Dataintrånget mot Helsingfors stad visar att den offentliga sektorn behöver nya sätt att förbereda sig, berätta om och stoppa dataintrång

Våren 2024 drabbades Helsingfors stad av ett dataintrång. I juli 2024 grundade statsrådet en grupp som utreder dataintrånget. Gruppen arbetar tillsammans med Olycksutredningscentralen (OTKES). Dataintrånget drabbade ungefär 300 000 personer och är det största dataintrång som någonsin har hänt i Finland. Utredningsgruppen har nu gjort klart säkerhetsutredningen och regeringen fick rapporten om utredningen den 17 juni 2025. [1]

Brott på nätet ökar hela tiden, och de orsakar stora problem – speciellt nu när så kallade hybridhot är vanliga. Den offentliga verksamheten är ett intressant mål för brottslingar eftersom de har mycket och viktig information. Den offentliga sektorn behöver bli bättre på att möta hot om brott på nätet. De använder inte tillräckligt med metoder för att märka attacker och svagheter.

Många olika myndigheter bestämmer hur offentliga verksamheter ska ta hand om information, skydda data och personuppgifter. Varje myndighet ger råd och regler utifrån sina egna uppgifter. De enheter som hanterar information får regler och råd från många olika håll. Det betyder att de kan följa reglerna på lite olika sätt. Myndigheterna ger råd och regler, men de övervakar inte så mycket. Det är viktigt för säkerheten och för att kunna skydda personuppgifter att man tar hand om informationen hela den tid den finns där. Den offentliga sektorn kan bli bättre på att möta hot på nätet. Man behöver skapa och använda fler sätt att märka attacker och svagheter.

”Att förbereda sig på dataintrång och att stoppa dem sätter oss i en ny situation på många sätt: I Finland är det vanligt att myndigheter samarbetar. Men då det händer en nätattack försöker olika aktörer stoppa dem på eget håll. Samtidigt är det ofta experter från privata företag som måste hjälpa till för att lösa och hantera dataintrång. Det finns inget liknande samarbete för dataintrång som till exempel SAR-samarbetet[2]*. Offret själv måste också ta mycket ansvar”*, säger utredningsgruppens ledare Hanna Tiirinki.

”Vi behöver också fundera på vad som egentligen menas med offer. Vi använder nästan varje dag olika databaser och tjänster utan att ens tänka på det. Kommunerna har mycket personuppgifter om oss. Vid nätattacker kan angriparen spara mycket information för att använda senare. Det är extra farligt när olika uppgifter kombineras – då blir offren mer sårbara. Vid dataintrång finns det alltid en risk att uppgifterna används på fel sätt senare. De kan användas för till exempel identitetsstölder eller bedrägerier. Unga tänker kanske inte på vad som kan hända med deras uppgifter när de blir vuxna”, säger Tiirinki.

Den nationella cybersäkerhetslagen började gälla den 8 april 2025. Cybersäkerhetsdirektivet NIS2 är en del av Cybersäkerhetslagen. Men i Finland bestämmer kommunerna och städerna mycket själva, så NIS2-direktivet gäller inte dem.

”NIS2-direktivet gäller inte kommunerna i Finland. Istället för direktivet ska vi använda de rekommendationer som utredningen har gett oss”, säger Tiirinki.

NIS2 kräver att organisationer berättar om attacker inom 24 timmar. Då det skett ett dataintrång är det viktigt att berätta om det för att skydda människorna. Då man får veta vad som hänt, minskar

[1] Med exceptionell händelse avses sådana synnerligen allvarliga händelser som inte är olyckor men som har lett till döden eller har hotat eller allvarligt skadat samhälleliga basfunktioner. Lag om säkerhetsutredning av olyckor och vissa andra händelser 525/2011.

[2] Search and Rescue, sök och räddning.

osäkerheten, rykten slutar spridas och offren kan få det stöd de behöver. Det är mycket viktigt att informationen är lätt att hitta, når alla och är enkel att förstå.

