P2024-01 Lühikokkuvõte

2024. aasta kevadel leidis aset tõsine sissemurd Helsingi linna kasvatuse ja hariduse (KASKO) valdkonna andmebaasi. Andmerikkumise tagajärjel sattus suur hulk õppijate ja töötajate andmeid ründaja kätte. Lisaks sisaldasid võrguketta dokumendid andmeid isikute, ettevõtete ja muude koostööpartnerite kohta, kes olid linnaga otseselt või kaudselt seotud.

Andmerikkumine algas 2024. aasta aprilli keskel ja pärast seda hakkas ründaja kaardistama sihtkohti sisevõrgus ja laiendama oma ligipääsu erinevatele serveritele. Aprilli lõpus kopeeris ründaja võrgukettalt neljas osas kokku ligikaudu kaks terabaiti andmeid. Failide täpset arvu ega sisu ei olnud võimalik kindlaks teha. Uurimise käigus jõuti hinnanguni, et ründaja sai enda valdusse umbes 750 000 dokumenti, millest osa sisaldas delikaatseid isikuandmeid.

Andmerikkumine kestis kaua, kuna organisatsiooni võrguseire oli puudulik ja märgatud teadetele ei reageeritud õigeaegselt. Kui andmerikkumine sai kinnitust, võttis Helsingi linn viivitamatult kasutusele haldus- ja parandusmeetmed, millega õnnestus rünnak peatada.

Märkimisväärselt suure andmete hulga kopeerimise võimaldasid kaks tegurit: Infosüsteemi õnnestus sisse murda puudulikult hallatud VPN-kaugühenduse serveri kaudu ning võrgukettale oli aastatega kogunenud suur hulk andmeid. Puudulik haldus tulenes personali- ja organisatsioonimuutustest, mille tulemusel muutusid vastutused ebaselgeks. Failid kogunesid võrgukettale, kuna andmehaldus oli puudulik ja ketta kasutamise juhiste täitmist ei kontrollitud.

Andmehaldust reguleerivad mitmed seadused ja määrused, kuid neid praktikas kohaldavad isikud tunnevad neid puudulikult. Seadusandlus ja riiklikud juhised on osaliselt raskesti mõistetavad ja killustunud. Eriti omavalitsussektorile on kehtestatud kohustusi mitme erineva ametiasutuse poolt, mis teeb terviku haldamise keerukaks.

Andmerikkumise tagajärjel sattus suur arv isikuandmeid sisaldavat materjali ründaja valdusse. Andmeid võidakse hiljem kasutada kahjulikul eesmärgil, näiteks identiteedivargusteks ja pettusteks. Uurimise ajal selle kohta mingeid märke ei ilmnenud.

Andmerikkumise ohvreid oli sadu tuhandeid. Uurimine näitas, et kõigi kannatanute täielik kaardistamine oli raske. Linna teenistuses töötavate isikutega saadi hästi ühendust, kuid endiste töötajate ja õppijate ning praeguste õppijate täielik kättesaamine osutus praktiliselt väga keeruliseks ja seda isegi mitte ei püütud teha.

Uurimise käigus anti neli soovitust. Need on suunatud peamiselt Finantsministeeriumile, kes vastutab nende elluviimise eest koostöös Justiitsministeeriumi, Majandus- ja kommunikatsiooniministeeriumi, Haridusministeeriumi ja Omavalitsusliiduga.

1. Finantsministeerium tagab koostöös Justiitsministeeriumiga, et avaliku halduse andmehaldust reguleeriv seadusandlus ühtlustatakse ning selle järelevalve- ja juhtimisstruktuurid muudetakse selgemaks.
2. Finantsministeerium koostöös Majandus- ja kommunikatsiooniministeeriumiga selgitab välja, kuidas avaliku halduse infoturbe puuduste avastamist saaks üleriigiliselt parandada ning tagab, et avaliku sektori asutustel oleksid piisavad võimekused infoturbe puuduste tuvastamiseks ja kõrvaldamiseks.
3. Finantsministeerium koostöös Haridusametiga tagab, et omavalitsused ja linnad arendavad andmerikkumiste juhtumite kommunikatsiooniks selged ja ligipääsetavad juhised, mille abil ohvrid saavad end andmerikkumise tagajärgede vastu kaitsta ja oma isikuandmeid turvata.

4. Finantsministeerium toetab koostöös Omavalitsusliiduga omavalitsusi infoturbe kriitiliste puuduste identifitseerimisel ja kõrvaldamisel ning arendab andmehalduse ja infoturbe riskijuhtimist.