Dataintrånget mot Helsingfors stad 2024

P2024-01

FÖRORD

Statsrådet beslutade den 4 juli 2024 att inleda en utredning av dataintrånget mot Helsingfors stad och tillsatte en självständig och oberoende utredningsgrupp i anslutning till Olycksutredningscentralen. Utredningsbeslutet grundar sig på 32 § i lagen om säkerhetsutredning av olyckor och vissa andra händelser (525/2011). Det är fråga om en utredning av en exceptionell händelse enligt 5 kap. i lagen om säkerhetsutredning av olyckor och vissa andra händelser.

Till chef för utredningsgruppen utsågs ledande forskare, docent Hanna Tiirinki och medlemmar ekonomie doktor, psykologie magister Petri Koistinen, magister i förvaltningsvetenskap Ville-Petteri Pulkkinen, datanom Kimmo Rousku, diplomingenjör Petteri Järvinen, diplomingenjör Tomi Lounema och tradenom, filosofiemagister Lilly Korpiola.

Till specialsakkunnig i lagstiftning utsågs professor i kommunikationsrätt, vicehäradshövding Päivi Korpisaari.

Fallet utreds också av Centralkriminalpolisen.

Utredningen av en exceptionell händelse genomförs enligt principerna för säkerhetsutredning. Syftet med säkerhetsutredningen är att öka den allmänna säkerheten medan utredningen inte görs för att fastställa det juridiska ansvaret.

I säkerhetsutredningen utreds händelseförloppet, orsakerna och följderna samt de räddningsåtgärder som vidtagits och myndigheternas verksamhet.

Utredningsrapporten innehåller en redogörelse för händelseförloppet, de faktorer som föranledde händelserna och deras konsekvenser samt säkerhetsrekommendationer till behöriga myndigheter och andra aktörer om sådana åtgärder som behövs för att öka den allmänna säkerheten, avvärja skador samt effektivisera räddnings- och andra myndigheters verksamhet.

Utredningsrapporten har varit på remiss hos de centrala aktörerna som varit delaktiga i händelsen. Utlåtandena har beaktats när utredningsrapporten färdigställdes. Ett sammandrag av utlåtandena finns i slutet av utredningsrapporten.

De grafer och illustrationer som använts i utredningsrapporten har gjorts för utredningsgruppen av Sole Lätti/Tiedekuvitus. Källan till figurerna för dessa grafer har inte antecknats separat i beskrivningen.

Utredningsrapporten har översatts till svenska och engelska av Lingsoft.

Utredningsrapporten lämnades till statsrådet den 17.06.2025 och publicerades på Olycksutredningscentralens webbplats *http://www.turvallisuustutkinta.fi/sv/*.

Utredningens beteckning: P2024-01
Utredningsrapport 3/2025
ISBN: 978-951-836-679-2 (PDF)
ISSN: 2341–5991

INNEHÅLLSFÖRTECKNING

1 HÄNDELSER

Helsingfors stad upptäckte ett omfattande dataintrång den 30 april 2024. Dataintrånget riktade sig mot fostrans- och utbildningssektorns (KASKO) nätverk och dess servrar. När saken uppdagades vidtog staden motåtgärder och lyckades stoppa attacken. I början kunde man inte skapa sig en bild av dataintrångets verkliga omfattning, eftersom det tog tid att ta reda på föremålen för dataintrånget.

Dataintrångets faser och hanteringsåtgärder beskrivs i följande avsnitt. Uppgifterna har samlats in genom att analysera olika loggar[1] efter händelsen, men eftersom alla nödvändiga logguppgifter inte fanns att tillgå har man inte kunnat skapa en fullständig bild av händelserna.

1.1 Dataintrångets faser

Våren 2024 försökte en okänd angripare tränga in i fostrans- och utbildningssektorns nätverk genom att söka svagheter i nätverket och pröva olika lösenord. Under perioden 29.2–4.4.2024 registrerades över 300 000 kontakter. Försöken riktades mot den utåt synliga VPN-routern[2], som dock avvärjde försöken.

En annan angripare från en annan adress samlade in information om fostrans- och utbildningssektorns webbmiljö den 15 mars 2024 och testade lösenord under tiden 8–12.4.2024. Angriparen försökte bryta sig in i VPN-routern med hjälp av två kända sårbarheter. Försöken ledde till att den tekniskt föråldrade routern som inte hade uppdaterats kraschade den 14 april 2024 kl. 20:14, men öppnade inte åtkomst till intranätet. De fick dock mer information om VPN-enheten och nätverkstekniken som angriparen senare kunde utnyttja. På grund av den bristfälliga övervakningen observerades inga intrångsförberedelser i fostrans- och utbildningssektorns egen övervakning.

Den andra angriparen lyckades logga in på VPN-routern eventuellt redan den 18 april 2024, men det egentliga dataintrånget inleddes den 25 april 2024 kl. 13:17 när angriparen loggade in i fostrans- och utbildningssektorns intranät genom att använda en högstadieelevs användarnamn och lösenord som denne hittat på mörka webben[3].

Efter det lyckade intrånget kartlade angriparen det intranätet genom att i två timmar skanna 34 nätportar på sammanlagt 9 945 IP-adresser i intranätet. Åtgärderna orsakade datasäkerhetslarm i brandväggsloggar den 25 april 2024 kl. 13:40 och kl. 13:59, men ingen reagerade till larmen eftersom staden hade ingen övervakningstjänst för brandväggens datasäkerhetslarm.

Angriparen loggade in första gången kl. 15:07 med fjärranslutning i fostrans- och utbildningssektorns servermiljö. Kort därefter gav DigiHelsinkis programvara för bekämpning av skadlig programvara ett larm på medelnivå, enligt vilket man hade från en Windows-server försökt logga in på nio andra servrar sammanlagt 122 gånger.

---

[1] I IT-miljöer samlas loggdata som systemet, applikationerna eller nätverket automatiskt producerar och som sparar händelser, användarfunktioner, systemfel och händelser i anslutning till informationssäkerheten för analys, felsökning och övervakning in i loggfiler.

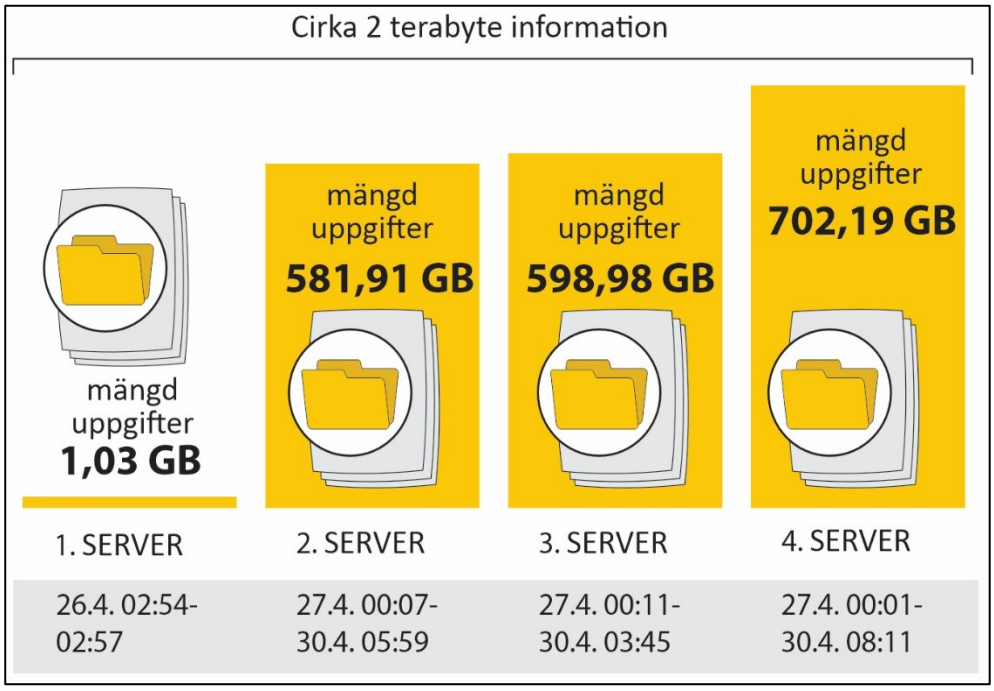
[2] VPN (Virtual Private Network) är en teknik som skapar en skyddad tunnel genom ett offentligt nätverk med internetuppkoppling. Med hjälp av den kan fjärranvändare på ett säkert sätt ansluta till servrar i ett internt nätverk.

[3] Mörka webben är en del av internet som kräver en separat TOR-webbläsare. Där finns nätbrottslingars handelsplatser där tjänster som brottslingarna behöver samt användarnamn, lösenord och kreditkortsuppgifter säljs.

DigiHelsinkis tjänsteleverantör öppnade ett ärende (ticket[4]) på genomsnittlig allvarlighetsnivå för observationerna den 25 april 2024 kl. 17:22. Ärendet styrdes kl. 18:36 till en annan tjänsteleverantör, men på grund av ett fel i ticketingsystemet gick ärendet inte fram.

Angriparen fortsatte logga in den 25 april 2024 kl. 16:36 med fjärranslutning i fostrans- och utbildningssektorns servermiljö och fick den 25 april 2024 kl. 17:24–18:40 åtkomst till uppgifterna i användarkatalogen Active Directory för två olika verksamhetsområden. Dessutom fick angriparen kontroll över fostrans- och utbildningssektorns centrala administrationsserver för virtuell servermiljö som innehöll Windows-servrar.[5] Angriparen lyckades också bryta sig in i servermiljön som sköter säkerhetskopieringen av fostrans- och utbildningssektorns servrar och filer. Övertagandet av servrarna och den efterföljande kopieringen av uppgifterna gjordes möjlig genom stöld av domänernas huvudanvändares (administrator) nödvändiga lösenord.

Efter att ha fått de nödvändiga koderna och användarrättigheterna till servrarna började angriparen kopiera de av fostrans- och utbildningssektorns filer som fanns på nätverksdisken till sig själv. Den första filöverföringen inleddes den 26 april 2024 kl. 2:54, då angriparen kopierade 1,03 gigabyte[6] data från fostrans- och utbildningssektorns nätverksdisk. Efter testöverföringen började angriparen stjäla filer från nätverksdisken med hjälp av tre servrar i intranätet. Filöverföringsoperationen inleddes den 27 april 2024 kl. 0:01. I fyra överföringar kopierades sammanlagt cirka två terabyte uppgifter. Filöverföringen från den sista servern avslutades morgonen den 30 april 2024 kl. 8:11.



Figur 1. Angriparens filöverföringar i dataintrånget mot Helsingfors stad.

[4] Ticket är ett formbundet meddelande som används för att anmäla en observation eller ett problem. Mottagaren vidtar åtgärder och avslutar ärendet när det är slutbehandlat.

[5] En virtuell servermiljö består av en högpresterande fysisk servermiljö med stort arbetsminne och diskutrymme och som samtidigt kan ha tiotals eller hundratals virtuella Windows- eller Linux-serverprogramvaror.

[6] Gigabyte (GB) är en enhet för minnesmängd (en miljard byte). Minnet kan bestå av ett internt arbetsminne (RAM) eller ett permanent lagringsutrymme (hårddiskar, USB-minnen osv.). Terabyte är 1024 gigabyte.

På grund av övervakningen av intranätet och den bristfälliga serverloggningen kunde man inte fastställa en fullständig lista över de kopierade filerna eller deras antal. Angriparen kopierade uppgifterna i första hand på natten finsk tid, vilket minskade risken för att åka fast.

DigiHelsinkis tjänsteleverantör upptäckte det ärende som hade fastnat i kön (on hold) först den 29 april 2024 kl. 11:34 vid en inspektion som på den tiden gjordes regelbundet för att identifiera integrationsproblem. Samtidigt observerades att ärendets prioritering hade klassificerats på medelnivå (medium), även om kritisk skulle ha varit en lämpligare nivå. Klassificeringen hade inte påverkat huruvida ärendet kom fram till behandling, men det var överenskommet att man skulle säkerställa att ett ärende på kritisk nivå når fram genom ett telefonsamtal.

På grund av problemet med ärendeförmedlingen fick fostrans- och utbildningssektorns IT-personer information om de tvivelaktiga inloggningarna och försöken att knäcka lösenord som observerades den 25 april 2024 först per e-post som skickades den 29 april 2024 kl. 11:54. Utredningen av ärendet inom fostrans- och utbildningssektorn inleddes, men det fördröjdes av de serverändringar som pågick samtidigt. Det ansågs möjligt att varningarna var obefogade på grund av serverändringarna.

Den 29 april 2024 försökte angriparen också ta över andra Windows-servrar genom att knäcka deras lösenord. Angriparen inledde den 30 april 2024 kl. 01:30 en råstyrkeattack[7] för att komma in i två andra av Helsingfors stads verksamhetsområden, varvid målet var sammanlagt 165 enheter i nätverket. Samma natt kl. 03:10 försökte angriparen med hjälp av de insamlade uppgifterna också komma in i nätverken för Helsingfors stads övriga verksamhetsområden.

Försöken att utvidga attacken genom att fråga efter administrationskoder från AD-servern producerade på natten ett nytt larm hos DigiHelsinki, varvid tjänsteleverantören låste de koder som angriparen använde. Dataintrånget började avslöjas när en anställd vid DigiHelsinki den 30 april 2024 kl. 8:55 via Teams kontaktade en anställd vid fostrans- och utbildningssektorn för att utreda ärendet.

1.2 Upptäckt av dataintrånget och åtgärder

Uppgifterna om dataintrånget som upptäcktes nattetid hämtades den 30 april 2024 kl. 9:30 till fostrans- och utbildningssektorns molntjänstteams möte. Därefter fortsatte utredningsarbetet tillsammans med DigiHelsinki. Det visade sig att det var fråga om en allvarlig händelse, då inkräktaren hade kopierat dokument som fanns på nätverksdisken över till sig själv. Inom fostrans- och utbildningssektorn beslöt man att sammankalla MIM-gruppen för allvarliga störningar på stadsnivå (Major Incident Management[8]) till möte samma dag kl. 13:00, varefter MIM-möten ordnades regelbundet.

Under förmiddagen fastställde fostrans- och utbildningssektorns och DigiHelsinkis experter hur angriparen hade tagit sig in i VPN-enheten. Enhetens förbindelse till stadens datanät avbröts den 30 april 2024 kl. 13:40. Enhetens nätverkskabel lösgjordes från intranätet i maskinsalen kl. 14:30, men enheten släcktes inte så att man skulle kunna spara uppgifterna i minnet.

Efter att ha förlorat förbindelsen till fostrans- och utbildningssektorns nätverk fortsatte angriparen inloggningsförsöken i åtminstone en vecka, eventuellt även längre. Försöken

[7] Vid en råstyrkeattack (eng. brute force) testar man systematiskt olika lösenordsalternativ tills man hittar rätt alternativ.
[8] MIM-gruppen är organisationens team som ansvarar för hanteringen av stora och kritiska störningssituationer.

lyckades dock inte, eftersom åtkomsten hade blockerats genom att bryta förbindelserna till VPN-routern.

När spåren av dataintrånget undersöktes observerade man den 8 maj 2024 kl. 16:28 att det även förekom ovanlig verksamhet på säkerhetskopieringsservern utanför verksamhetsområdet. Enheten isolerades från nätverket, varefter kontrollprogrammet hittade olika versioner av skadeprogrammet Neshta[9] som ofta används vid dataintrång på dess disk. Skadeprogrammet hade skadat operativsystemet så att servern inte längre fungerade och säkerhetskopiorna inte var användbara. Återhämtningen och rengöringen av nätverket lyckades dock utan säkerhetskopior.

Fostrans- och utbildningssektorn vidtog korrigeringsåtgärder för att genomföra den nya säkerhetskopieringstjänsten. De aktiva tekniska åtgärderna för att hantera dataintrånget avslutades och fostrans- och utbildningssektorns informationssystem ansågs till dessa delar vara i ett säkert tillstånd.

Rapporterna som utredningsgruppen hade tillgång till visade att angriparen hade försökt bryta sig in i sammanlagt 1 700 datorer i Helsingfors stads nätverk. I gruppen ingick också privata skolor i Helsingfors, men försöken misslyckades.

1.3 Ledning av åtgärderna för hantering av dataintrånget

Helsingfors stad inledde den systematiska ledningen av åtgärderna för hantering av dataintrånget i och med MIM-gruppens första möte den 30 april 2024 kl. 13:00. Staden och fostrans- och utbildningssektorn tillsatte följande grupper för att leda och hantera händelsen:

MIM-gruppen för hantering av störningssituationer sammanträdde för första gången den 30 april 2024 kl. 13:00 och därefter dagligen under maj (sammanlagt 32 möten). Från och med juni sammanträdde gruppen fortfarande regelbundet flera gånger i veckan.

Krisgruppen inom fostrans- och utbildningssektorn (KASKO MIM-gruppen) hade till uppgift att dela och upprätthålla lägesbilden över sitt eget verksamhetsområde. Gruppen sammanträdde första gången den 8 maj 2024 och hade fram till den 9 augusti 2024 hållit sammanlagt 15 möten.

Stadens koordineringsgrupp drog upp riktlinjer för de viktigaste åtgärderna i anslutning till ledningen och skötseln av situationen och kommunikationsfrågorna på föredragning av digitaliseringsdirektören, fostrans- och utbildningssektorns ledning och kommunikationsledningen. Gruppen sammanträdde 23 gånger under tiden 6.5–6.8.2024.

Beredningsgruppen hade till uppgift att upprätthålla lägesbilden, bereda ärenden för ledningen samt leda kommunikationen på stadsnivå. Gruppen sammanträdde för första gången den 4 maj 2024 och därefter nästan dagligen fram till den 31 maj 2024 sammanlagt 28 gånger. Därefter sammanträdde gruppen ännu nio gånger fram till den 10 juli 2024.

Den **operativa projektgruppen** hade till uppgift att arbeta under ledning av beredningsgruppen. Gruppen sörjde för att bedömningen av föremålen för dataintrånget och dess konsekvenser genomfördes samt skötte koordinering mellan staden och externa resurser samt myndighetssamarbetet. Dessutom hade gruppen i uppgift att sammanställa en lägesbild för bered-

[9] Neshta är ett gammalt skadeprogram med flera versioner. Det samlar in uppgifter om systemet och användarna som kan användas av den som utför dataintrånget.

ningsgruppen. Gruppen utarbetade också innehåll för kommunikationen på basis av beredningsgruppens anvisningar under leding av kommunikationen. Gruppen sammanträdde för första gången den 6 maj 2024 och sammanlagt åtta gånger i maj.

För **kommunikationen** ansvarade på stadens kanslis vägnar kommunikationsdirektören och för fostrans- och utbildningssektorns del kommunikations- och marknadsföringschefen. De bildade tillsammans med kommunikationspersonerna en koordineringsgrupp som skötte den intensifierade kommunikationen. På kommunikationens möten gick man bland annat igenom mediernas begäran om intervjuer, uppdatering av vanliga frågor, nyhetsrapportering, den interna kommunikationen och utbildning i informationssäkerhet för personalen.

På **stadsnivå** behandlades händelsen också vid kommunikations-, informationssäkerhets- och dataskyddsgruppernas möten samt i samband med stadsstyrelsens och stadsfullmäktiges möten. Ärendet behandlades även vid nämnden för fostran och utbildning.

1.4 Kommunikation om dataintrånget

Helsingfors stad informerade om dataintrånget den 30 april 2024 genom att publicera en störningsbanner på stadens intranät genast när ärendet uppdagades och vidtog åtgärder för intensifierad kommunikation som leddes från stadens kansli På stadens intranät publicerades ett *störningsbanner*-meddelande där man berättade om situationen och dessutom informerade man sektorernas ledningsgrupper om ärendets utveckling per e-post.

Iltalehti var först med att rapportera om dataintrånget den 1 maj 2024 kl. 20:31 med rubriken ”Epäily: Venäjältä murtauduttu Helsingin tietoverkkoon – Henkilötietoja vaarassa.”[10] Nyheten fick stor spridning i olika medier.