[1] Med exceptionell händelse avses sådana synnerligen allvarliga händelser som inte är olyckor men som har lett till döden eller har hotat eller allvarligt skadat samhälleliga basfunktioner. Lag om säkerhetsutredning av olyckor och vissa andra händelser 525/2011.

[2] Search and Rescue, sök och räddning.

”Barn och unga är också en målgrupp. Därför är det viktigt att de får information på ett sätt som passar deras ålder. När man berättar om en kris eller störning vet man ofta inte så mycket i början. Då är det ändå viktigt att man ger ut lite information istället för ingen alls”, säger Tiirinki.

”Det är bra att komma ihåg att lokala aktörer är väldigt olika och inte går att jämföra. Vissa är redan bra förberedda – andra har fortfarande saker att förbättra. Finland är väldigt bra förberett jämfört med andra länder. Efter dataintrången har vi förstått problemet och börjat rätta till det. Så det görs redan mycket för att förhindra och stoppa dataintrång”, säger Tiirinki.

Utredningen ger fyra rekommendationer. De gäller mest Finansministeriet, som ska se till att de genomförs tillsammans med Justitieministeriet, Kommunikationsministeriet, Utbildningsstyrelsen och Kommunförbundet. Rekommendationerna ger anvisningar för hur man ska berätta om dataintrång. De handlar också om att hantera informationen enhetligt, följa upp hur informationen hanteras och ge tydliga instruktioner. Rekommendationerna ska också hjälpa den offentliga sektorn att bli bättre på att märka och rätta till problem med datasäkerheten.

Uttalande från den nationella informationssäkerhetsmyndigheten:

Cybersäkerhetscentret: *”Vi är den nationella myndigheten för informationssäkerhet. Vår uppgift är att hjälpa företag, myndigheter och medborgare att förbereda sig på och känna igen dagens och framtidens cyberhot. Traficoms cybersäkerhetscenter har stött Helsingfors stad sedan man märkte dataintrånget. Nu fortsätter vi samarbeta med staden och tjänsteleverantörerna”,* säger direktör Samuli Bergström från Cybersäkerhetscentret vid Traficom. *”När det sker en nätattack blir kommunikationen extra viktig. Traficom gav ut kriskommunikationsguiden* Hur man kommunicerar om cyberattacker *våren 2025. Guiden förklarar olika typer av nätattacker och vilka metoder brottslingar använder. Guiden ger också tips om hur man kan förbereda sig på att ge ut information och hur man ger information under och efter en nätattack”*, säger Bergström.

Andra utredningar som handlar om dataintrånget mot Helsingfors stad:

Centralkriminalpolisen (CKP): CKP leder förundersökningen om dataintrånget mot Helsingfors stad. Dataintrånget utreds som grovt dataintrång. I en annan förundersökning utreder CKP om staden har skyddat uppgifterna tillräckligt bra. I den undersökningen utreds intrånget som ett misstänkt dataskyddsbrott.

Dataombudsmannens byrå utreder dataintrånget för att se om staden har följt dataskyddslagen. Utredningen granskar särskilt om Helsingfors har skyddat personuppgifterna tillräckligt och tagit hand om de drabbades rättigheter. Utredningen pågår, och man håller på att gå igenom Helsingfors stads förklaring om vad som hänt.

Var får jag hjälp?

Brottsofferjouren (RIKU) har delat tips på sin webbplats för dem som drabbats av dataintrång eller läckor. På webbplatsen lyfter man fram att det är viktigt att följa myndigheternas råd och

spärra personuppgifter så att de inte kan användas i bedrägerier. Du får också hjälp från RIKU om du vill prata med någon. Tjänsterna är gratis.

Mer information:

Ledare för utredningsgruppen Hanna Tiirinki, tfn 02951 50747, fornamn.efternamn@om.fi

Även tfn 02951 50738 eller 050345 1931. Du kan ta kontakt per telefon tills den 1 augusti 2025. Du kan också skicka frågor per e-post till viestintä.otkes@om.fi

Efter den 1 augusti ber vi dig skicka frågor till e-postadressen viestinta.otkes@om.fi eller direkt till utredningsgruppens ledare.