on käimas ning praegu analüüsitakse Helsingi linna esitatud selgitusi juhtunu kohta.

Kust abi saada?

Soome Kuriteoohvrite Valvekeskus (RIKU) on avaldanud oma kodulehel nõuandeid inimestele, kes on sattunud andmemurde või andmelekkega seotud ohvriteks. Veebilehel rõhutatakse, et on oluline järgida ametiasutuste juhiseid ja rakendada vajalikke tõkestusmeetmeid, et vältida isikuandmete kasutamist pettusteks. RIKU pakub samuti võimalust vestluseks. Teenused on tasuta.

Lisateave:

Uurimisrühma juht Hanna Tiirinki, tel 02951 50747, etunimi.sukunimi@om.fi

Lisaks tel 02951 50738 või 050345 1931. Uurimise jaoks avatud telefoniliin on avatud kuni 01.08.2025.

Pärast 01.08.2025 palume saata võimalikud küsimused e-posti aadressile viestinta.otkes@om.fi või otse uurimisrühma juhile.