Helsingfors stad publicerade ett *pressmeddelande* den 2 maj 2024 kl. 13:25 och berättade på sin webbplats om dataintrånget inom fostrans- och utbildningssektorn.[11] I meddelandet berättade staden att den som gjort dataintrånget har kommit över alla anställdas användarnamn och e-postadresser samt personbeteckningar och adressuppgifter för elever, vårdnadshavare och personal inom fostrans- och utbildningssektorn. Uppgifterna förmedlades också till stadens elever och vårdnadshavare inom den grundläggande utbildningen och på andra stadiet i Wilma och skickades till daghemmen för vidarebefordran. Dessutom publicerades nyheten på stadens intranät.

Eftersom den personuppgiftsansvarige, dvs. Helsingfors stad, dess styrelse och nämnder med stöd av lagen ansvarar för kommunikationen om personuppgiftsincidenter och för att ge ytterligare upplysningar, tog staden ansvar för koordineringen av kommunikationen. Offren för dataintrånget kunde inte identifieras, så staden meddelade dataombudsmannens byrå den 8 maj 2024 att de registrerade kommer att informeras genom offentlig delgivning.[12]

Cybersäkerhetscentret inrättade den 7 maj 2024 en intern diskussionsgrupp med fokus på dataintrånget. I gruppen deltog ett företag som undersökte dataintrånget samt centrala myndigheter. Gruppen användes för att koordinera utredningen och stöda kommunikationen.

---

[10] Nyhet i Iltalehti 1.5.2024. 26.2.2025 https://www.iltalehti.fi/kotimaa/a/8d3e0f58-76fe-42e3-acb8-41f51eb70fac

[11] Helsingfors stad: Offentligt meddelande till de grupper som eventuellt blivit offer för dataintrånget vid fostrans- och utbildningssektorn. 1.9.2024 https://www.hel.fi/sv/beslutsfattande-och-forvaltning/stadens-organisation/sektorer/stadskansliet/fostrans-och-utbildnings-dataintrang/offentligt-meddelande-till-de-grupper-som-eventuellt-blivit-offer-for-dataintranget-vid-fostrans-och

[12] Dataskyddsförordningen artikel 34.3 c.

Helsingfors stad berättade nästa gång om dataintrånget i offentligheten vid ett informationsmöte på *Helsingforskanalen*[13] den 13 maj 2024, där representanter för Helsingfors stad samt Cybersäkerhetscentret och polisen var närvarande. På plats fanns fem representanter för medierna. Uppskattningsvis 1 300 tittare följde evenemanget direkt via webben och upptagningen kunde ses på stadens webbplats.

Under informationsmötet berättade man om resultaten av utredningen av dataintrånget och gav offren anvisningar för att skydda sina egna personuppgifter. Helsingfors stad berättade att man informerar de registrerade som offentlig delgivning på webbadressen *hel.fi/tietomurto*. På webbplatsen fanns information om hur utredningsarbetet framskrider, svar på frågor och anvisningar för registrerade.[14]

På informationsmötet meddelade polisen att målsäganden i fallet är Helsingfors stad och att det inte lönar sig för enskilda medborgare att kontakta polisen för att göra en egen brottsanmälan. Samtidigt meddelade polisen att den undersöker fallet som grovt dataintrång och lovade att informera mer senare.

Cheferna som arbetar inom fostrans- och utbildningssektorn informerades vid ett Teamsmöte. Kanslichefen skickade ett e-postmeddelande till stadens personal. Via Wilma informerades vårdnadshavare, elever och personal inom den grundläggande utbildningen och på andra stadiet inom staden. Inom småbarnspedagogiken förmedlades meddelandet per e-post till familjerna.

Polisen i Helsingfors meddelade den 13 maj 2024 kl. 14:26 att den undersöker ett omfattande dataintrång i Helsingfors stads datanät. Polisen undersöker fallet för närvarande som grovt dataintrång.

Dataombudsmannen informerade den 14 maj 2024 om utredningsåtgärderna i anslutning till dataintrånget och gav anvisningar till dataintrångets offer.

Helsingfors stads kunder inom fostran och utbildning representerar över hundra olika språkgrupper.[15] Eleverna och deras vårdnadshavare informerades till en början på finska, svenska och engelska. Senare utökades informationen på bland annat ryska, arabiska och somaliska.

Grundskolornas meddelande till vårdnadshavare skickades via Wilma och småbarnspedagogikens meddelande via daghemsföreståndarna. Gymnasiernas och Stadin Ammattiopistos meddelanden skickades till eleverna och vårdnadshavarna via Wilma.

Information om dataintrånget lades till i lärarstigen Digipolku. Staden genomförde ingen separat riktad kommunikation enligt åldersnivå till minderåriga registrerade.

Staden öppnade en telefonservicekanal och en separat e-postadress för vårdnadshavarna och eleverna. För begäran om information skapades en elektronisk blankett som styrdes direkt till e-posten i anslutning till dataintrånget.

Polisen meddelade den 17 maj 2024 att Centralkriminalpolisen och polisen i Helsingfors i samarbete undersöker ett grovt dataintrång i stadens system. Polisen gav anvisningar om att var och en som misstänker att hans eller hennes uppgifter har äventyrats ska vidta åtgärder

[13] En kanal där Helsingfors stad sänder direktsändningar samt publicerar videor och poddar.
[14] Helsingfors stad. 1.9.2024 https://www.hel.fi/sv/beslutsfattande-och-forvaltning/dataintrang
[15] Vieraskielinen väestö: kieliperusteisen tilastoinnin ongelmia ja ratkaisuvaihtoehtoja. 15.1.2025 https://kaupunkitieto.hel.fi/fi/vieraskielinen-vaesto-kieliperusteisen-tilastoinnin-ongelmia-ja-ratkaisuvaihtoehtoja

för att skydda sin identitet. Polisen berättade att polisen ansvarar för informationen i anslutning till brottsutredningen och att Helsingfors stad som personuppgiftsansvarig berättar vilka uppgifter som har läckt ut ur systemen och vilka personer som berörs av detta.

Helsingfors stad publicerade ett *pressmeddelande* den 21 maj 2024 där man berättade om hur utredningsarbetet framskrider och om att de eventuella målgrupperna för dataintrånget har utvidgats. Samtidigt berättades att gärningsmannen kan ha fått tillgång till mer information än vad man tidigare uppskattat om personer som använt tjänster inom fostran och utbildning. Enligt bedömningen som gjordes då gällde dataintrånget cirka 150 000 elever och deras vårdnadshavare. Motsvarande meddelande skickades via Wilma till vårdnadshavarna, till elever inom den grundläggande utbildningen och på andra stadiet samt på daghemmen. Dessutom förmedlades meddelandet till privata daghem samt privata och statliga skolor. Torsdagen den 23 maj 2024 skickades kanslichefens meddelande om situationen till alla stadens chefer. Ett meddelande om informationen om dataintrånget sommartid förmedlades i Wilma och på daghemmen den 30 maj 2024.

Staden publicerade den 21 maj 2024 på sidan *hel.fi/uutiset* expertens anvisningar om hur man ska agera mitt i dataintrånget och berättade att den som genomfört dataintrånget kan ha fått information om alla läropliktiga i Helsingfors. Samma dag meddelade staden på sociala medieplattformen X att aktuell information om dataintrånget finns på sidan hel.fi/tietomurto.

Den interna kommunikationen förlängdes och chefsbrevet skickades ut den 23 maj 2024 för kännedom per e-post.

Personalen vid fostrans- och utbildningssektorn informerades om intensifierad övervakning av datasäkerheten på intranätet.

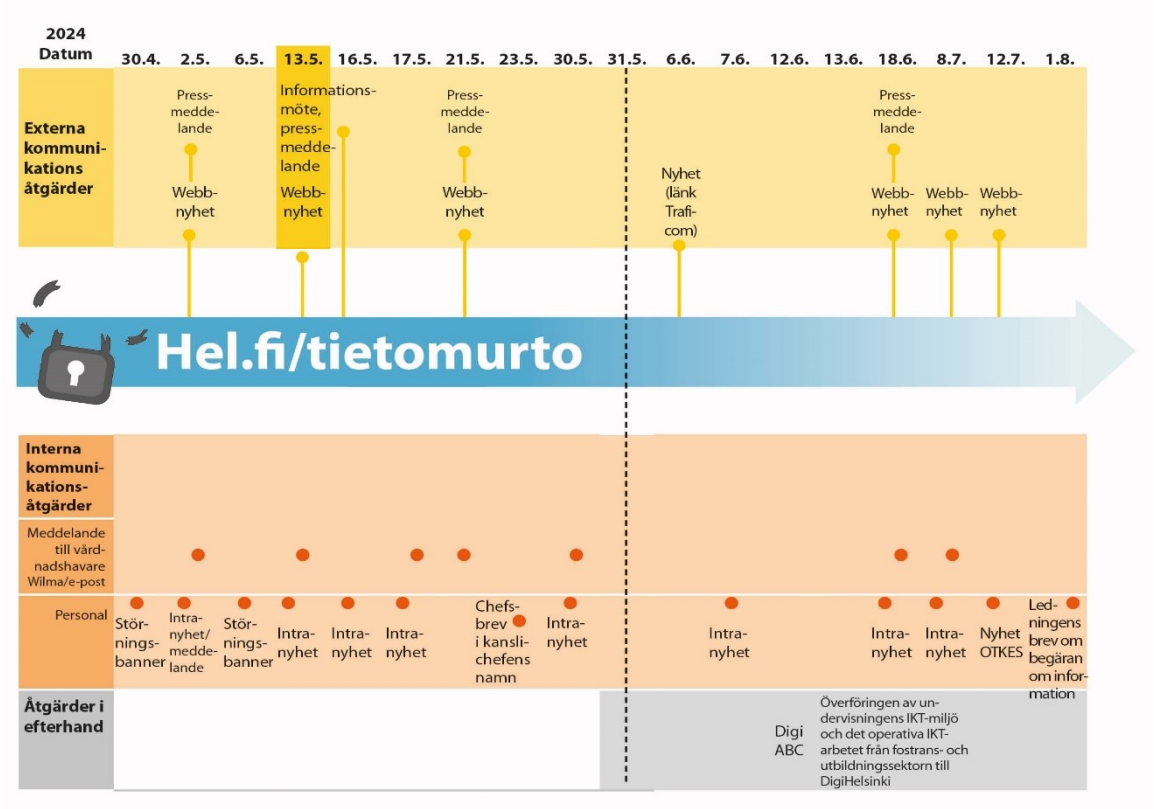
De registrerade som hade spärrmarkering kunde inte nås omedelbart efter dataintrånget. En spärrmarkering är en extraordinär åtgärd som begränsar utlämnandet av kontaktuppgifter ur befolkningsdatasystemet. Hos personer med spärrmarkering får uppgifter om adress och hemkommun lämnas ut endast till sådana myndigheter som får behandla uppgifter som omfattas av spärrmarkering.

Som åtgärder för kommunikation i efterhand publicerade staden den 6 juni 2024 en nyhet där man berättade om Transport- och kommunikationsverket Traficoms anvisningar för skydd av personuppgifter på somaliska, arabiska och ryska. Staden meddelade den 18 juni 2024 att dataintrånget mot staden inte har utvidgats ytterligare. Inspelningen *Turvaa yhteinen tietomme* publicerades på stadens intranät den 7 juni 2024.

I webbnyheten berättades den 8 juli 2024 att dataombudsmannen har fått preciserad information om dataintrånget. Staden meddelade den 12 juli 2024 att det i anslutning till Olycksutredningscentralen har inrättats en oberoende utredningsgrupp som inleder en utredning av dataintrånget mot Helsingfors stad. Motsvarande meddelanden skickades till vårdnadshavare, till elever inom den grundläggande utbildningen och på andra stadiet via Wilma medan daghemmen förmedlade meddelandena till vårdnadshavarna.

Den interna kommunikationen fortsatte i juni i form av intranätnyheter och uppdatering av DigiABC-utbildningen.

Staden publicerade den 17 december 2024 en webbnyhet om situationen kring dataintrånget och förmedlade också detta meddelande i Wilma inom den grundläggande utbildningen och på andra stadiet. Meddelandet förmedlades också inom småbarnspedagogiken.



Figur 2: Helsingfors stads kommunikationsåtgärder om dataintrånget.

1.5 Larm och räddningsåtgärder

Även om angriparen försökte agera så obemärkt som möjligt genom att använda Windows-operativsystemets interna kommandon och verktyg, orsakade verksamheten dock larm både i servrarnas och nätverksenheternas loggar. Det är svårt att identifiera den LOTL-tekniken (Living Off The Land[16]) som angriparen följer, eftersom den utnyttjar laglig programvara och vanliga systemkomponenter då användningen av dessa i allmänhet inte leder till larm.

På grund av fel i ticketingsystemet gick larmen inte från programvara för bekämpning av skadlig programvara fram till fostrans- och utbildningssektorn den 25 april 2024. Larmen förmedlades den 29 april 2024 men ingen reagerade till anmälan. Först framåt morgonen den 30 april 2024 ledde nya larm till att bekämpningsresponsen inleddes inom fostrans- och utbildningssektorn och DigiHelsinki.

[16] Living Off The Land är en cyberattackteknik där man i stället för skadeprogram i så stor utsträckning som möjligt använder målsystemets egna verktyg och resurser för skadliga ändamål.

Larmet markerat i gult

Tidpunkt		Händelse	Angripare	Helsingfors stad	Fostrans- och utbildningssektorn	DigiHelsinki Oy	Kommersiella tjänsteproducenter	Cybersäkerhetscentret	Dataombudsmannens byrå	Polisen i Helsingfors	Centralkriminalpolisen	Skyddspolisen
2014		Upphandling av Cisco ASA 5515 VPN-router till Utbildningsverket (föregångare till fostrans- och utbildningssektorn) för genomförande av fjärrförbindelser.			X							
2016		Fostrans- och utbildningssektorns senaste informationssäkerhetsuppdatering för VPN-routern, programvaran på 2015 års nivå.			X							
2017		De personer som ansvarat för underhållet av VPN-routern lämnar fostrans- och utbildningssektorn.			X							
2018		Vid sidan av ASA 5515 skaffas en nyare ASA 5545, men man hinner inte ta i bruk den innan personen som ansvarar för enheten lämnar fostrans- och utbildningssektorn.			X							
2019		Upphandlingsbeslutet för att skaffa nya VPN-enheter för att ersätta de gamla godkänns, men enheterna skaffas dock inte.		X	X							
2020		De som använder VPN-routern börjar övergå till nya DigiHelsinkis fjärranvändningstjänst.			X	X						
29.2.2024		Råstyrkeattack (brute force) mot fostrans- och utbildningssektorns nätverk 29.2–4.4.2024.	X									
31.3.2024		Dustin Oy uppdaterar via fjärrförbindelse VPN-routerns certifikat, som gäller ett år framåt.			X	X	X					
8.4.2024		Råstyrkeattack 8.4–12.4.2024 genom vilken teknisk information om fostrans- och utbildningssektorns nätverk och den föråldrade VPN-routern samlas in.	X									
14.4.2024	20:14	VPN-routern kraschar till följd av att en sårbarhet utnyttjas. Saken undersöks inte närmare.	X		X							
18.4.2024	11:17	Det är sannolikt angriparens första inloggning i VPN-routern.	X									
23.4.2024	11:14	Angriparens kartlägger fostrans- och utbildningssektorns IT-infrastruktur, vilket registreras i loggarna, men det saknas aktiv övervakning och inget larm utlöses.	X									
25.4.2024	13:17	Angriparen får för första gången ett fotfäste i fostrans- och utbildningssektorns intranät.	X									
	13:40	Inloggningen utlöser det första informationssäkerhetslarmet på låg nivå kl. 13:40 och larm på hög nivå kl. 13:59 samt efter detta larm från nio olika enheter.				X	X					
	15:07	Angriparens första inloggning i fostrans- och utbildningssektorns server via fjärrförbindelse.	X									
	17:22	Programvaran mot skadlig kod larmar om misslyckade inloggningsförsök. DigiHelsinkis underleverantör öppnar ett ärende på medelsvår nivå om sina observationer. Ärendet styrs kl. 18.36 till en annan underleverantör som handhar integrationen av Helpdesk nivå och andra tjänster för olika aktörer.					X					
	18:40	Angriparen kommer över administratörens rättigheter till två Microsoft Windows-domäner, servern för hantering av virtuell servermiljö och säkerhetskopieringssystemet.	X									
26.4.2024	2:54	Angriparen inleder den första dataöverföringen på 1,03 GB till en server utomlands. Överföringen varar tre minuter.	X									
27.4.2024	0:01	Angriparen inleder tre större dataöverföringar till en server utomlands.	X									
29.4.2024	11:34	25.4 kl. 17.22 upptäcks det inlämnandet ärendet (ticket) och behandlas. På grund av ett tekniskt fel har ärendet stannat i on hold-läge.				X	X					
	11:54	Fostrans- och utbildningssektorn får det första larmet om ett eventuellt dataintrång från DigiHelsinkis helpdesk om inloggningsförsöken och försöken att knäcka lösenord 25.4.			X	X	X					

Larmet markerat i gult

Tidpunkt		Händelse	Angripare	Helsingfors stad	Fostrans- och utbildningssektorn	DigiHelsinki Oy	Kommersiella tjänsteproducenter	Cybersäkerhetscentret	Dataombudsmannens byrå	Polisen i Helsingfors	Centralkriminalpolisen	Skyddspolisen
30.4.2024	1:30	Angriparen inledde en råstyrkeattack på 165 datorer för att komma åt två andra domäner vid Helsingfors stad. Klockan 3.19 försökte angriparen bryta in sig i Helsingfors stads övriga sektorers nätverk, vilket utlöste larm i programvarorna mot skadlig kod.	X									
	9:30	De larm som inträffade framåt morgonen behandlas på DigiHelsinkis och fostrans- och utbildningssektorns ordinarie möte. Misstanken om ett data-intrång fastställs och information om dess svårighetsgrad börjar klarna.			X	X						
	13:00	På basis av förmiddagens uppgifter inleds MIM-störningshanteringsgruppens verksamhet och det första mötet ordnas kl. 13.00.		X	X	X						
	13:40	På basis av den utredning som görs under dagen fastställs det att angriparen har kommit åt fostrans- och utbildningssektorns intranät via Cisco ASA 5515 VPN-routern som lösgjordes från nätverket.			X	X						
		Helsingfors stad lämnar myndighetsanmälningar till Cybersäkerhetscentret, Dataombudsmannens byrå och polisen i Helsingfors.		X	X			X	X			
		Kritiska lösenord till nätverket och servrarna började förnyas.			X	X						
1.5.2024		Brottsanmälan gjort 1 maj på morgonen.								X		
		I fostrans- och utbildningssektorns nätverk isolerar man eller stänger ner de servrar som man vet att angriparen har gjort intrång i. Projektet för att förnya lösenorden fortsätter.			X	X						
2.5.2024		Informationsutbyte mellan Cybersäkerhetscentret vid Traficom och fostrans- och utbildningssektorn.			X			X				
3.5.2024		En extern tjänsteproducent inleder hanterings- och utredningsåtgärder på uppdrag av Helsingfors stad.			X		X					
		Den nätverksdisk som var föremål för dataintrånget lösgörs från fostrans- och utbildningssektorns nätverk och flyttas till en annan säker server.			X	X						
		Skyddspolisen kontaktar Helsingfors stad.			X							X
4.5.2024		Beredningsgruppen inleder sin verksamhet.		X	X	X						
		Den externa tjänsteproducenten inleder en begränsad informationssäkerhet-sövervakning 24/7 (SoC, Security Operation Center).			X		X					
8.5.2024		Säkerhetskopieringssystemet fastställs vara skadat och oanvändbart, men det finns inget behov för det.			X	X						
9.5.2024		Cybersäkerhetscentret inleder en särskild övervakning av det som skett.			X		X	X		X		
13.5.2024		Helsingfors stad ordnar ett öppet informationsmöte.		X	X			X		X		
31.5.2024		Nätverksdisken fungerar på den nya plattformen och öppnas åter för personalens bruk.		X	X							

Figur 3. Tidslinje för dataintrånget och återhämtningen.

De datatekniska räddningsåtgärderna inleddes egentligen den 30 april 2024 kl. 13:40 när fostrans- och utbildningssektorns och DigiHelsinkis personal stängde åtkomsten till VPN-routern. Experterna förhindrade först användningen av enheten och därefter lösgjordes enheten fysiskt från nätet. Elen bröts dock inte för att man skulle kunna spara uppgifterna i enhetens RAM-minne[17] för en noggrannare undersökning. I utredningen av logg- och andra digitala spår som hittades i enheten användes tillverkarens experttjänster utomlands som hjälp.

Administratörerna för fostrans- och utbildningssektorns intranät uppmanades den 30 april 2024 kl. 17:15 att byta sina lösenord. Samtidigt inleddes byte av lösenord till servrarnas lokala och tekniska användarnamn, som fortsatte den 1 maj 2024. Samma dag började

[17] RAM-minne (Random-Access Memory) är IT-enhetens interna minne.

fostrans- och utbildningssektorn och DigiHelsinki isolera och stänga servrar som utsatts för dataintrånget.

När misstanken om dataintrånget uppdagades gjorde Helsingfors stad anmälningar till följande myndigheter:

- Cybersäkerhetscenter vid Transport- och kommunikationsverket Traficom den 30 april 2024
- Dataombudsmannens byrå den 30 april 2024
- Brottsanmälan till polisen den 1 maj 2024, som registrerades i polisens system som grovt dataintrång som inleddes den 30 april kl. 4:26.

Vid tidpunkten för anmälningarna hade man ingen uppfattning om dataintrångets omfattning eller allvar. I anmälningarna beskrevs att den som gjorde dataintrånget fått tillgång till användarnas och underhållets domännamn samt e-postadresser.

Cybersäkerhetscentret fick för första gången kännedom om en personuppgiftsincident inom Helsingfors stad den 30 april 2024 kl. 23:30. Helsingfors stad gjorde den första anmälan på blanketten ”Anmäl en informationssäkerhetsincident” på Cybersäkerhetscentrets webbplats. Anmälan besvarades för första gången 12 timmar efter den första anmälan, dvs. den 1 maj 2024 av jourhavande vid Cybersäkerhetscentret. Cybersäkerhetscentret inledde ett informationsutbyte i ärendet den 1 maj 2024. Ärendet togs upp till behandling vid Cybersäkerhetscentret för första gången den 1 maj 2024 kl. 19:30.

Avvikelsen som anmälts på basis av de uppgifter som angetts i den första anmälan som Cybersäkerhetscentret mottog verkade inte i centrets bedömning av fallets allvarlighetsgrad vara sådan att den skulle ha krävt omedelbara åtgärder av Cybersäkerhetscentret som avviker från den normala processen. Utifrån uppgifterna i anmälan verkade situationen vara väl under kontroll inom Helsingfors stad: bland annat hade man skaffat en utomstående partner för att utreda fallet och man hade redan vidtagit begränsningsåtgärder i anslutning till informationssäkerhetsincidenten.

Cybersäkerhetscentret aktiverade samordningen av Helsingfors stads informationssäkerhetsincidenter mellan olika myndigheter och andra aktörer.

Dataombudsmannens byrå tog emot anmälan om informationssäkerhetsincidenten och började behandla den i enlighet med sin normala undersökningsprocess. Dataombudsmannens byrå vidtog inga omedelbara åtgärder, men bad fostrans- och utbildningssektorn komplettera materialet som den lämnat in. Fostrans- och utbildningssektorn svarade på dataombudsmannens tilläggsbegäran den 9 maj 2024, den 5 juni 2024 och den 8 juli 2024.

Utredningsledaren vid polisen i Helsingfors kontaktade fostrans- och utbildningssektorn den 2 maj 2024.

Helsingfors stad bad en känd kommersiell aktör den 30 april 2024 om utomstående hjälp för att hantera och undersöka informationssäkerhetsincidenten, men aktören hade inte beredskap att leverera tjänsten i Finland. Därefter vände sig fostrans- och utbildningssektorn till Elisa Santa Monica, som inledde utredningsåtgärderna för dataintrånget den 3 maj 2024 kl. 8:00. De startade en datasäkerhetsövervakning dygnet runt den 4 maj 2024 kl. 17:00 och lyckades preliminärt försäkra sig om att attacken endast riktades mot fostrans- och utbildningssektorns IT-miljö och att angriparen inte hade fått tillgång till andra sektorers IT-miljöer.

Elisa Santa Monica avslutade utredningen av dataintrånget den 11 september 2024, varefter de lämnade in en rapport till Helsingfors stad den 7 oktober 2024. Samarbetet fortsatte genom att producera informationssäkerhetstjänster för Helsingfors stad.

Som skyddsåtgärd tog man den 2 maj 2024 i bruk ett tekniskt landskydd (geoblockering), som begränsade inloggningen i Helsingfors stads tjänster utanför Finlands gränser.

Fostrans- och utbildningssektorn lösgjorde den nätverksenhet som utsatts för attacken och förhindrade dess användning den 3 maj 2024. I samband med detta flyttades nätverksenheten från den server som var föremål för dataintrånget till en ny plattform som var säkrad i fråga om informationssäkerheten och där experterna fick undersöka enheten.

Skyddspolisen kontaktade Helsingfors stad den 3 maj 2024 och bad om mer information eftersom man i medierna hade lyft fram en eventuell koppling till Ryssland.

Huvudanvändarna började byta lösenord till servrar och nätets huvudanvändare och servicekoder den 3 maj 2024. I detta sammanhang förnyades certifikat som intygar servrarnas äkthet och de gamla certifikaten togs ur bruk.

Tekniska och kommunikationsåtgärder för att hantera dataintrånget

Elisa Santa Monica, som hjälpte med att utreda dataintrånget, inledde en utredning (dataintrångsundersökningstjänst) i syfte att identifiera omfattningen av angriparens åtkomst, förhindra att angreppet spreds till nya enheter samt att eventuella aktiva fotfästen avlägsnades från miljön. Därefter var den centrala åtgärden att säkerställa att inga bakdörrar lämnades kvar i miljön för att angriparen skulle kunna återvända.

Företaget startade upp ett kontrollrum för datasäkerhet dygnet runt (Security Operation Center, SoC), vars verksamhet utvidgades den 14 maj 2024 genom att installera mer avancerade terminalövervakningssensorer på fostrans- och utbildningssektorns servrar och enheter för att upptäcka informationssäkerhetsincidenter.

Som en säkerhetsåtgärd stängdes en domain controller-server i två olika AD-domäner för att skydda uppgifterna i användarkatalogen.

För huvudanvändarna togs i bruk nya arbetsstationer som säkert är fria från skadliga programvaror. Överföringen av filer från den nätverksenhet som utsattes för dataintrånget till en annan server började förberedas den 6 maj 2024.

Den 9 maj 2024 började man ta skivavbilder av enheterna som inte längre fanns i nätverket eller fjärrhanteringen för att utreda dataintrångets omfattning.

Som första åtgärder för kommunikationen lade Helsingfors stad den 30 april 2024 omedelbart upp en *störningsbanner* på intranätet och informerade offentligt om dataintrånget den 2 maj 2024.

Cybersäkerhetscentret vid Transport- och kommunikationsverket gav också utredningshjälp bland annat i anslutning till insamling av material som är kritiskt för informationssäkerhetsutredningen. Centret bistod Helsingfors stad och den leverantör av informationssäkerhetstjänster som staden anlitade i insamlingen av kriminaltekniskt undersökningsmaterial som var kritiskt med tanke på utredningen av situationen kring dataintrånget och dess omfattning från servrar som var föremål för dataintrånget. Dessutom gjorde Cybersäkerhetscentret i början av utredningen då situationen var som allvarligast också en egen analys av händelsen.

Svar på begäran om information

Helsingfors stad började den 2 maj 2024 planera en tjänst som skulle kunna svara på begäran om granskning av personuppgifter som fanns lagrade på nätverksenheten Eftersom det inte fanns något lämpligt färdigt program beslöt teamet för data och ny teknik som hör till digitaliseringsenheten vid stadens kansli att bygga upp ett separat system för detta.

Staden öppnade den 13 maj 2024 ett webbformulär på sin webbplats, med vilken en starkt identifierad användare kunde lämna en begäran om granskning av sina egna och vårdnadshavarnas uppgifter. Därefter söker de personer som utsetts för uppgiften uppgifter om de personer som ska granskas i handlingarna utifrån personbeteckning och elevnummer. Resultaten skickades till den som bad om dem antingen elektroniskt med krypterad e-post, traditionell brevpost eller avhämtas från registratorskontoret beroende på hur den som begärde handlingarna önskade ta emot dem.

Ansökan begränsades till personbeteckningar och elevnummer, eftersom det är omöjligt att skilja personer med samma namn från varandra genom att enbart söka med namn. Dessutom visste man att största delen av de handlingar som innehöll personuppgifter innehöll någon av dessa tre identifierare. En helt fri textsökning på basis av namn, adress eller telefonnummer skulle ha ökat risken för att personuppgifter lämnas ut till fel person.

Nätverksenheten som var föremål för dataintrånget kopierades till en nätverksenhet i DigiHelsinkis tjänsteleverantörs datorsal den 19 maj 2024.

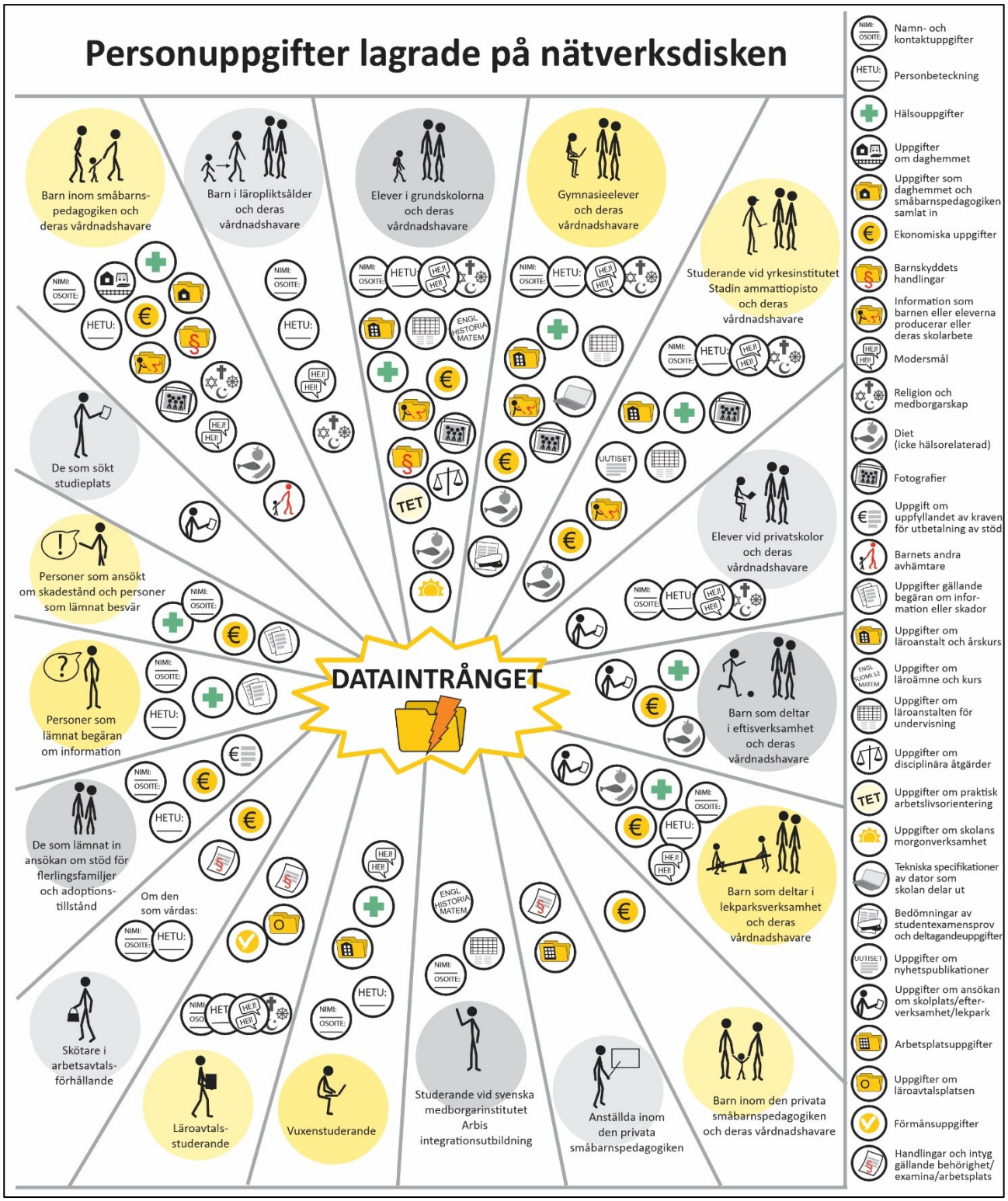
Den nya nätverksenheten sattes i teknisk drift så att kunde användas av personalen den 31 maj 2024, när filerna hade kontrollerats och säkrats med två datasäkerhetsprogram för att hitta eventuella skadliga programvaror. Användarna fick anvisningar om att filer inte får raderas och att nya filer inte får sparas på nätverksenheten. Eventuella nya filer skulle sparas på den personliga H-disken.

1.6 Följder

Till följd av dataintrånget fick angriparen tillgång till en stor mängd information från AD-användardatabasen och från nätverksenheten. Uppgifterna innehöll personuppgifter och en del av dem hör till särskilda kategorier av personuppgifter[18] eller var på annat sätt sekretessbelagda.

Det material som omfattades av dataintrånget innehöll uppgifter om hundratusentals människor. En del av dessa gällde personalen vid fostrans- och utbildningssektorn eller Helsingfors stad, en del eleverna och deras vårdnadshavare. Dessutom innehöll nätverksenheternas handlingar uppgifter om andra personer, företag och andra samarbetspartner som uträttat ärenden indirekt eller direkt med staden.

[18] Med särskilda personuppgifter avses uppgifter av vilka framgår en persons ras eller etniska ursprung, politiska åsikt, religiösa eller filosofiska övertygelse, medlemskap i ett fackförbund, hälsotillstånd, sexuella läggning eller beteende, genetiska och biometriska uppgifter som kan användas för att identifiera en person.



Figur 4. Datainnehåll som fanns på nätverksenheten per persongrupp.

Stängningen av nätverksdisken försvårade fostrans- och utbildningssektorns dagliga verksamhet särskilt i maj 2024. Flera av fostrans- och utbildningssektorns informationssystem för hantering av IT-infrastruktur eller produktion av tjänster var ur bruk, vilket påverkade fostrans- och utbildningssektorns interna verksamhet och de tjänster som erbjuds kunderna även ännu hösten 2024.

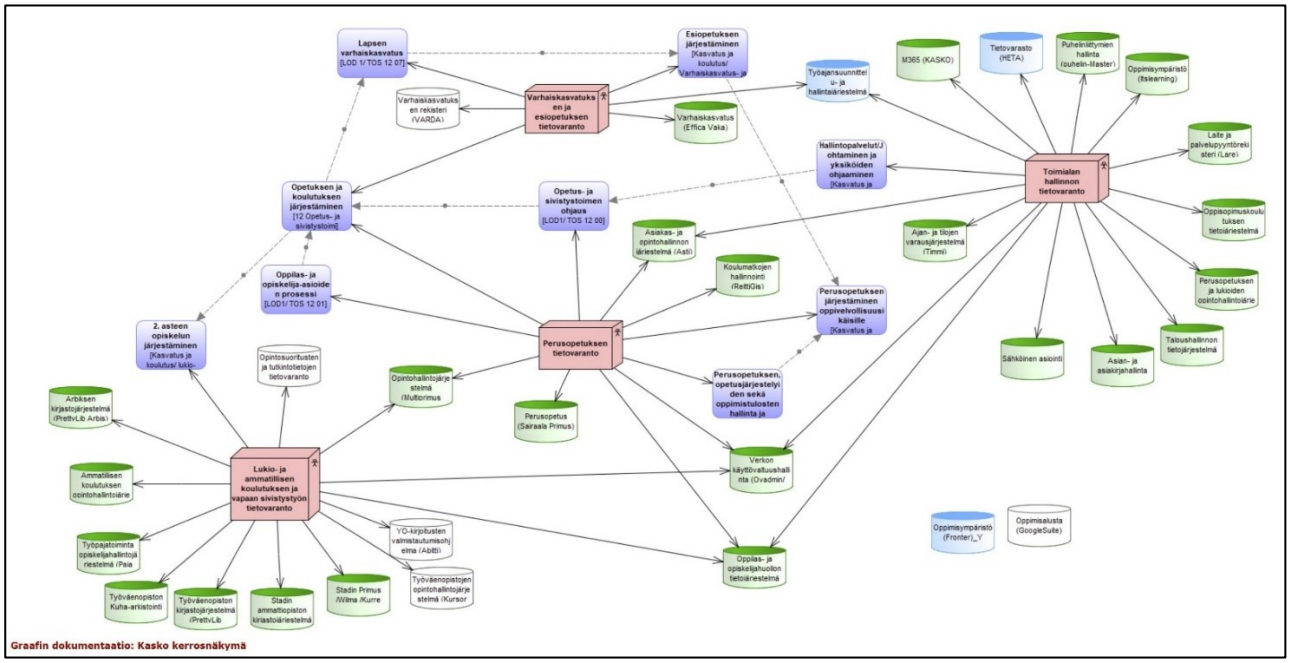
Utredningen och åtgärdande av händelsen orsakade betydande kostnader för Helsingfors stad. De direkta kostnaderna för undersökningar och återställande åtgärder efter datainträngetunder maj–september 2024 uppgick till cirka 650 000 euro. Dessutom orsakade bland annat ibruktagandet av nya informationssäkerhetstjänster kostnader på minst 400 000 euro. En del av dessa investeringar kan anses vara reparationsskuld för föråldrad IT-infrastruktur. Utredningen av händelsen och de utvecklingsåtgärder som inleddes på basis av den påverkade också genomförandet av andra planerade ICT-projekt inom Helsingfors stads sektorer.

Dessutom var Helsingfors stads personal och dess underleverantörer som producerar IT-tjänster tvungna att utföra en betydande mängd övertidsarbete i synnerhet i maj–juni. Dessa kostnader utreddes inte närmare i utredningen.

2 VERKSAMHETSMILJÖ, ANORDNINGAR OCH SYSTEM

Helsingfors stad använder nästan 600 separata informationssystem. Fostrans- och utbildningssektorn har sammanlagt cirka 300 egna system. Systemhelheten har bildats under en lång tid. Typiska problempunkter för en sådan helhet är splittrade system, informationsutbytet mellan dem och hanteringen av den tekniska livslängden. Det har dessutom varit svårare att skapa en bild av helheten på grund av att förfarandena för ibruktagande av informationssystem inte alltid är standardiserade. Särskilt snäva informationssystem som reserverats för vissa uppgifter tas i eller ur bruk som en del av normala förändringar i verksamheten och dessa ändringar behandlas eller dokumenteras inte alltid.

I arkitekturbeskrivningarna för Helsingfors stads informationssystem fanns inte den nätverksdisken som var föremål för dataintrånget beskriven. Nätverksdisken saknades uppenbarligen i beskrivningarna antingen för att den inte hade betraktats som ett informationssystem eller för att nätverksdiskar håller på att hamna i skuggan när olika molntjänstmiljöer tas i bruk. Före coronaepidemin hade nätverksdisken en större roll i fostrans- och utbildningssektorns verksamhet vid Helsingfors stad. Sedan dess har man i större utsträckning övergått till att använda Teams och Office 365, som upplevs som smidigare än nätverksdiskar. Denna trend fortsatte också efter att den nätverksdisk som var föremål för dataintrånget togs i bruk på nytt.



Figur 5. Fostrans- och utbildningssektorns beskrivning av informationssystemarkitekturen. (Bild: Helsingfors stad)

Helsingfors stad har stegvis övergått till att använda Microsofts M365-tjänster sedan 2022.[19] I samband med ibruktagandet har staden i allt högre grad börjat använda molntjänster.

[19] Ibruktagande av Microsofts M365-tjänster vid Helsingfors stad. 26.2.2025 https://paatokset.hel.fi/fi/asia/hel-2022-012015

Helsingfors stads kanslichef har den 12 oktober 2022 gett anvisningar om behandling av personuppgifter vid ibruktagandet av molntjänster.[20]

Ahjo-systemet[21] är Helsingfors stads ärendehanteringssystem. Enheten för förvaltningsförfarande och staben vid stadskansliets förvaltningsavdelning ansvarar för utvecklingen och upprätthållandet av systemet. I Ahjo registreras och sparas ärenden och handlingar som anhängiggörs hos myndigheten samt upprättas och lagras allmänna administrativa beslut, såsom upphandlingsärenden, ärenden som gäller tillsättande av tjänster samt ärenden som gäller ekonomiskt beslutsfattande. Beslut av tjänsteinnehavare finns också i Helsingfors stads övriga informationssystem och de gäller skötsel av speciallagstiftning eller andra specialuppgifter.

Beredningen av beslut genomförs vanligtvis så att den person som bereder ärendet upprättar ett utkast till handling och tilläggsmaterial som Word- eller Excel-filer. Beredaren sparar dessa filer under tiden för bearbetningen på en nätverksdisk, i en molntjänst eller på en gemensam nätverksdisk. På basis av materialet som upprättats bereds beslut i ärendehanteringssystemet genom att bifoga handlingar eller kopiera texter från dem till beslutshandlingen.

Problemet med det beskrivna arbetsflödet är att handlingar i beslutsärendet kopieras till flera lagringsställen, varav endast det egentliga ärendehanteringssystemet har egenskaper för hantering av ärendets livscykel. I andra lagringsplatser förutsätter hanteringen av handlingarnas livscykel att användaren själv vidtar åtgärder, såsom att filen raderas. Beredarnas arbetssätt vid förvaltningsärenden har varit att lämna tidigare dokument på nätverksdisken och i molntjänsten, eftersom de används som underlag vid beredningen av följande ärenden.

I enlighet med Helsingfors stads plan för informationsstyrning har en del av besluten fattats utanför ärendehanteringssystemet och dessa beslutshandlingar har sparats på en nätverksdisk. På detta sätt har man särskilt behandlat beslut som gäller arbetsgivarverksamheten.

Vanligtvis är dock största delen av de handlingar som upprättas annat än egentligt beslutsmaterial. Detta är vanligt i den faktiska förvaltningsverksamheten, såsom i undervisningsarbetet. Det har inte funnits någon systematisk hantering och lagringsmiljö för det material som utarbetats i detta syfte och praxisen har varierat mellan upprättarna och verksamhetsenheterna, såsom skolor eller daghem.

Helsingfors stad fattade ett upphandlingsbeslut om dokumenthanteringssystemet den 8 november 2023. Beslutet har inte kunnat genomföras eftersom marknadsdomstolen den 26 april 2024 upphävde upphandlingsavtalet på grund av ett formfel.

Fostrans- och utbildningssektorns centrala kunddatasystem är Effica Vaka för småbarnspedagogiken, MultiPrimus för den grundläggande utbildningen, gymnasierna och yrkesutbildningen, AURA för elevvården inom den grundläggande utbildningen och gymnasierna, AMMAURA för elevvården inom yrkesutbildningen samt Wilma för informationsutbytet mellan hemmet och skolan. Dataintrånget gällde inte direkt informationsmaterialet i kunddatasystemen, men föremålet för dataintrånget var filer som till exempel var rapporter om uppgifter i kunddatasystemen eller beredningshandlingar för

[20] Förutsättningar som gäller det geografiska läget för och överföringen av personuppgifter och sekretessbelagda uppgifter. 26.2.2025 https://paatokset.hel.fi/fi/asia/hel-2022-012014?paatos=252eaeba-1bed-4edb-a7a7-a0b55ee0f9f2

[21] Ahjo är ett dokumenthanteringssystem med vilket handlingar kan styras till rätt aktörer i organisationen.

lagring i kunddatasystemet. AURA och AMMAURA har sedermera ersatts med det Kanta-kompatibla Apotti-systemet.

2.1 Dataintrånget mot VPN-router

Dataintrånget gjordes på Ciscos brandvägg av typen ASA 5515 (Adaptive Security Appliance). I fostrans- och utbildningssektorn användes den som en router som tog emot VPN-förbindelser.[22] Fjärrförbindelsen från användarens dator till routern skapas med Ciscos AnyConnect-program, varefter fjärranvändaren får säker tillgång till intranätet.

Figur 6. Cisco ASA 5515 VPN-router som var föremål för dataintrånget enligt utredningen i oktober 2024.

ASA 5515 är en prisvärd produkt med begränsad prestanda och begränsade egenskaper i Ciscos kollektion som stöder upp till 250 samtidiga användare. Den hade skaffats åt fostrans- och utbildningssektorns föregångare Utbildningsverket 2014 för att göra det möjligt för ämbetsverkets IT-personal att få tillgång till intranätet för undervisningen samt via hoppservern även till förvaltningsnätet. Näten är helt självständiga, men hoppservern är kopplad till båda näten och möjliggör kontrollerad trafik mellan näten.

Ciscos ASA 5515-modell nådde slutet av sin livscykel 2017 när dess produktstöd upphörde. I februari 2017 meddelade tillverkaren EOL-tidtabellen (End-of-Life), enligt vilken mottagningen av beställningar skulle upphöra i augusti samma år, men tillgången till reservdelar för kunder som ingått serviceavtal garanterades fram till augusti 2022. Stödet för programvaran fortsätter, eftersom samma programvara också fungerar i nyare enheter i ASA-serien. I slutet av april 2024 var den senaste programversionen 9.12.4, vilken enheten borde ha uppdaterats

[22] En VPN-router är en enhet som fjärranvändare ansluter till via internet. Därefter bildar VPN (Virtual Private Network) en skyddad tunnel genom vilken användaren tryggt kan använda filer och servrar på intranätet.

till om man hade velat hålla den så säker som möjligt. Uppdatering av programvaran förutsätter ett avgiftsbelagt stödavtal, men korrigeringar av kritiska fel publicerar Cisco för alla som använder enheten.

Fostrans- och utbildningssektorn kände till att stödet för ASA 5515 upphörde och i slutet av 2018 skaffades en nyare ASA 5545-apparat för VPN-användning, med vilken man hade för avsikt att dubblera fjärranslutningarna. Personen som ansvarade för upphandlingen och underhållet av enheten lämnade dock fostrans- och utbildningssektorn våren 2020, då ibruktagandet av 5545 apparaten ännu pågick. Brandväggen lämnades fysiskt och färdigt konfigurerad i datorsalens utrustningsrack ovanför den gamla 5515-enheten, men den kopplades inte till nätet och hade ingen eltillförsel.

Fostrans- och utbildningssektorns egen IT-personal ansvarade för installationen och det dagliga underhållet av ASA 5515. De nyckelpersoner som ansvarade för enhetens datasäkerhet slutade dock i fostrans- och utbildningssektorns tjänst 2017 och de hade ingen skriftlig dokumentation. Våren 2024 användes ASA 5515 fortfarande utan att någon särskilt övervakade dess funktion.

År 2019 gjordes ett upphandlingsförslag för att ersätta Ciscos två nya VPN-enheter. Förslaget godkändes enligt fostrans- och utbildningssektorns normala praxis, men av okänd anledning beställdes dessa enheter aldrig.

Figur 7. Enhetsskåpet i fostrans- och utbildningssektorns datorhall i oktober 2024. Figuren visar en VPN-reservenhet ASA 5545 som aldrig togs i bruk. ASA 5515 som användes vid dataintrånget låg under den.

Överföringsprojektet för VPN-routrarna inleddes 2020 när man började överföra fostrans- och utbildningssektorns anställdas användarnamn från ASA 5515 till det nyare VPN-systemet som upprätthålls av DigiHelsinki. Överföringsprojektet framskred normalt, men ansågs inte vara särskilt brådskande. Fostrans- och utbildningssektorns IT-personal sysselsattes mer av

att bygga datakommunikationsförbindelser i skolorna och uppdatera de aktiva enheterna i nätverket.

Våren 2024 fanns det ännu 20–30 användarnamn som inte överförts från ASA 5515 VPN-enheten. Vissa användare hade ett användarnamn för både det nya och det gamla VPN. De återstående ASA 5515-användarna var främst partnerföretag, såsom underleverantörer som ansvarade för övervakningskameror och passerkontrollutrustning.

Under 2019 beredde Helsingfors stad projektet Digitaalinen perusta, vars verksamhet inleddes i början av 2021. Den nya organisationen rekryterar två datakommunikationsexperter från fostrans- och utbildningssektorn. Produktionsansvaret för datakommunikationstjänster överfördes i detta sammanhang till Digitaalinen perusta.

Det gjordes ingen skriftlig lista över de enheter som överfördes från fostrans- och utbildningssektorn, så situationen kring ASA 5515 förblev oklar. Digitaalinen perusta (från början av 2023 bolagiserades under namnet DigiHelsinki Oy) att enheten fortfarande hör till fostrans- och utbildningssektorns ansvar. Å andra sidan utfördes det praktiska underhållet av ASA 5515 också av tidigare anställda vid fostrans- och utbildningssektorn som flyttat till DigiHelsinkis organisation.

Underhållsåtgärderna omfattade främst uppdatering av certifikatet och hantering av användarnamn. Eftersom edu.hel.fi-certifikatet som hänför sig till serverns adress endast gäller ett år åt gången måste certifikatfilen förnyas regelbundet. DigiHelsinki beställde uppdateringsarbetet av ett utomstående företag som det hade ett gällande avtal med. Den senaste uppdateringen av certifikatet genomfördes i mars 2024, eftersom certifikatet höll på att gå ut den 1 april 2024.

I Ciscos ASA-enheter kan programvaran och certifikatet uppdateras lokalt med ett USB-minne eller över nätet via fjärrförbindelse. Det kommersiella företag som fungerade som underleverantör utförde de begärda underhållsåtgärderna på distans och testade att ändringarna fungerade, men granskade inte serverns programversioner eller funktionsinställningar som en helhet.

VPN-användarnamn till ASA 5515-enheten hade skapats endast för fostrans- och utbildningssektorns personal och personalen hos utkontrakterade tjänsteleverantörer. Eleverna hade inga fjärranvändarnamn till enheten. Användarna verifierade sig själva i VPN med användarnamn och lösenord. Stark autentisering, såsom ett engångslösenord som skickas per sms eller en separat autentiseringsapplikation, användes inte, eftersom detta inte kunde krävas av användare med personliga telefoner.

Rektorerna, prorektorerna, speciallärarna och lärarna inom yrkesutbildningen använde telefon som staden skaffat. Endast en del av de övriga lärarna hade en telefon från arbetsgivaren. De som använde personlig telefon ville inte installera en separat autentiseringsapplikation i sin telefon eller meddela sitt personliga nummer till arbetsgivaren, så stark autentisering kunde inte genomföras.

VPN-routerns konfiguration innehöll ett avgörande fel med tanke på dataintrånget. Konfigurationsfilen innehåller vanligtvis tiotals eller till och med hundratals inställningar som kan ändras och som definieras med hjälp av ett grafiskt användargränssnitt eller genom att redigera en textfil direkt.

Utöver de tekniska funktionsinställningarna listas i konfigurationsfilen per användargrupp de rättigheter som beviljas för intranätet. Om användarnamnet inte hör till någon specificerad

grupp får det standardrättigheter (default-group-policy). I VPN-serverns konfigurationsfil fanns en felaktig inställning:

```
default-group-policy AC-TUKI
```

Definitionen gav AC-TUKI-gruppens rättigheter till alla dem som inte hörde till någon särskilt utsedd grupp. Gruppnamnet AC-TUKI hänvisar till AnyConnect-programmet och den grupp som IT-stödet skapat för sig själv och för vilken det på annat håll i konfigurationen hade fastställts omfattande åtkomsträttigheter till hela intranätet för utredning och korrigering av fel.

Rätt inställning skulle ha varit:

```
default-group-policy DENY
```

Detta skulle ha förhindrat åtkomst till intranätet för andra användare än dem som beviljats åtkomsträtt separat. I modell 5545 som hade skaffats som reservenheten hade DENY-inställningen gjorts korrekt.

I utredningen kunde man inte fastställa varför eller när de felaktiga inställningarna hade gjorts i konfigurationsfilen. De ursprungliga installatörerna hade lämnat Helsingfors stads tjänst i samband med organisationsreformen 2017. I konfigurationsfilen hittades inga tidigare versioner vilka man skulle ha kunnat använda för att dra slutsatser om tidpunkten för tillägget.

Angriparen lyckades logga in på VPN-routern med två elevers användarnamn och lösenord. Sannolikt hade uppgifterna hamnat på mörka webben till följd av ett tidigare, odefinierat dataläckage.

Elevnummer gav inte rätt till fjärranvändaning av servern. Koderna stämde dock överens med utbildningsväsendets gamla användardatabas och därför gav VPN-routern felaktigt dem AC-TUKI-gruppens rättigheter.

Enbart teknisk åtkomst räcker inte till för att läsa filer eller använda filservrar. Därför började angriparen undersöka intranätet genom att systematiskt skanna servrar och leta efter metoder för att utvidga sina användarrättigheter. På ett sätt som inte helt kunde fastställas i utredningen lyckades angriparen logga in med admin-rättigheter[23] med fjärrförbindelse till intranätets server.

Efter att ha fått ett fotfäste på den första servern i intranätet kunde angriparen knäcka andra användarkonton och på så sätt utvidga sin åtkomst. Angriparens agerande underlättades av att samma lösenord användes med admin-användarnamn på flera servrar. Angriparen kom också över admin-användarnamn till säkerhetskopieringsservern, med hjälp av vilket angriparen kunde läsa hela filserverns innehåll.

På en server hittade angriparen de lösenord som administratören sparat i webbläsarens interna lager. Bland dem fanns både personliga lösenord och lösenord till fostrans- och utbildningssektorns servrar.

2.2 Dataintrånget på nätverksdisken

Windows-filservern (nedan ”nätverksdisk”) skaffades till Utbildningsverket för uppskattningsvis 15–20 år sedan. Enhetens exakta historia kunde inte fastställas i utredningen. Under

[23] Admin-rättigheterna (administrator) är mer omfattande än basanvändarens rättigheter och med dem kan man vanligtvis ändra inställningarna samt ta kontroll över andra användares filer. Admin-rättigheterna kan vara enhetsspecifika eller omfatta större områden i intranätet (domän).

årens lopp ökade antalet användare och diskutrymmet utökades, så det han samlas ett stort antal föråldrade filer.

Alla arbetsstationer och verksamhetsställen vid fostrans- och utbildningssektorns förvaltning hade tillgång till den nätverksdisk som blev föremål för dataintrånget. Därmed fanns det flera tusen användare.

Användarrättigheterna till nätverksdisken hade fördelats på rätt sätt organisations- och funktionsspecifikt, men vid dataintrånget förlorade de sin betydelse, eftersom säkerhetskopieringskoden som angriparen fått tag på hade läsrätt till alla filer.

Det förekom skillnader i hur nätverksdisken användes mellan verksamhetsställena. På en del ställen användes den knappt alls, eftersom man använde molntjänster. I vissa enheter använde hela personalen nätverksdiskar och i vissa endast den administrativa personalen. Olika behov och etablerad praxis hade skapat skillnader mellan verksamhetsställena.

Nätverksdisken visades för de flesta användare som datorns diskenhet V:. En del av mapparna visades som disk R:. Utöver de gemensamma diskarna hade användarna en personlig nätverksdisk (H:) som fanns i en annan servermiljö. Denna lyckades angriparen inte bryta sig in i.

På nätverksdisken förbereds, distribueras och lagras information. Helsingfors stad har flera informationssystem som inte är helt kompatibla. Därför måste uppgifterna sparas i ett ”mellanlager” på nätverksdisken, så att även andra användare kan redigera dem. På motsvarande sätt bereds många handlingar i anslutning till besluten först på nätverksdisken och först i sinom tid registreras de slutliga uppgifterna i informationssystemen.

Under årtiondenas lopp hade mycket information lagrats på nätverksdisken (se figur 4). En del av filerna gällde skolornas verksamhet, såsom anvisningar, meddelanden och promemorior. En del innehöll konfidentiella personuppgifter, såsom information om sjukdomar, allergier eller medicineringar.

Innehållet på nätverksdisken hade under årens lopp knappt alls utvärderats eller städats upp och det fanns inga tydliga anvisningar för att använda innehållet. Anvisningar om förvaring av uppgifter på nätverksdisken hade getts på allmän nivå, men iakttagandet av anvisningarna övervakades inte. Beredningshandlingar som var avsedda att vara tillfälliga blev kvar på disken även efter att de inte längre användes.

Nätverksdisken var ett centralt verktyg för de enheter som använde den. Efter dataintrånget var nätverksdisken ur bruk i cirka en månad, vilket orsakade mycket extra arbete i organisationerna. Driftavbrottet inträffade under den värsta möjliga tiden, eftersom man i maj upprättar betygen och förbereder elevantagningen för följande läsår.

Nätverksdisken hade skapats som en virtualiserad server som fanns i fostrans- och utbildningssektorns egen datorsal. Fostrans- och utbildningssektorns egen IT-personal ansvarade för underhållet av den. Planen var att flytta disken till DigiHelsinki så att utrymmet skulle ha köpts som en kapacitetstjänst av underleverantören från dennes datorsal. Överföringen hann dock inte genomföras innan dataintrånget inträffade.

Antal filer på nätverksdisken och användning av dem

Efter dataintrånget listade fostrans- och utbildningssektorn de filer som fanns i säkerhetskopian av nätverksdisken. I kommentarerna till medierna berättade staden att det fanns ”tiotals miljoner dokument” på nätverksdisken.[24]

Utredningsgruppen analyserade nätverksdiskens filförteckning och observerade att den innehåller sammanlagt 4 983 854 rader. Det fanns 521 774 mappar och 4 462 080 filer. Skillnaden till det antal som angavs i det inledande skedet förklaras av en viruskontroll av disken som gjordes i samband med säkerhetskopieringen.

Helsingfors stad berättade i offentligheten det totala antalet skannade filer som viruskontrollprogrammet meddelat. Viruskontrollen öppnar alla komprimerade filer som hittas, såsom ZIP-filer[25] samt CAB- och MSI-filer[26] som används vid installation av program. Programmens distributionspaket innehåller inte användarens egna filer, så de är inte väsentliga med tanke på dataintrånget. Viruskontrollen räknar även dessa filer med i det totala antalet.

Operativsystemet sparar minst två tidsstämplar för filerna: tidpunkten då filen skapades och den sista tidpunkten då filen sparades efter att den redigerats. I vissa fall sparas också den sista användningstidpunkten som kan gälla öppnande av filen för läsning eller till exempel start av en programfil. En vanlig filförteckning för Windows visar endast den sista lagringstidpunkten.

Eftersom filerna under årens lopp hade samlats på disken från olika källor är tidsstämplarna inte alltid helt tillförlitliga. Av stämplarna kan man dock dra slutsatsen att flest nya filer skapades på disken 2020 och 2021, varefter det årliga antalet nya filer minskade till cirka hälften.

På basis av ändringsdatumen redigerades filerna mest 2019, varefter också antalet redigerade filer minskade jämnt varje år.

Av de dokument som sparats på nätverksdisken är Word-, Excel-, PowerPoint- och PDF-filer som skapats med Microsoft Office centrala.

I utredningen granskades förteckningens filnamn. Utifrån dem innehöll Office-dokumenten bland annat protokoll, undersökningar av inomhusluften, planeringsprotokoll i anslutning till renoveringar, handelskvitton, grund- och byggnadsritningar, handböcker, anvisningar, brottsanmälningar, planer, verksamhetsberättelser och verksamhetsplaner samt föredragningslistor.

[24] Yle-nyhet 25.5.2024: Helsingin kaupungin selvitys paljastaa yhä vakavampia piirteitä tietomurrosta. 26.2.2025 https://yle.fi/a/74-20090447

[25] ZIP är en utbredd komprimeringsteknik utan förluster som används för att samla ihop och komprimera filer så att de tar mindre plats på disken.

[26] CAB (Cabinet) och MSI (Microsoft Installer) är installationspaket för Windows-applikationer som innehåller alla filer som programmet behöver och programmakarens digitala signatur som verifierar ursprunget.

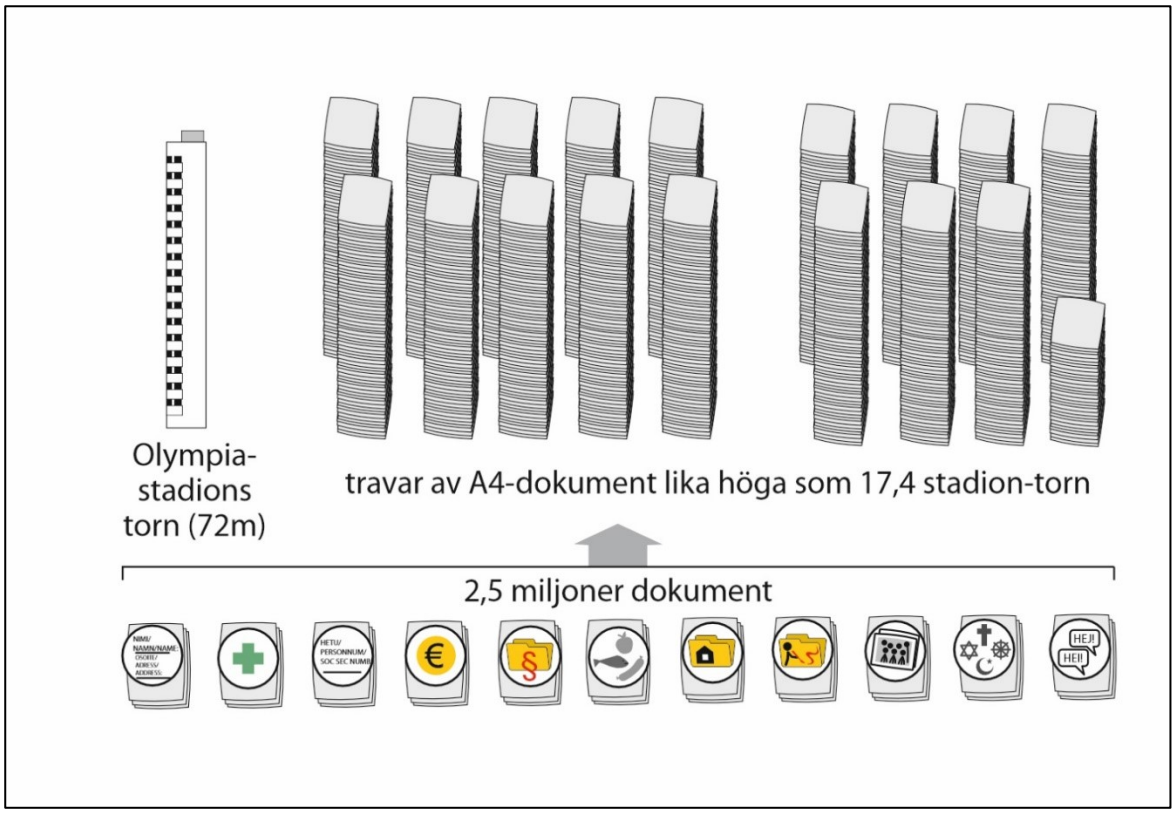
Tabell 1: Dokumenttyper och deras antal

Typ av dokument	Antal
Word (DOC, DOCX)	1 094 684
Excel (XLS, XLSX)	513 060
PowerPoint (PPT, PPTX)	109 378
PDF-filer (PDF)	766 455
Totalt	**2 483 577**

PDF-filer kan förutom originaldokument även innehålla pappersdokument som skannats in. Att döma av namnen innehöll filerna bland annat körkort, hygienpass, fakturor, beställningar, läkarintyg, ansökningar om biträde, meddelanden, personliga arvodeskalkyler, beslut om tjänstledighet, elevbedömningar, skattekort, tjänsteförordnanden, avgångsanmälningar, olycksfallsanmälningar till försäkringsbolaget samt lönespecifikationer.

På grund av dokumentens karaktär innehåller nästan alla antagligen personuppgifter som kan hänföras till personer och som identifierar personer. Särskilt konfidentiella dokument var beslut om särskilt stöd, utredningsmaterial om daghemsavgifter, läkarintyg, passkopior samt föräldrarnas person- och inkomstuppgifter.

Mängden information kan åskådliggöras med antagandet att varje dokument innehåller fem utskrivbara sidor. Då skulle dokumenten innehålla sammanlagt 12,5 miljoner utskrivbara sidor och eftersom ett A4-ark är cirka 0,1 millimer tjockt skulle de som ensidiga A4-pappersutskrifter bilda en 1,25 km hög stapel.



Figur 8. Illustration av antalet dokument som sparats på nätverksdisken.

Av mappnamnen att döma fanns det också rikligt med filer som överförts från andra diskar samt säkerhetskopior från USB-minnen. Utöver de egentliga dokumenten fanns det på disken över 1,1 miljoner JPEG-fotografier från bland annat daghems- och skolutflykter samt olika evenemang. Andra filtyper som identifierades på nätverksdisken var videofiler, e-postmeddelanden (MSG), webbplatser (HTM), animerade bilder (GIF), vanliga textfiler (TXT) samt installationspaket för programvara.

På grund av bristfälliga loggar kan man endast få en summarisk bild av **antalet läckta filer**. Filerna överfördes till angriparens server via en krypterad förbindelse med FTP-programmet[27] FileZilla. Den totala trafikmängden kunde utredas i brandväggsloggarna, men på grund av krypteringen kunde filnamn eller andra detaljer inte utredas.

Angriparen installerade FileZilla på flera servrar, men tog bort programmen efter användningen, så programmets egna loggar hjälpte inte i utredningsarbetet. I en servers RAM-minne fann man spår av överförda filnamn och mappar på nätverksdisken, men listan var ofullständig. Det är således omöjligt att fastställa vilka enskilda filer eller mappar angriparen fick tag på.

På basis av den totala mängden data som angriparen överförde (två terabyte) i förhållande till det totala antalet filer på nätverksdisken (6,73 terabyte) kan man uppskatta att 30 procent av filerna hann kopieras, dvs. cirka 1,3 miljoner filer hamnade hos angriparen, varav cirka 750 000 var dokument (Office och PDF-filer).

2.3 Dataintrånget i användardatabasen

Utöver filerna på nätverksdisken fick angriparen också tillgång till hela stadsförvaltningens AD-användaruppgifter samt AD-databaserna för den grundläggande utbildningen och yrkesutbildningen. AD (Active Directory) är en centraliserad användarkatalog i Microsoft-nätverk som innehåller användarnamn, e-postadresser och tillhörande personuppgifter samt i fostrans- och utbildningssektorns fall även elevnummer.

2.4 Förmåga att observera webbmiljön

Arbetsstationer i fostrans- och utbildningssektorns intranät användes ett skyddsprogram mot skadliga program. Dessutom hade ett datasäkerhetsprogram installerats på servrarna för att trygga serverns säkerhet. Fostrans- och utbildningssektorn hade dock ingen heltäckande uppföljning som kunde analysera nättrafiken och observera avvikelser (anomalier).

Fostrans- och utbildningssektorns och DigiHelsinkis underleverantör som övervakar brandväggstjänsterna samlar in information om trafiken mellan stadens intranät och internet. Med hjälp av dessa loggar har man kunnat i efterhand utreda händelser i anslutning till förberedelserna för dataintrånget och själva attacken i februari–maj 2024. Larmövervakning i realtid hörde inte till brandväggstjänsten.

Living off the land-tekniken som angriparen använde sig av gjorde det svårare att upptäcka verksamheten, eftersom aktiva angrepp närmast kan identifieras endast på basis av avvikande beteende i nätverket och programmen.

Ur angriparens synvinkel är avsaknaden av ett permanent fotfäste en svaghet i metoden. Om brottslig verksamhet upptäcks räcker det med att bryta förbindelsen, byta lösenord och korrigera sårbarheter för att avvisa angriparen.

---

[27] FTP (File Transfer Protocol) är en gammal metod som utvecklats för filöverföring. Det ursprungliga FTP överför filerna utan kryptering, men den nyare SFTP-metoden (Secure FTP) som FileZilla använder innehåller också kryptering.

Helsingfors stad strävade efter att förbättra övervakningen av nätmiljön och inledde upphandlingen av ett servicesystem för cybersäkerhet (Cyber Security Operations Center, CSOC) med en EU-upphandlingsannons som publicerades den 28 juni 2021. Enligt upphandlingsannonsen upphandlas CSOC för att upprätthålla cybersäkerheten för IKT-system och tjänster som Helsingfors stad äger och förvaltar samt som skaffas eller hyrs av tredje parter.

En leverantör svarade på anbudsförfrågan. Kanslichefen fattade upphandlingsbeslutet i ärendet den 28 oktober 2021 så att urvalsgrunden var totalekonomisk fördelaktighet, dvs. priset. Minimikraven för de tjänster som upphandlades var kvalitativa krav (kvalitetskriterier) som de tjänster som erbjöds skulle uppfylla. Upphandlingens uppskattade värde var 5,2 miljoner euro beräknat på fyra år. Upphandlingsavtalet undertecknades den 4 april 2022.

Efter upphandlingsbeslutet inledde leverantören och staden ett ibruktagningsprojekt. I enlighet med serviceavtalet testades tjänsten i slutet av ibruktagningsprojektet. Staden skaffade en utomstående aktör för testningen som utförde arbetet 11.5–31.5.2023. Helheten klarade inte godkännandetestningen. DigiHelsinki lämnade en uppsägningsanmälan till leverantören den 16 juni 2023 och ibruktagningsprojektet avbröts.

2.5 Förhållanden

Cybersäkerhetscentret[28] och Skyddspolisen[29] ordnade i april 2023 ett gemensamt informationsmöte där man berättade att Finlands cyberhotnivå har hållits på en förhöjd nivå och att cyberhotnivån för första gången höjdes i samarbete mellan myndigheterna hösten 2022.

Enligt de anmälningar som Cybersäkerhetscentret hade fått hade antalet cyberangrepp mot finländska organisationer ökat, speciellt i fråga om antalen skadliga program, nätfiske och överbelastningsangrepp. Enligt Cybersäkerhetscentrets analys verkade attackerna mot finländska organisationer vara mer skräddarsydda och riktade än tidigare. När det gäller företag inom cyberspionage och cyberpåverkan bekräftar Skyddspolisen Cybersäkerhetscentrets bedömning.

En central faktor som höjer hotnivån är den allt vanligare nätbrottsligheten mot både organisationer och medborgare. Även statliga aktörer har aktiverat sig i den digitala verksamhetsmiljön. En väsentlig förändring i datasäkerhetshoten mot organisationer har på 2020-talet varit att attacker som gjorts med utpressningsprogram har blivit vanligare. Detta fenomen har behandlats av Cybersäkerhetscentrets aktualitetsöversikt ”Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa” som anknyter till temat Informationssäkerhet nu! i september 2024.[30]

Cybersäkerhetscentret informerade den 7 mars 2024, dvs. mindre än två månader före dataintrånget om händelserna i sin Informationssäkerhet Nu!-artikel ”Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena”[31] om riskerna i anslutning till nätets kantenheter och hur de öppnar dörren till organisationens datatekniska miljö.

---

[28] Cybersäkerhetens hotnivå har stigit – även aktivitet mot Finland har ökat. 25.2.2025 https://www.traficom.fi/sv/aktuellt/cybersakerhetens-hotniva-har-stigit-aven-aktivitet-mot-finland-har-okat

[29] Cybersäkerhetens hotnivå har stigit – även aktivitet mot Finland har ökat. 25.2.2025 https://www.traficom.fi/sv/aktuellt/cybersakerhetens-hotniva-har-stigit-aven-aktivitet-mot-finland-har-okat

[30] Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa. 26.2.2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa

[31] Informationssäkerhet Nu! -artikel ”Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena” https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena

Cybersäkerhetscentrets månatliga rapport Cyberväder[32] berättar om betydande datasäkerhetsavvikelser och -fenomen i Finland. Cyberväderrapporten för maj 2024 publicerades den 13 juni 2024. I meddelandets ingress konstateras att cybervädret fortsatt oroande även i maj. Situationen förvärrades särskilt av dataintrång och -läckage som kom till kännedom. I sammandragstabellen för cybervädret lyfts Helsingfors stads fall fram genom att konstatera att Helsingfors stads sektor för fostran och utbildning utsattes för ett omfattande dataintrång. I fråga om dataintrången beskrevs situationen i maj som allvarlig, vilket är den mest kritiska bedömningen på skalan.

I största delen av dataintrången är gärningsmännens mål ekonomisk nytta. I vissa fall kan orsaken vara att testa eller presentera sina egna förmågor, stjäla kommersiellt värdefull information från en konkurrent eller påverka samhället.

2.6 Logguppgifter

Logghanteringen för fostrans- och utbildningssektorns nätverksenheter, servrar och terminaler baserade sig i huvudsak på enheternas interna loggning och hade ingen enhetlig praxis eller centraliserad hantering. Därför var man delvis tvungen att göra dataintrångsutredningar med bristfälliga uppgifter. Uppgifter från DigiHelsinkis underleverantörs brandvägg, som främst gäller trafiken mellan internet och fostrans- och utbildningssektorns intranät, var en central informationskälla. Det fanns endast knapphändig information om händelser i intranätets servrar och terminaler.

Fostrans- och utbildningssektorns tjänsteleverantörer hade vissa övervakningstjänster på server- och nätnivå som gav larm om angriparens åtgärder i fostrans- och utbildningssektorns servermiljö. Dessa åtgärder märktes under granskningsarbetet av dataintrånget. Larmen övervakades inte på ett sätt, som skulle ha lett till bekämpningsåtgärder under dataintrången.

2.7 Helsingfors stad

Helsingfors stad är Finlands största arbetsgivare och i slutet av 2023 hade staden cirka 37 000 anställda. Organisationen är indelad i fyra huvudsektorer: Fostrans- och utbildningssektorn (KASKO), Stadsmiljösektorn (KYMP), Kultur- och fritidssektorn (KUVA), Social-, hälsovårds- och räddningssektorn (SOTEPE). Dessutom har Helsingfors stad en centralförvaltning (stadskansliet). Av dessa är fostrans- och utbildningssektorn som utsattes för dataintrånget störst och har cirka 15 000 anställda. Helsingfors är organiserat på ett sätt som avviker från de finländska städerna, eftersom sektorerna är mycket självständiga och kansliet har en beställarlik eller övervakande roll i förhållande till sektorerna.

Fostrans- och utbildningssektorn ansvarar för stadens småbarnspedagogik, förskoleundervisning, grundläggande utbildning, gymnasieutbildning och finskspråkiga yrkesutbildning samt den fria bildningen. Verksamheten är mycket omfattande; till exempel finns det cirka hundra grundskolor där det går cirka 45 000 barn och unga. Det finns cirka 320 daghem och de erbjuder småbarnspedagogik för cirka 27 000 barn.

Fostrans- och utbildningssektorn har en egen förvaltnings- och stödtjänstorganisation som omfattar informationsförvaltning på cirka 80 personer. Av dessa arbetar cirka 20 personer med IKT-infrastruktur och dess informationsförvaltning. Som helhet har informationsförvaltningen fungerat mycket självständigt och separat från informationsförvaltningen vid stadens andra sektorer.

[32] Cyberväder 26.2.2025 https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/cybervader

Helsingfors stad fastställde riktlinjerna för datasäkerheten den 1 juni 2020. I riktlinjerna för datasäkerheten presenterades principiella lösningar som är bindande för stadsorganisationen för att främja och säkerställa datasäkerheten. I dokumentet presenteras 14 olika riktlinjer och de innehåller bland annat grunderna för ansvarsfördelningen.

Den övergripande styrningen och samordningen av stadens informationshantering genomförs i informationshanteringsgruppen, som stadsstyrelsen tillsatte den 21 mars 2022. Informationshanteringsgruppens uppgift är att på stadsnivå samordna de åtgärder, anvisningar samt kommunikation och utbildning som skyldigheterna i anslutning till informationshanteringen förutsätter. Informationshanteringsgruppen utvecklar, följer upp, övervakar och rapporterar om fullgörandet av skyldigheterna i anslutning till informationshanteringen i Helsingfors stads organisation. Informationshanteringsarbetsgruppens arbete har varit regelbundet, haft goda resurser och man har aktivt deltagit i dess verksamhet. Informationshanteringsarbetsgruppens verksamhet har kunnat främja fullgörandet av stadens informationshanteringsskyldigheter och utvecklingen av datasäkerheten. Samma vår grundades en egen koordineringsgrupp för informationshantering vid fostrans- och utbildningssektorn. Gruppens uppgift är att på sektornivå samordna de åtgärder, anvisningar samt kommunikation och utbildning som skyldigheterna i anslutning till informationshanteringen förutsätter. Gruppens uppgift är dessutom att följa upp, övervaka och rapportera om fullgörandet av skyldigheterna i anslutning till informationshantering inom sektorn.

I stadens informationshanteringsgrupp utarbetas årligen en tillsynsplan för informationshanteringen och de lägesrapporter som sektorerna, affärsverken och ämbetsverken ger behandlas. Med tillsynsplanen sörjer staden för dess lagstadgade styrnings- och tillsynsskyldighet i fråga om behandlingen av uppgifter.

Målet med egenkontrollen är att utveckla informationshanteringen på stadsnivå, beakta förändringar i verksamhetssätten och informationssystemen samt rapportera till kanslichefen. Rapporterna ger en heltäckande bild av informationshanteringsgruppens verksamhet och observationer. I rapporterna har man också identifierat risker i anslutning till informationshanteringsmiljön, såsom det stora antalet informationssystem och deras splittring samt bristfälliga informationshanteringsmiljöer.

I den revisionsrapport från Helsingfors stads interna revision som färdigställdes i februari 2023 har man identifierat att ansvarsfördelningen inom datasäkerheten mellan stadskansliet och sektorerna (inkl. fostrans- och utbildningssektorn) varit oklar. För detta gavs en rekommendation enligt vilken fostrans- och utbildningssektorn skulle uppdatera sin egen ansvarsfördelningstabell före utgången av september 2023. Som en del av revisionen genomfördes en enkät och i den var fostrans- och utbildningssektorn mest nöjda av de fyra granskade sektorerna med nivån på sin egen datasäkerhet.

I rapporten identifierades också att Helsingfors stad inte har effektiva sätt att upptäcka nätattacker. Orsaken var delvis fördröjningar i upphandlingen och ibruktagandet av tjänsten som hänför sig till detta. I ärendet gavs en rekommendation om att upphandla en centraliserad övervakningstjänst före utgången av maj 2023. På grund av att konkurrensutsättningen misslyckades kunde tjänsten inte skaffas före maj 2024 och därmed var den inte i bruk när dataintrånget skedde.

Tjänsteinnehavarnas ansvar

Helsingfors stadsstyrelse har genom sitt beslut av den 28 februari 2022 bekräftat Helsingfors stads anvisningar, praxis, ansvar och tillsynsmekanismer för informationshantering och dokumentförvaltning. Enligt beslutet ansvarar de ledande tjänsteinnehavarna inom sektorerna,

ämbetsverken och affärsverken för genomförandet av åtgärderna i anslutning till informationshanteringen. De ledande tjänsteinnehavarna utser de instanser som ansvarar för genomförandet i sin egen organisation.

Ansvaren på stadsnivå fastställs i stadsstyrelsens beslutsprotokoll. Digitaliseringsdirektören ansvarar för styrningen på stadsnivå av informationsförvaltningsmodellen och informationsförvaltningen. I synnerhet digitaliseringsdirektören ansvarar för organiseringen på stadsnivå av planeringen, anvisningarna och uppföljningen av genomförandet av informationssystem, informationslager samt integrationer och gränssnitt och förändringseffekter enligt 5 § i informationshanteringslagen[33].

Informationshanteringschefen sörjer för ledningen av stadens dokumentförvaltning, ger anvisningar om dokumentförvaltningens ansvar, uppgifter och praxis, styr och utvecklar stadens dokumentförvaltning som en del av informationshanteringen, godkänner stadens gemensamma plan för informationsstyrning, övervakar iakttagandet av anvisningarna samt sörjer för utbildning och rådgivning i anslutning till dokumentförvaltningen (innehåller ansvar för styrning av informationssäkerheten gällande det analoga materialets arkivduglighet, arkivutrymmen och skydd av handlingar under undantagsförhållanden).[34]

Vid fostrans- och utbildningssektorn hade utvecklingsuppgifter inom ämnesområdet organiserats på ett sätt som motsvarade stadsorganisationens gemensamma utvecklingsarbetsgrupper. För utvecklingsarbetet hade fyra separata arbetsgrupper bildats och experter från sektorn hade utsetts till dem. På detta sätt strävade man efter att säkerställa att de ändrade skyldigheterna i informationshanteringslagen och dataskyddsförordningen kan fullgöras. I samband med arbetsgruppernas arbete observerades dock att det finns för många arbetsgrupper och att deras verksamhet är dåligt samordnad sinsemellan. Av dessa orsaker förnyades arbetsgruppsarrangemangen i ett senare skede.

Sektordirektören för fostrans- och utbildningssektorn fattade den 28 maj 2020 ett beslut om de underlydande tjänsteinnehavarnas informationshanteringsansvar. Genom beslutet delades uppgifter som hänför sig till dataskydd, datasäkerhet, informationshantering och datatekniska lösningar till tjänsteinnehavarna inom sektorn. Uppgifterna beskrevs genom att beskriva deras innehåll med korta meningar eller ämnesord. Centrala tjänsteinnehavare var förvaltningsdirektören, datasystemchefen och IT-direktören samt informationssäkerhetschefen i arbetsavtalsförhållande som enhetschef.

Helsingfors stad har omfattande **anvisningar för informationshantering, dataskydd och informationssäkerhet**. En del av anvisningarna är gemensamma för staden och en del interna inom sektorerna. Informationshanteringsenheten vid stadskansliet har upprätthållit 33 separata anvisningar om informationshantering och informationshanteringsmetoder.

Styrgruppen för informationshantering beredde den 27 september 2022 en guide om tjänsteansvar inom informationshantering. Guiden riktades som en allmän presentation till stadens chefer. I dokumentet presenterades strukturerna för genomförande av informationshanteringen. I guiden konstateras bland annat att staden ska föra ett ärenderegister över de ärenden som den behandlar. Hit hör ärenden där man fattar något slags beslut. De som bereder ärendena ska se till att ärendenas behandlingsskeden jämte handlingar registreras utan dröjsmål så att registret hålls uppdaterat. Enligt guiden hör inte alla handlingar till ärenderegistret, utan de omfattas av bestämmelserna om informationshantering i 27 § i informationshanteringslagen. Handlingar i anslutning till

[33] 906/2019.
[34] Helsingfors stadsstyrelses delegeringsbeslut (24.4.2017 § 441).

arbetsuppgifterna ska registreras och hanteras så att de hittas utan besvär även om inget administrativt beslut har fattats om dem.

I anvisningen konstateras också att informationshanteringsmodellen ska innehålla en anteckning av vilken framgår förvaringsform, -sätt och -tid för informationsmaterialet i datalagren samt information om hur materialet förstörs, om detta har fastställts i lagen eller informationsstyrningsplanen. Uppgifter som ska förvaras varaktigt ska förvaras på behörigt sätt och uppgifter som ska förstöras ska förstöras efter att förvaringstiden gått ut. De system där handlingar produceras i ärenderegistret ska beskrivas i beskrivningen av handlingars offentlighet.

I stadskansliets anvisning ”Väliaikainen ohje tietoaineistojen sähköisestä säilyttämisestä” av den 14 mars 2022 fastställs att beredningen och förvaringen av handlingar ska genomföras i ett centraliserat hanteringssystem (Ahjo). Anvisningen tillåter dock bl.a. följande undantag:

> *Staden har ännu inte digitala verktyg för att sköta alla uppgifter, så arbetet utförs också analogt, dvs. pappersdokument används. Upphandlingen av ärendehanterings- och dokumenthanteringslösningar bereds. I avsaknad av lösningar för förvaring av stadens gemensamma handlingar måste den elektroniska förvaringen avgöras tillfälligt, eftersom skyldigheten trädde i kraft den 1 januari 2022. Handlingar som inte förvaras i ett lämpligt elektroniskt informationssystem lagras på en nätverksenhet i en gemensam mapp.*

Informationshanteringsmodellen, som styr Helsingfors stads verksamhet, består av flera olika helheter. I den ingår beskrivningar av informationslager och informationssystem (arkitekturbeskrivningar), applikationsförteckningar, processbeskrivningar, planer för informationsstyrning och riskbedömningsmaterial. Dessutom kan informationshanteringsmodellen anses omfatta beslut om ansvarspersoner och principbeslut.

I arkitekturbeskrivningen för fostrans- och utbildningssektorns informationssystem presenteras de informationssystem, informationslager och allmänna principer för informationshantering som används inom sektorn. I beskrivningarna saknas den nätverksdisk som var föremål för dataintrånget.

Planen för informationsstyrning upprätthålls av Helsingfors stad som en del av dess informationsstyrningssystem.[35] Avsikten är att systemet ska innehålla alla Helsingfors stads informationsstyrningsuppgifter oberoende av informationens form (elektroniskt material och pappersmaterial).

Planen för informationsstyrning färdigställdes 2019 för alla uppgiftsklasser. Planen för informationsstyrning är till sin natur en aktuell version som uppdateras kontinuerligt och sp, finns tillgänglig i datanätet.

Bland de anställda har fostrans- och utbildningssektorns informationshanteringsprocesser upplevts som komplicerade. Till exempel kan det hända att en elektroniskt undertecknad blankett behöver skrivas ut, undertecknas för hand och sedan skannas in i systemet. I vissa skolor är det endast rektorn och skolsekreteraren som använder en nätverksdisk. Lärarna använder dessutom andra lösningar, till exempel molntjänstlösningar och lagringsutrymmen på den egna datorn. Det finns skillnader mellan skolor och personer i fråga om vilka förfaranden de använder för att spara information.

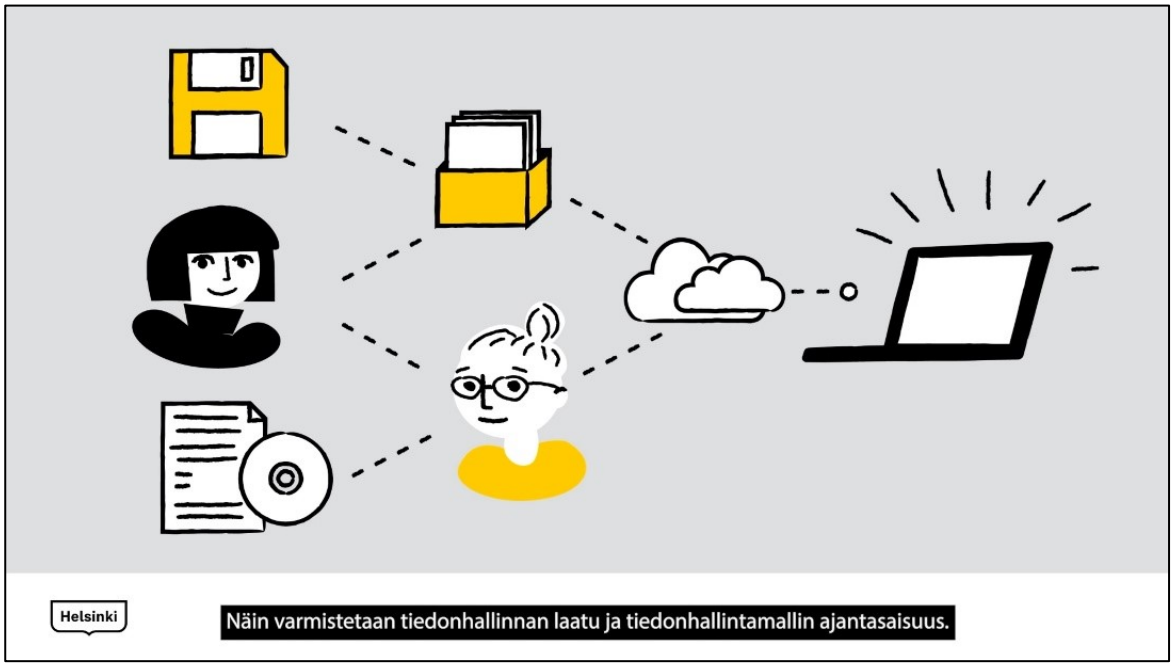
[35] Helsingfors stad: System för informationsstyrning. 26.2.2025. https://tiedonohjaus.hel.fi

DigiABC-utbildning för anställda

Helsingfors stad har gjort en DigiABC-videoutbildning om dataskydd och -säkerhet. Den cirka en timme långa utbildningen kan genomföras som självstudier på den egna datorn och den omfattar en flervalstentamen till slut. Stadskansliet har producerat undervisningsvideor om datasäkerhet som också är öppet tillgängliga på internet.

Utgångspunkten är att en ny arbetstagare ska genomgå DigiABC inom två veckor, men prestationsmängderna varierar sektorsvis. Innehållet i utbildningsvideorna uppdateras regelbundet, så de som varit i huset en längre tid måste förnya provet. Cheferna följer upp antalet slutförda utbildningar. Dessutom har staden erbjudit grundkurser i informations- och dokumenthantering.

På våren 2024 behandlade DigiABC-utbildningen förutom allmänna informationssäkerhetsfrågor även klassificering av uppgifter och skyddsmärkningar. På allmän nivå gavs anvisningar om dataskydd när det gäller betydelsen av personuppgifter och säker behandling. Informationens livscykel och radering av föråldrade uppgifter nämndes inte separat.



Figur 9. Skärmbild av Helsingfors stads DigiABC-självstudieutbildning.

DigiHelsinki Oy är ett aktiebolag som hör till Helsingfors stadskoncern och som är infört i handelsregistret den 2 augusti 2022. År 2023 var dess omsättning cirka 58 miljoner euro och den sysselsatte 134 personer. Helsingfors stad äger 100 procent av bolagets aktier och utövar på det sätt som upphandlingslagen förutsätter ett avgörande inflytande över bolagets strategiska mål och viktiga beslut med hjälp av rätten att utse styrelsemedlemmar, ägarstyrningen och koncernövervakningen.

Bolagets uppgift är att producera digitala bastjänster för Helsingfors stad. Sådana tjänster är bland annat första gradens stöd, stödtjänst för förtroendemannaorganisationernas möten, närstödtjänst, livscykeltjänster för terminaler, standardprogramtjänster, utskriftstjänster, lokalnät, datakommunikationsanslutningar, brandvägg, stomnät, kapacitetstjänster för servrar

och lagringssystem, databastjänster, säkerhetskopiering och återställning, AD-katalog, arbetsgruppstjänster, IT-experttjänster, cybersäkerhetstjänst, stödtjänster för kundarbetsstationer samt informationstavlor.[36]

Bakgrunden till grundandet av bolaget är projektet Digitaalinen perusta som inleddes 2019 och vars syfte var att inleda åtgärder för att uppdatera och modernisera stadens digitala verksamhetsmiljö. Projektet Digitaalinen perusta ingick i Helsingfors stads mer omfattande digitaliseringsprogram 2019–2022 och var ett centralt utvecklingsobjekt för programmet. Projektet organiserades som en del av verksamheten vid stadskansliets strategiska avdelning och en del av stadens IT-personal överfördes till den verksamhetsenhet som inrättades vid stadskansliet. I denna form fortsatte verksamheten fram till början av 2023, då funktionerna överfördes till DigiHelsinki Oy som grundats för att producera dem. I och med bolagiseringen övergick fler av stadens IT-personer i DigiHelsinkis tjänst.

I enlighet med bolagiseringsbeslutet fungerar DigiHelsinki Oy som stadens och dess dottersammanslutningars inköpscentral, vilket har antecknats som bolagets verksamhetsområde i dess bolagsordning. Som inköpscentral kan bolaget konkurrensutsätta bland annat ramavtal och dynamiska inköpssystem för stadens och dess dottersammanslutningars bruk, genom vilka staden och dottersammanslutningarna kan upphandla varor eller tjänster. Dustin Finland Oy valdes genom konkurrensutsättning till leverantör av installationstjänster för datakommunikationsutrustning.

DigiHelsinki Oy producerar digitala bastjänster i enlighet med ramavtalet på stadsnivå samt anslutningsavtalen för varje användarorganisation (t.ex. sektor, ämbetsverk och affärsverk) och det årliga upphandlingsbeslutet för varje användarorganisation. Det har bestämts att avvikelser från tjänsterna på stadsnivå ska avtalas i de användarorganisationsspecifika anslutningsavtalen. Alla stadens sektorer har ingått upphandlingsavtal med bolaget, vilka varit i kraft från och med den 1 januari 2023. Det finns skillnader mellan de avtalsenliga leveranserna och tjänsternas omfattning enligt sektor. Överföringen av IKT-servicehelheterna till det nya bolaget på en gång upplevdes som utmanande, så överföringen av tjänster graderades bland annat så att fostrans- och utbildningssektorn fortfarande hade egen produktion av IKT-bastjänster och IKT-personal.

Efter att bolagets verksamhet inleddes och de sektorsspecifika upphandlingsavtalen ingicks har situationen fortsatt, där produktionen av tjänster ställvis har fördelats mellan DigiHelsinki och stadsorganisationens egen verksamhet. Organiseringsändringarna har i praktiken blivit en övergångsperiod på cirka fyra år, under vilken det har skett många förändringar i arbetsfördelningen och ansvaren samt i personalens uppgifter. I övergångsskedet har fördelningen av uppgifter och ansvar fördunklats åtminstone i fråga om vissa detaljer. En sådan detalj med oklart ansvar var VPN-routern som utnyttjades i dataintrånget (se 2.1).

Händelsen var förknippad med privata företag från vilka Helsingfors stad skaffade informationsförvaltnings- och informationssäkerhetstjänster redan före dataintrånget. När intrånget upptäcktes skaffades tjänster för att reda ut händelsen och återhämta sig från den. De privata aktörer som var förknippade med händelsen är etablerade och kända företag inom IKT-branschen.

Telia Cygate ansvarar för underhållet av Helsingfors stads brandväggstjänst och hanteringen av loggar. Telia Cygate Oy:s omsättning 2023 var cirka 137 miljoner euro och dess personalantal cirka 400.

[36] Stadsfullmäktige § 142 1.6.2022

Fujitsu Finland Oy ansvarar bland annat för att tillhandahålla Helsingfors stad nät- och molntjänstkapacitet. Dessutom erbjuder den tjänster för förmedling och integrering av ärenden som produceras av stadens olika underleverantörer som tillhandahåller ICT-tjänster mellan de olika leverantörernas informationssystem. Fujitsu Finland Oy:s omsättning 2024 var cirka 300 miljoner euro och dess personalantal cirka 1 400.

Dustin Finland Oy utförde på uppdrag av fostrans- och utbildningssektorn underhållsuppgifter för nätverksenheter. Företaget har årligen uppdaterat certifikatet för Cisco ASA 5515 VPN-enheten som utsattes för dataintrånget med hjälp av fjärrhantering. Dustin Finland Oy:s omsättning 2024 var cirka 165 miljoner euro och dess personalantal cirka 220.

Elisa Santa Monica Oy gjorde från och med den 3 maj 2024 en teknisk utredning av dataintrånget på beställning av Helsingfors stad. Företagets team för utredning av dataintrång ger stöd för att utreda dataintrång och återställa situationen. Företaget utför årligen flera tiotals motsvarande konsultationer. Företaget erbjuder också andra informationssäkerhetstjänster, såsom nätverksövervakningstjänster (SOC, Security Operations Center). Elisa Santa Monica Oy:s omsättning 2023 var cirka 64 miljoner euro och dess personalantal cirka 180.

Palo Alto Networks Oy levererade brandväggar till Helsingfors stad. Telia Cygate ansvarade för brandväggarnas administrationstjänster. Efter dataintrånget analyserade Palo Alto Networks Oy brandväggarnas logguppgifter. Palo Alto Networks (Finland) Oy:s omsättning 2024 var cirka 9 miljoner euro och dess personalantal cirka 30.

Cisco Systems har efter dataintrånget producerat experttjänster för Helsingfors stad särskilt för analys av utspridda logguppgifter och minnesdumpar som samlats in från Cisco ASA 5515 VPN-enheten. Cisco Systems Finland Oy:s omsättning 2024 var cirka 15 miljoner euro och dess personalantal cirka 55.

	HELSINGFORS STADSKONCERN			FÖRETAG SOM PRODUCERAR TJÄNSTER FÖR STADEN	
Aktörens namn	**Helsingfors stad**	**Helsingfors stads verksamhetsområde KASKO**	**Serviceproducent DigiHelsingfors**	**Flera företag**	**Företag**
Allmän beskrivning	Aktör med organiseringsansvar	Produktionsuppgift enligt verksamhetsområde	Produktion av stadens interna digitala bastjänster.	Företag som producerar olika IKT-tjänster	Experttjänst inom informationssäkerhet
Före dataintrånget	• Utveckling av informationshanteringsmiljön på stadsnivå. • Administrativ informationssäkerhet. • Utveckling av stadens övergripande arkitektur. • Digital grundledning av programmet. • Koncernstyrning av DigiHelsingfors.	• Ansvar för genomförandet och utvecklingen av verksamhetsområdets informationshantering. • Informationshanteringens tekniska ansvar som inte har överförts till DigiHelsingfors. • Delvis administrativa och delvis tekniska informationssäkerhetsuppgifter. • Oklarheter i ansvarsfördelningen med DigiHelsingfors särskilt i fråga om tekniskt underhåll.	• Hantering och underhåll av informationssäkerheten enligt stadens och DigiHelsingfors avtal • Övervakning av datakommunikationen i eget nät. • Teknisk informationssäkerhet enligt stadens och DigiHelsingfors avtal • Oklarheter i ansvarsfördelningen med KASKO.	• Levererar och upprätthåller ICT-utrustning och -tjänster som staden eller DigiHelsingfors skaffat. • Sörjer för bland annat dessa tjänsters tekniska informationssäkerhet, dataskydd och kontinuitetshantering.	Producerar inga tjänster för staden.
Under dataintrånget	• **MiM**-arbetet inleds. • Ansvarar för den centraliserade kommunikationen på stadsnivå.	• Identifierar dataintrånget och inleder bekämpningsåtgärder. • Underrättar myndigheter, skaffar experthjälp samt informerar om det inträffade i stadsorganisationen. • **MiM**-arbetet startas.	• Deltar i det tekniska genomförandet av bekämpningsåtgärderna • Avbryter angreppet tillsammans med KASKO.	DigiHelsingfors informeras om upptäckten av dataintrång viaett företag.	• Skapar en lägesbild och bistår i att avsluta attacken. • Staden ger ett uppdrag till företaget efter att dataintrånget har upptäckts.
Efter dataintrånget	• Hanterar och leder situationen. • Informationsskyldighet för dem som varit föremål för säkerhetsöverträdelsen. • Utarbetar en utvecklingsplan för att förbättra informationssäkerheten.	Utredningsåtgärder enligt verksamhetsområde, bl.a. utredning av innehållet i nätverksenheter.	Föreslår utvecklingsåtgärder som förbättrar informationssäkerheten och genomför åtgärderna.	• Vid utredning av dataintrång nödvändig hjälp t.ex. gällande forensisk undersökning av utrustning och nödvändiga logguppgifter. • Utvecklar informationssäkerhetstjänsterna.	• Producerar nya nödvändiga informationssäkerhetstjänster. • Forensisk undersökning av och rapportering om händelsen, utarbetar rekommendationer.

Figur 10. Helsingfors stads interna och externa aktörer samt ansvar vid dataintrång.

2.8 Myndigheternas verksamhet

Till **finansministeriets** uppgifter hör allmän utveckling av informationssäkerheten inom den offentliga förvaltningen. Den deltar också i utvecklingen av den nationella cybersäkerhetsstrategin samt i utvecklingen av lagstiftningen om informations- och cybersäkerhet. Under de senaste åren har tyngdpunkten i utvecklingen bland annat legat på att utveckla störningshanteringen och beredskapen för gemensamma informations- och kommunikationstekniska tjänster samt på att förbättra informationssäkerheten och dataskyddet inom kritiska samhällssektorer (Titukri). Finansministeriet utvecklar upprättandet av en lägesbild av cybersäkerheten inom den offentliga förvaltningen vid sidan av andra myndigheter och stöder utvecklingen och användningen av Myndigheten för digitalisering och befolkningsdatas tjänster för digital säkerhet och informationstjänster.

Kommunikationsministeriet

Kommunikationsministeriet ansvarar för lagstiftningen och strategiarbetet i anslutning till informationssäkerheten i kommunikationsnäten och -tjänsterna. Kommunikationsministeriets uppgift är att möjliggöra fungerande och hållbara lösningar för digitalisering, trafik och kommunikation. Målet är att säkerställa och främja medborgarnas, näringslivets och den offentliga förvaltningens förtroende för säkerheten hos informationssamhällets tjänster. Förtroendet grundar sig bland annat på att tjänsterna är lätta att använda, att integritetsskyddet säkerställs och att innehållet är äkta.

Kommunikationsministeriet bereder de politiska och strategiska riktlinjerna och lagstiftningen för sitt verksamhetsområde. Dessutom är ministeriet en aktiv aktör i internationella forum. Ministeriet sörjer för att förbindelserna fungerar och är säkra, för en rättvis grön och digital omställning samt för förutsättningarna för att utnyttja informationen.

Kommunikationsministeriet ansvarar för upprätthållandet av den nationella samarbetsmodellen för cybersäkerhet i enlighet med säkerhetsstrategin för samhället. Transport- och kommunikationsverket inom kommunikationsministeriets förvaltningsområde ansvarar för myndighetsuppgifterna inom trafik och kommunikation och Cybersäkerhetscentret vid Transport- och kommunikationsverket stöder, styr och övervakar informationssäkerheten och integritetsskyddet i den elektroniska kommunikationen samt upprätthåller lägesbilden över den nationella cybersäkerheten.

Statens cybersäkerhetsdirektörs byrå vid Kommunikationsministeriet är en från ministeriets avdelningar fristående verksamhetsenhet som koordinerar och samordnar frågor som gäller den nationella cybersäkerheten på hela statsrådets nivå. Byrån ansvarar nationellt för koordineringen och samordningen av utvecklingen, planeringen, beredskapen och beredskapen för kritisk informations- och kommunikationsteknisk infrastruktur på strategisk nivå. Den samordnar också uppföljningen av åtgärderna i Finlands cybersäkerhetsstrategi tillsammans med den uppföljningsgrupp som ministerierna bildar och dess sekretariat.

Den nationella informationssäkerhetsmyndigheten är **Transport- och kommunikationsverket Traficom**, som är verksamt inom kommunikationsministeriets förvaltningsområde. **Cybersäkerhetscentret** hör till Transport- och kommunikationsverket Traficom och dess uppgifter regleras i lagen om Transport- och kommunikationsverket[37].

Cybersäkerhetscentret stöder, styr och övervakar informationssäkerheten och integritetsskyddet i den elektroniska kommunikationen. Den upprätthåller lägesbilden över den nationella cybersäkerheten. Cybersäkerhetscentrets verksamhet främjar och säkerställer informationssäkerheten i informationssystemen och datakommunikationen. Cybersäkerhetscentret ansvarig myndighet för den offentliga reglerade satellittjänsten och nationellt samordningscentrum enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Dessutom sörjer Cybersäkerhetscentret för kommunikationssektorns beredskap för störningar under normala förhållanden och undantagsförhållanden, främjar och övervakar funktionssäkerheten i den elektroniska kommunikationen samt stöder inom sitt verksamhetsområde samhällets allmänna beredskap för störningar under normala förhållanden och undantagsförhållanden. (19.11.2021/1002)

Bestämmelser om Traficoms uppgifter som hänför sig till cybersäkerhet finns dessutom i 304.1 § i lagen om tjänster inom elektronisk kommunikation (917/2014). Enligt 1, 7, 8 och 10 punkten i denna paragraf ska Transport- och kommunikationsverket, utöver vad som föreskrivs någon annanstans i denna lag

1) främja den elektroniska kommunikationens funktion, störningsfrihet och trygghet,

7) samla in information om kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem samt om fel och störningar i kommunikationsnät och kommunikationstjänster,

[37] 936/2012.

8) informera om frågor som gäller informationssäkerhet samt om kommunikationsnäts och kommunikationstjänsters funktion,

10) utreda kränkningar och hot om kränkningar av informationssäkerheten för nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem.

Utifrån dessa lagstadgade uppgifter är CERT-funktionens lagstadgade uppgift också att sammanställa och dela den nationella lägesbilden över cybersäkerheten för att utreda och förebygga informationssäkerhetsincidenter.

För att sköta sina lagstadgade uppgifter tar Cybersäkerhetscentret emot frivilliga anmälningar om informationssäkerhetsincidenter som klassificeras utifrån incidentens betydelse och konsekvensernas omfattning. Syftet med klassificeringen är att göra en första bedömning av hur kritisk incidenten är och hur snabbt man borde reagera på den i ljuset av de uppgifter som anmälaren angett. Dessutom kan den utifrån anmälningarna varna andra aktörer så att de kan förbättra nivån på sin egen cybersäkerhet.

Cybersäkerhetscentret fungerar som ett nationellt samordningscentrum[38] och en nationell NIS-samordningspunkt mellan olika myndigheter. Uppgiften utvidgades i fråga om verkställandet av NIS 2-direktivet[39] som trädde i kraft den 8 oktober 2024 genom cybersäkerhetslagen som trädde i kraft den 8 april 2025.[40]

Cybersäkerhetslagen[41] innehåller bestämmelser om uppgifter i anslutning till cybersäkerheten vid CSIRT-enheten vid Cybersäkerhetscentret vid Transport- och kommunikationsverket. Enligt 20 § 1 mom. i cybersäkerhetslagen är CSIRT-enhetens uppgift bland annat att reagera på incidentanmälningar och vid behov bistå den part som anmält incidenten i hanteringen av incidenten samt samla in och analysera information om hot och information om utredning av kränkningar av informationssäkerheten. Dessutom innehåller cybersäkerhetslagen mer detaljerade bestämmelser än tidigare om de lagstadgade uppgifterna och befogenheterna i anslutning till produktionen av Cybersäkerhetscentrets HAVARO- och Hyöky-tjänster.

Enligt 303.1 § i lagen om tjänster inom elektronisk kommunikation (917/2014) ska Transport- och kommunikationsverket till uppgift att utöva tillsyn över efterlevnaden av denna lag samt bestämmelser som utfärdats och beslut som meddelats med stöd av den, om inte något annat föreskrivs i denna lag.

I lagen om tjänster inom elektronisk kommunikation föreskrivs bland annat om skyldigheter som gäller informationssäkerhet vid behandling av elektronisk kommunikation hos teleföretag, sammanslutningsabonnenter och andra kommunikationsförmedlare. Dessutom innehåller lagen och de föreskrifter som utfärdats med stöd av den många krav på televerksamhetens informationssäkerhet och beredskap. Inom Traficom ansvarar Cybersäkerhetscentrets styrnings- och övervakningsavdelning för styrningen och övervakningen av aktörerna i anslutning till dessa bestämmelser och de föreskrifter som utfärdats med stöd av dem.

[38] Europaparlamentets och rådets förordning om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (EU) 2021/887.
[39] Europeiska unionens direktiv NIS 2 dvs. Network and Information Security Directive (nätverks- och informationssäkerhetsdirektivet).
[40] RP 243/2022.
[41] 124/2025.

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom är dessutom tillsynsmyndighet för vissa aktörer inom den offentliga förvaltningen och sektorn för digital infrastruktur, forskningsorganisationer, tillhandahållare av digitala tjänster samt aktörer som tillhandahåller hantering av ICT-tjänster i enlighet med den nationella cybersäkerhetslagen som grundar sig på NIS2-/cybersäkerhetsdirektivet.

Cybersäkerhetscentret utvecklar och övervakar kommunikationsnätens och -tjänsternas driftsäkerhet och säkerhet samt producerar en lägesbild av cybersäkerheten. Centret publicerar en månatlig Cyberväderrapport och en veckoöversikt över aktuella händelser.

Cybersäkerhetscentrets kunder kan utnyttja lägesbildsinformationen för att ordna och prioritera sin egen beredskap. Vid skapandet av lägesbilden utnyttjas hela Traficoms verksamhetsområde inom trafik- och kommunikationssektorn samt nätverk av nationella källor, såsom försörjningsberedskapskritiska organisationer och säkerhetsmyndigheter. Dessutom utnyttjas officiella eller frivilliga internationella samarbetsnätverk som grundar sig på ömsesidigt förtroende.

Hyöky-tjänsten[42] är en tjänst som Cybersäkerhetscentret erbjuder organisationer inom den offentliga förvaltningen och aktörer som är kritiska för samhällets funktion för att kartlägga angreppsytan i det offentliga nätet. En kund som ansluter sig till Hyöky-tjänsten meddelar vilka IP-adressrymder denne använder och mot vilka informationssäkerhetskartläggningen riktas. Hyöky-rapporter skickas till beställaren med några månaders mellanrum eller vid behov.

Helsingfors stad blev kund hos Hyöky-tjänsten i slutet av 2023. I utredningen granskades fyra Hyöky-rapporter från 2023–2024. I rapporterna lyfts fram kritiska sårbarheter med hög risk.

I den första kartläggningen meddelades endast IP-rymden för offentliga tjänster för fostrans- och utbildningssektorn. På så sätt ville man säkerställa att portskanningarna inte har oönskade sidoeffekter, såsom obefogade varningar för nätattacker. VPN-routern som var föremål för dataintrånget ansågs inte höra till de offentliga tjänsternas IP-rymd, så dess IP-adress ingick inte i kartläggningen.

Om VPN-routern hade ingått i kartläggningen skulle den ha visats som en enhet som observerats i rapporten. Skanningen skulle ha listat servern och fostrans- och utbildningssektorn kunde ha upptäckt att det i nätverket finns en ”glömd” enhet som syns utåt.

Cybersäkerhetscentret genomförde tillsammans med Helsingfors stad i samband med utredningen av dataintrånget vid sidan av de externa Hyöky-skanningarna även andra mer omfattande interna skanningar i Helsingfors stadsmiljö med olika skanningsverktyg. Cybersäkerhetscentret säkerställde bland annat i samarbete med Helsingfors stads olika sektorer att alla tillgängliga IP-adressblock är kända. Flera skanningar gjordes i blocken för att upptäcka andra potentiellt sårbara objekt. Dessutom strävade man efter att med hjälp av skanningarna utreda om angriparen hade kunnat utvidga sin åtkomst till stadens övriga verksamhetsområden, om angriparen ännu var aktiv i stadens webbmiljö och hitta de bakportar som angriparen eventuellt installerat.

Cybersäkerhetscentret utförde en separat skanning av Finlands adressrymd för att utreda om andra organisationer använder motsvarande föråldrade och sårbara VPN-enheter.

[42] Tjänst för kartläggning av angreppsyta.

Havaro (HAvainnointi ja VAROitus) är en tjänst som är avsedd att upptäcka och på förhand varna för allvarliga informationssäkerhetsincidenter. Informationssäkerhetstjänsten i fråga produceras av Transport- och kommunikationsverket (Traficom). Havaro övervakar kundorganisationens datakommunikation och söker tecken på avancerade attacker, såsom statliga spionprogram och APT-verksamhet (Advanced Persistent Threat).

Tjänsten skaffas från ett kommersiellt servicecenter för informationssäkerhet (SOC) och Cybersäkerhetscentret ansvarar för dess verksamhet tillsammans med kommersiella aktörers experter inom branschen. Försörjningsberedskapskritiska aktörer som är viktiga för samhällets verksamhet samt aktörer inom den offentliga förvaltningen kan ta i bruk HAVARO-tjänsten genom att placera egen sensorutrustning eller programvara som den förutsätter i sin egen IT-miljö. Sensorerna strävar efter att upptäcka och varna för hotfull trafik. De data som HAVARO-tjänsten producerar används vid Cybersäkerhetscentret för att utreda betydande cyberincidenter och skapa en nationell lägesbild av cybersäkerheten.

CERT-funktionen (Computer Emergency Response Team) är en funktion vid Cybersäkerhetscentret, vars uppgift är att förebygga informationssäkerhetsincidenter och informera om informationssäkerhetsfrågor. Dessutom hjälper funktionen till att tekniskt utreda allvarliga informationssäkerhetsincidenter.

Anmälan om informationssäkerhetsincidenter lämnas till Cybersäkerhetscentret med en webblankett. Anmälningarna statistikförs och klassificeras. En klassificeringsgrund är hur stor grupp människor och aktörer som påverkas av incidenten, hur viktigt objektet är för samhället och hur omedelbara åtgärder som behövs. Efter klassificeringen bedöms vilka åtgärder som eventuellt behöver vidtas på basis av anmälan.

Cybersäkerhetscentret är i aktionsberedskap under alla tider på dygnet. Under natten har jouren ordnats med beredskapsarrangemang som vid behov kan reagera på allvarliga situationer.

Cybersäkerhetscentrets roll i vid informationssäkerhetsincidenter begränsas främst till att bistå och stödja den aktör som utsatts för incidenten. Syftet med den hjälp och det stöd som ges är att genom rådgivning främja utredningen och bekämpningen av informationssäkerhetsincidenter samt återhämtning. Omfattningen av den hjälp eller det stöd som ges har inte fastställts på förhand, utan påverkas bland annat av de resurser som finns tillgängliga vid tidpunkten i fråga. Dessutom påverkas saken av i vilken mån aktören själv förmår sköta och utreda frågan. För att sköta sina lagstadgade uppgifter som utredning av informationssäkerhetsincidenter i exceptionella fall, såsom i Helsingfors stads dataintrång, kan Cybersäkerhetscentrets experter bistå kunden även i den konkreta hanteringen av incidenter (DFIR, Digital Forensics & Incident Response).

Föremål för informationssäkerhetsincidenter kan vara aktörer med mycket varierande resurser och därför kan behovet av myndighetshjälp variera oförutsägbart. Cybersäkerhetscentret hade ingen allmän processbeskrivning för utredning av dataintrångsfall vid tidpunkten för dataintrånget i fråga.

Beredskapen att utreda och bekämpa informationssäkerhetsincidenter grundar sig i Finland på ett omfattande samarbete och informationsförmedling mellan myndigheter och informationssäkerhetsföretag samt andra aktörer. Cybersäkerhetscentret är en aktör som samlar och främjar verksamheten. Dess hjälptjänster är avgiftsfria för organisationer som fallit offer för incidenter.

I anslutning till den nationella samordningen av cybersäkerheten koordinerar Cybersäkerhetscentret ISAC-grupperna för utbyte av information[43], som är samarbetsorgan för cybersäkerhet som grundats inom olika branscher. I ISAC-grupperna behandlas frågor som gäller cybersäkerhet konfidentiellt, såsom hot, fenomen och god praxis. Det finns också egna grupper för kommunerna och statsförvaltningen.

Utbildningsstyrelsen är ett ämbetsverk som lyder under undervisnings- och kulturministeriet och som ansvarar för utvecklingen, styrningen och utvärderingen av utbildningen och småbarnspedagogiken. Till dess uppgifter hör att utarbeta läroplaner och examensgrunder, genomföra utbildningspolitiska mål samt utveckla åtgärder som främjar utbildningens kvalitet och jämlikhet. Utbildningsstyrelsen stöder läroanstalter, lärare och elever genom att erbjuda anvisningar, material och finansiering. Dessutom ansvarar den för det internationella samarbetet inom utbildningen och deltar i utvecklingen av det finländska utbildningssystemet.

Utbildningsstyrelsen har utarbetat omfattande anvisningar för undervisnings- och bildningsförvaltningen om behandling av skolornas och daghemmens uppgifter, dataskydd och informationssäkerhet. Materialet har utarbetats tillsammans med dataombudsmannen. Dataombudsmannen lämnade den 15 oktober 2021 en motion till Utbildningsstyrelsen om att utveckla användningen av personuppgifter i de informationssystem som används i undervisningen. Åtgärderna enligt motionen pågår fortfarande.

Informationshanteringsnämnden är en specialmyndighet som inrättats i anslutning till finansministeriet och vars uppgift är att utvärdera och främja tillgodoseendet av kraven och genomförandet av förfaringssätten som föreskrivs i informationshanteringslagen. Informationshanteringsnämnden består av representanter för den offentliga förvaltningen. I den finns representanter för centrala myndigheter som styr informationshanteringen samt myndigheter som tillämpar informationshanteringslagen. Informationshanteringsnämnden utarbetar en utvärderingsrapport vartannat år om resultaten av dess utvärderingar och utarbetar i sin rapport rekommendationer riktade till finansministeriet. Informationshanteringsnämnden har inte heller behörighet att bedöma fullgörandet av informationssäkerhetskraven i 4 kap. i informationshanteringslagen.

Informationshanteringsnämnden har i sin utvärderingsberättelse fäst uppmärksamhet vid att uppgifterna att styra informationshanteringen fördelas på flera olika myndigheter och att de överlappar varandra.[44] Utöver informationshanteringsnämnden delar åtminstone Cybersäkerhetscentret, Försörjningsberedskapscentralen och Myndigheten för digitalisering och befolkningsdatas tjänster för digital säkerhet rekommendationer eller bästa praxis som styr informationssäkerheten. Dessutom har utrikesministeriet, Försörjningsberedskapscentralen och Riksarkivet uppgifter som hänför sig till ämnesområdet.

ISAC-grupper för utbyte av information, Information Sharing and Analysis Centre https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/isac-grupper-utbyte-av-information

[44] Informationshanteringsnämndens bedömningsrapport 2022–2023 s. 42. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165453/VM_2024_16.pdf (på finska)

Figur 11. Myndigheter i anslutning till styrningen av den allmänna lagstiftningen om informationshantering. (Bild: Informationshanteringsnämnden)

Informationshanteringsnämnden utvärderade Helsingfors stads verksamhet 2020–2023 som en del av sitt normala arbete enligt tillsynsplanen för kommunfältet. Övervakningen är till sin natur laglighetsövervakning och genomförs främst genom begäran om information och enkäter. Inget egentligt övervakningsbesök gjordes hos Helsingfors stad. På basis av utvärderingarna observerades inga brister i efterlevnaden av Helsingfors stads skyldigheter enligt informationshanteringslagen.

Polisinrättningen i Helsingfors är Finlands största polisenhet. Där arbetar cirka 1 600 personer, varav cirka 1 300 är poliser. Enheten verkar inom Helsingfors stads område och ansvarar för den lokala polisens uppgifter. Dessutom ansvarar enheten för säkerheten för republikens president, statsrådets medlemmar och statsgäster. Även polisens riksomfattande beredskapsenhet Karhu, den riksomfattande gruppen för utredning av människohandel samt trafiksäkerhetscentralen har förlagts vid polisinrättningen i Helsingfors.

Polisinrättningen ansvarar för förundersökningen av brott inom sitt område, om inte något annat följer av polisens arbetsfördelning. Polisinrättningen i Helsingfors tog emot Helsingfors stads brottsanmälan via det elektroniska anmälningssystemet. Brottsanmälan förbehandlades och en utredare och undersökningsledare förordnades för den.

Polisinrättningens förundersökningsåtgärder var bland annat inhämtande av information från Helsingfors stad samt publicerande av ett meddelande om inledande av förundersökning. Polisinrättningen inledde också ett samarbete med centralkriminalpolisen.

Centralkriminalpolisen (CKP) är en riksomfattande specialenhet inom polisförvaltningen i Finland med hela Finland som verksamhetsområde. Centralkriminalpolisen har specialkompetens inom till exempel bekämpning av organiserad brottslighet, narkotikabrottslighet, ekonomisk brottslighet och cyberbrottslighet. Den samarbetar internationellt med myndigheter i andra länder och samordnar Finlands deltagande i

Europols och Interpols verksamhet. Centralkriminalpolisen stöder den lokala polisen i komplicerade brottsutredningar och ansvarar för sin del för att upprätthålla landets säkerhet.

Centralkriminalpolisen samarbetar med den lokala polisen så att den lokala polisen sköter ärenden som gäller sakägare och centralkriminalpolisen ärenden som gäller teknisk undersökning och internationellt samarbete. Den allmänna ledaren för undersökningen är från Centralkriminalpolisen.

Centralkriminalpolisens åtgärder i samband med dataintrånget mot Helsingfors hänför sig till förundersökningen. Till dessa delar avviker polisens verksamhet vid datanätsbrott från andra brottstyper, eftersom polisens möjligheter att avbryta brottet i datanätet är mycket begränsade.

Efter att intrånget upptäcktes återställde andra aktörers räddningsåtgärder fostrans- och utbildningssektorns nät till ett säkert tillstånd. Polisen har inga verksamhetsförutsättningar för att ta kontroll över nätmiljöer, börja övervaka dem eller avlägsna inkräktare från nätet. Sådana åtgärder är beroende av den organisation som utsatts för attacken eller de tjänsteproducenter som organisationen anlitar.

Utredningen av nätbrott och förverkligandet av straffansvaret kräver i allmänhet betydande internationellt samarbete och kontakter som Centralkriminalpolisen ansvarar för.

CKP meddelade den 13 mars 2025 att man misstänker ett dataskyddsbrott i anslutning till dataintrånget mot Helsingfors stad och att den inledde en förundersökning av det. I utredningen fastställs huruvida staden hade skyddat uppgifterna på behörigt sätt.

Skyddspolisen (Skypo) förebygger och bekämpar de allra allvarligaste hoten mot den nationella säkerheten, såsom terrorism och olaglig underrättelseverksamhet som främmande stater riktar mot Finland. I och med coronapandemin och digitaliseringen har företagens och samhällets funktioner i allt högre grad flyttats till nätet, varvid även nätets roll i Skyddspolisens underrättelseverksamhet har ökat. I utredningen av dataintrånget följde Skyddspolisen främst förundersökningens framskridande.

Dataombudsmannen är en självständig myndighet vars uppgift är att övervaka behandlingen av personuppgifter och säkerställa att dataskyddsförordningen och annan speciallagstiftning om behandling av personuppgifter iakttas. Dataombudsmannen ger råd i dataskyddsfrågor, behandlar klagomål som gäller personuppgiftsincident och kan påföra påföljdsavgifter. Dataombudsmannen har rätt att granska organisationernas dataskyddspraxis. Vid dataombudsmannens byrå arbetar förutom dataombudsmannen två biträdande dataombudsmän samt cirka 60 andra tjänstemän.

Den personuppgiftsansvarige är skyldig att underrätta dataombudsmannen om en personuppgiftsincident inom 72 timmar. Dataombudsmannens byrå inleder utredningen av fallet på basis av anmälan.

Dataombudsmannen har utrett dataintrånget mot Helsingfors stad med stöd av bestämmelserna om behandling av förvaltningsärenden och kommer att ge ett avgörande i ärendet senare. Den tillsyn som dataombudsmannen utövar är till sin natur laglighetsövervakning och genomförs i behandlingsprocessen för ett förvaltningsärende i den ordning som föreskrivs i förvaltningslagen.

Dataombudsmannen tog emot Helsingfors stads anmälan om informationssäkerhetsincidenten efter att dataintrånget upptäckts den 30 april 2024, på basis av vilken dataombudsmannens byrå började utreda ärendet. Helsingfors stad kompletterade sin anmälan flera gånger efter att de interna utredningsåtgärderna framskridit och på basis av

de tilläggsutredningar som dataombudsmannens byrå begärt. Dataombudsmannen gav Helsingfors stad råd i frågor som gäller efterlevnaden av dataskyddsförordningen, såsom skyldigheten att informera om dataintrång.

Utöver det ovan nämnda har dataombudsmannen stött Helsingfors stads kommunikationsåtgärder samt tagit emot kontakter från personer vars uppgifter kan ha funnits i materialet som ingick i dataintrånget.

Finlands Kommunförbund rf är en registrerad förening som består av kommunerna. I föreningens verksamhet deltar också landskapsförbund, samkommuner och aktiebolag med kommunal bakgrund. Kommunförbundet är en gemensam intressebevakare för kommunfältet, i vars organisation arbetar cirka 140 personer. Kommunförbundets dotterbolag är FCG Finnish Consulting Group Oy, KL-Kuntahankinnat Oy och KL-Kustannus Oy. Kommunförbundets intressebevakning omfattar alla ärenden som gäller kommunfältet. Detta omfattar också frågor som gäller kommunernas småbarnspedagogik, grundläggande utbildning och utbildning på andra stadiet samt digitalisering, cybersäkerhet och dataskydd. Kommunförbundet stöder kollegial utveckling och nätverksbildning inom kommunernas informationshantering, informationssäkerhet och dataskydd till exempel genom att upprätthålla nätverk för kommunernas informationssäkerhets- och dataskyddsansvariga och informationshantering samt erbjuda sina medlemmar rådgivning. Dessutom ordnar FCG avgiftsbelagda evenemang och utbildningar om digital säkerhet för kommunfältet.

I myndigheternas förebyggande verksamhet betonas handledande och rådgivande verksamhet, med vilken man strävar efter att se till att verksamhetsutövaren har identifierat de centrala ansvaren som hänför sig till behandlingen av personuppgifter och informationshanteringen. Fullgörandet av dessa skyldigheter omfattas dock begränsat av regelbunden tillsynsverksamhet. Informationshanteringsnämndens tillsynsarbete strävar närmast efter att beskriva verkställandet av informationshanteringsskyldigheterna på riksnivå. Dataombudsmannen genomför planerade och oanmälda tillsynsbesök. Tillgodoseendet av ansvaren kan närmast bedömas i efterhand i samband med olika informationssäkerhetsincidenter eller via klagomål över verksamheten.

Med Hyöky- och Havaro-tjänsterna som upprätthålls med offentliga medel har man kunnat identifiera och förhindra hot och sårbarheter som den organisation som använder dem eller den informationssäkerhetsleverantör som organisationen anlitat inte har upptäckt. Tjänsterna används dock inte i stor utsträckning inom den offentliga sektorn. Tjänsterna behöver också utvecklas tekniskt.

Centrala åtgärder i brottsbekämpningen är att förebygga brott och säkerställa att straffansvaret förverkligas. Dessa åtgärder förutsätter internationellt samarbete. Nationella utvecklingsprojekt för bekämpning av nätbrottslighet är också betydelsefulla.

Kärnan i hanteringen av en dataintrångsfallet är den organisation som innehar de uppgifter som dataintrånget gäller. Detta förutsätter att organisationen har tekniska och administrativa skyddsmetoder som står i proportion till datariskerna samt förmåga att upptäcka och avvärja ett påbörjat dataintrång. Dessutom ska organisationen på förhand säkerställa att den vid behov har den kompetens som behövs för att bekämpa, utreda och hantera ett dataintrång. Den organisation som har förvaltat uppgifterna ansvarar också för att informera offren för dataintrånget.

Organisationen kan genom förberedelser på förhand se till att den har tillgång till tillräckligt sakkunnig hjälp för att utreda och hantera dataintrång. I Finland finns flera sådana företag

som erbjuder DFIR-tjänster (Digital Forensics & Incident Response). För att utreda ett brottmål behövs kunskap om organisationen och informationssystemmiljön, vilket förundersökningsmyndigheterna inte har. Därför har utredningar som organisationen själv gjort eller inhämtat från företag en central roll i utredningen av brottet.

Flera olika myndigheter deltar i utredningen av dataintrång i enlighet med sina egna uppgifter (lokalt, nationellt och internationellt). Cybersäkerhetscentret ger den mest omfattande avgiftsfria experthjälpen för att stödja den som utsatts för dataintrång.

Lagstiftningen fastställer inte någon den ledande myndighet för **dataintrång** på samma sätt som för olyckor och brott i den verkliga världen, där det allmänna ledningsansvaret vanligtvis fördelas mellan räddnings- eller polismyndigheten. Modellen för hantering av störningssituationer avviker från det ovan nämnda och följer ansvarsfördelningen i riskhanteringen, där aktören också mycket självständigt ansvarar för behandlingen av avvikande och störningssituationer.

Den nationella samarbetsmodellen för cybersäkerhet har decentraliserats i Finland och motsvarar till sina principer samarbetsmodellen för övergripande säkerhet. I samarbetsmodellen för cybersäkerhet leder de behöriga myndigheterna hanteringen av störningssituationer inom ramen för sina uppgifter och befogenheter. Upprätthållandet av samarbetsmodellen för cybersäkerhet är en av de strategiska uppgifterna i säkerhetsstrategin för samhället och dess mål är att säkerställa ett nära samarbete mellan samhällets centrala aktörer i alla förhållanden.

I och med cybersäkerhetslagen utarbetas för krissituationer som gäller cybersäkerheten en plan för hantering av omfattande cybersäkerhetsincidenter och kriser. I planen specificeras de tillgängliga beredskaperna, resurserna och förfarandena. Dessa omfattar också nödvändig information om myndigheternas uppgifter och ansvar.

Hanteringen av störningssituationer som hotar samhällets vitala funktioner stöder sig i enlighet med modellen för övergripande säkerhet på ett så omfattande samarbete som möjligt mellan myndigheter, lokalförvaltningen, olika förvaltningsområden och ministerier samt näringslivet och på att stödja andra säkerhetsaktörer. Denna modell gäller också hanteringen av cyberincidenter, där flera myndigheter har en uppgift beroende på incidentens fas. Cybersäkerhetscentret vid Traficom ansvarar för att utreda incidenten och samordna åtgärderna i den första fasen av cyberincidenten som anmälts till centret. I det skede då en organisation som utsatts för en cyberincident gör en brottsanmälan överförs ansvaret för att leda och utreda ärendet till polisen. Den behöriga myndigheten leder den operativa verksamheten, inleder åtgärder i anslutning till hanteringen av störningssituationer, ansvarar för kommunikationen och informerar om situationen enligt överenskommen praxis.

Lagstiftningen om bekämpning av cybersäkerhetshändelser kommer att ändras. Till exempel kommer samarbete mellan myndigheter vid hantering av omfattande cybersäkerhetsincidenter och kriser att granskas på nytt.

	KOMMUNIKATIONS-MINISTERIETS FÖRVALTNINGSOMRÅDE	INRIKESMINISTERIETS FÖRVALTNINGSOMRÅDE			ANDRA MYNDIGHETER
Aktörens namn	**Cybersäkerhetscentret vid Traficom**	**Polisinrättningen i Helsingfors**	**Centralkriminalpolisen**	**Skypo**	**Dataombudsmannens byrå**
Allmän beskrivning	Cybersäkerhetscentrets CERT-funktion (Computer Emergency Response Team) har i uppgift är att förebygga informations-säkerhetsincidenter och informera om informations-säkerhetsfrågor.	Förundersökningsmyndigheter		Nationell säkerhet	Nationell dataskyddsmyndighet
Före data-intrånget	• Lägesbild- och nätverkstjänst, observation och handräckning • Upprätthåller partnerskap och internationella relationer för att sköta sina uppgifter. • Kartläggningstjänst av angreppsytan för att förbättra cybersäkerheten. Hjälper er att rikta korrigeringsåtgärder till rätt frågor och minimera riskerna. • Upptäcker kränkningar av allvarlig informationssäkerhet inom klientens nätverk		• Projekt för förebyggande av nätbrottslighet. • Internationellt informationsutbyte och brottsbekämpning.	Upptäcka, förhindra och avslöja sådana gärningar, projekt och brott som kan hota stats- och samhällsskicket eller Finlands interna eller externa säkerhet.	Övervaka att dataskydds-lagstiftningen och andra lagar som gäller behandlingen av personuppgifter efterlevs, främja medvetenhet om risker, regler, skyddsåtgärder, skyldigheter och rättigheter som hänför sig till behandlingen av personuppgifter, utföra utredningar och inspektioner, påföra administrativa påföljder för brott mot dataskyddsförordningen.
Under data-intrånget	• Stöd för den utsatta organisationen och sakkunnighjälp. • Uppteckning av informationssäkerhetshot och lansering av motåtgärder.	• Mottagande av brottsanmälan enligt principen om områdesansvar. • Inledande av förundersökning. • Samarbete med CKP.	Deltagande i förundersökningen och stödja den	Sakkunnighjälp vid behov.	• Mottagande av anmälan om personuppgiftsincidenter. • Sakkunnighjälp vid behov.
Efter data-intrånget	• Genomförande av Hyöky-skanningar. • Förmedling och samman-ställande av informationen nationellt och internationellt. • Ge förslag till utveckling av informationssäkerhets-åtgärder. • Stödtjänst för utredning och återställning av verksamhet efter dataintrång. • Vid behov DFIR utredning	• Skyldighet att genomföra förundersökning. • Utredningsåtgärder. • Kontakt med målsägande i dataintrånget. • Ledningen för förunder-sökningen övergår till CKP.	• Frågor om den inter-nationella dimensionen för att identifiera och nå gärningsmannen. • Forensiska utrednings-åtgärder. • Kommunikation om utredningen av händelsen.	Dataintrångets betydelse för den nationella säkerheten.	• Övervakning av rättigheterna som hör till offren för personuppgiftsincidenten. • Påföra eventuella administrativa påföljder för brott mot dataskyddsförordningen.

Figur 12. Offentliga aktörer och myndigheter samt ansvar vid dataintrång.

2.9 Författningar, föreskrifter och anvisningar

I detta avsnitt behandlas föreskrifter, anvisningar och rekommendationer som utfärdats av aktörer utanför Helsingfors stad.

Enligt 8 § i **kommunallagen**[45] har kommunen organiseringsansvar för sina lagstadgade uppgifter. Ansvaret omfattar säkerställande av lika tillgång, fastställande av behovet, mängden och kvaliteten, val av produktionssätt, tillsyn över produktionen samt utövande av myndigheternas befogenheter och finansieringsansvar för uppgifterna.

Enligt kommunallagen ansvarar Helsingfors stad för att ordna småbarnspedagogik, grundläggande utbildning, gymnasieundervisning och yrkesutbildning. Närmare bestämmelser om uppgifterna finns i speciallagstiftningen, såsom lagen om småbarnspedagogik[46], lagen om grundläggande utbildning[47], gymnasielagen[48] och lagen om yrkesutbildning[49].

[45] 410/2015.
[46] 540/2018.
[47] 628/1998.
[48] 714/2018.
[49] 531/2017.

I 2 § 3 mom. i **Finlands grundlag**[50] föreskrivs om förvaltningens lagbundenhetsprincip som tryggar rättigheterna för dem som uträttar ärenden hos myndigheter. Enligt den ska all utövning av offentlig makt bygga på lag och i all offentlig verksamhet ska lag noggrant iakttas. I fråga om de lagstadgade tjänsterna är dock möjligheterna för kunder hos förvaltningen påverka behandlingen av sina egna ärenden eller uppgifter begränsade och därför är myndighetens åtgärder för att tillgodose rättsskyddet centrala.

Förvaltningens lagbundenhet framhävs av tjänsteansvaret enligt 118 § i grundlagen, enligt vilket en tjänsteman svarar för att hans eller hennes ämbetsåtgärder är lagliga. Detta tjänsteansvar kompletteras av strafflagen[51], där det i kapitel 40 föreskrivs om tjänstebrott, som omfattar bland annat brott mot tjänsteplikt enligt 9 § och brott mot tjänsteplikt av oaktsamhet enligt 10 §. När dataskyddslagen[52] stiftades ansågs kravet på lagenlighet inom förvaltningen och en tjänstemans tjänsteansvar vara en grund för att myndigheter inte ska omfattas av administrativ påföljdsavgift.[53]

Enligt de grunder för god förvaltning som anges i andra kapitlet i **förvaltningslagen**[54] tryggas rättigheterna för personer som uträttar ärenden hos myndigheterna, bland annat kravet på jämlikt och opartiskt bemötande av dem som uträttar ärenden hos förvaltningen samt utövandet av myndighetens befogenheter enbart för syften som är godtagbara enligt lag. Andra krav är serviceprincipen, informationsskyldigheten, rådgivningsarbetet, kravet på sakligt och klart språkbruk samt samarbetet mellan myndigheterna. Förvaltningens kunder tryggas också genom förvaltningslagens förfarandebestämmelser samt genom möjligheten att överklaga beslut eller anföra förvaltningsklagan. Dessutom övervakar riksdagens justitieombudsman och justitiekanslern att myndigheternas och tjänstemännens verksamhet är lagenlig samt att myndigheter och tjänstemän fullgör sina skyldigheter.

Enligt 90 § i **kommunallagen**[55] ska varje kommun och samkommun ha en förvaltningsstadga. I förvaltningsstadgan ges enligt lag behövliga bestämmelser om åtminstone ordnandet av kommunens förvaltning och verksamhet, om besluts- och förvaltningsförfarandet samt om fullmäktiges verksamhet.

I förvaltningsstadgan för Helsingfors stad föreskrivs bland annat att stadsstyrelsen svarar för att anvisningar, praxis, ansvarsfördelningen och övervakningen har fastställts för informationshanteringen och dokumentförvaltningen (24 kap. 5 §). I förvaltningsstadgan bestäms vidare att ledningen av informationshanteringen och dokumentförvaltningen ankommer på stadskansliets förvaltningsavdelning och att styrningen av informationsförvaltningen ankommer på stadskansliets strategiavdelning.

Bestämmelser om dataskydd och dokumenthantering

I artikel 8 i **Europeiska unionens stadga om de grundläggande rättigheterna** tryggas skyddet för personuppgifter som en egen grundläggande rättighet, medan skyddet för privatlivet och familjelivet tryggas i artikel 7 i samma rättsakt. Personuppgifterna tryggas också av artikel 8 om skydd för privatlivet i Europakonventionen, rätten till privat- och familjeliv enligt artikel 17 i den internationella konventionen om medborgerliga och politiska rättigheter samt skyddet för privatlivet enligt 10 § och skyldigheten att tillgodose de grundläggande fri- och rättigheterna och de mänskliga rättigheterna enligt 22 § i Finlands

[50] 731/1999.
[51] 39/1889.
[52] 1050/2018.
[53] RP 9/2018 rd s. 57–58.
[54] 434/2003.
[55] 410/2015.

grundlag. Skyddet för personuppgifter omfattar också sådana personuppgifter som inte hör till privatlivet.

Det har skett många förändringar i lagstiftningen om dataskydd, informationssäkerhet och behandling av personuppgifter 2018–2025.

Tillämpningen av **Europeiska unionens allmänna dataskyddsförordning**[56] (GDPR, svensk förkortning DSF, dvs. dataskyddsförordningen) inleddes den 25 maj 2018. För att verkställa förordningen gjordes ändringar i flera författningar i Finland, varav den viktigaste var att stifta en dataskyddslag och upphäva personuppgiftslagen[57].

Dataskyddsförordningen innehåller bestämmelser om behandling av personuppgifter och om deras fria rörlighet. Enligt artikel 2 ska förordningen tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

Dataskyddsförordningen är till största delen tvingande reglering om den kan det inte föreskrivas något annat nationellt. Därför ger dataskyddslagen ingen heltäckande uppfattning om dataskyddets innehåll. I den nationella dataskyddslagen föreskrivs endast om de omständigheter för vilka dataskyddsförordningen förutsätter eller åtminstone tillåter nationell reglering.

Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person (*registrerad*), dvs. utöver direkta identifikationsuppgifter även sådana uppgifter med hjälp av vilka en viss person kan identifieras till exempel med hjälp av tilläggsuppgifter. Som *personuppgiftsansvarig* betraktas en person eller en juridisk person, en myndighet, en institution eller något annat organ som ensamt eller tillsammans med andra *bestämmer* ändamålen och medlen för behandlingen av personuppgifter Personuppgiftsansvar kan också fastställas genom lagstiftning.

Helsingfors stad är personuppgiftsansvarig för de personuppgifter som den har behandlat i sin verksamhet antingen genom att själv fastställa ändamålen och medlen för behandlingen eller genom att behandla personuppgifter för att fullgöra sin lagstadgade uppgift. Dataskyddsförordningen ålägger den personuppgiftsansvarige många skyldigheter i anslutning till behandlingen.

Lagen om informationshantering inom den offentliga förvaltningen[58] (informationshanteringslagen) tillämpas också på myndigheternas informationshantering och användning av informationssystem. Syftet med lagen är att säkerställa en enhetlig och kvalitativ hantering samt informationssäker behandling av myndigheternas informationsmaterial så att offentlighetsprincipen förverkligas samt att främja interoperabiliteten mellan informationssystem och informationslager. Enligt 3 § i informationshanteringslagen tillämpas lagen på informationshantering och på användning av informationssystem, då myndigheter behandlar informationsmaterial. I 2 § i informationshanteringslagen definieras de begrepp som används i informationshanteringslagen. I 4 § 1 mom. i informationshanteringslagen föreskrivs att kommuner och samkommuner är sådana informationshanteringsenheter som avses i lagen. Innan informationshanteringslagen trädde i kraft fanns det inte bestämmelser om hantering av informationsmaterial och informationshantering inom den offentliga förvaltningen i en enda allmän författning. Även efter att informationshanteringslagen trädde i kraft föreskrivs

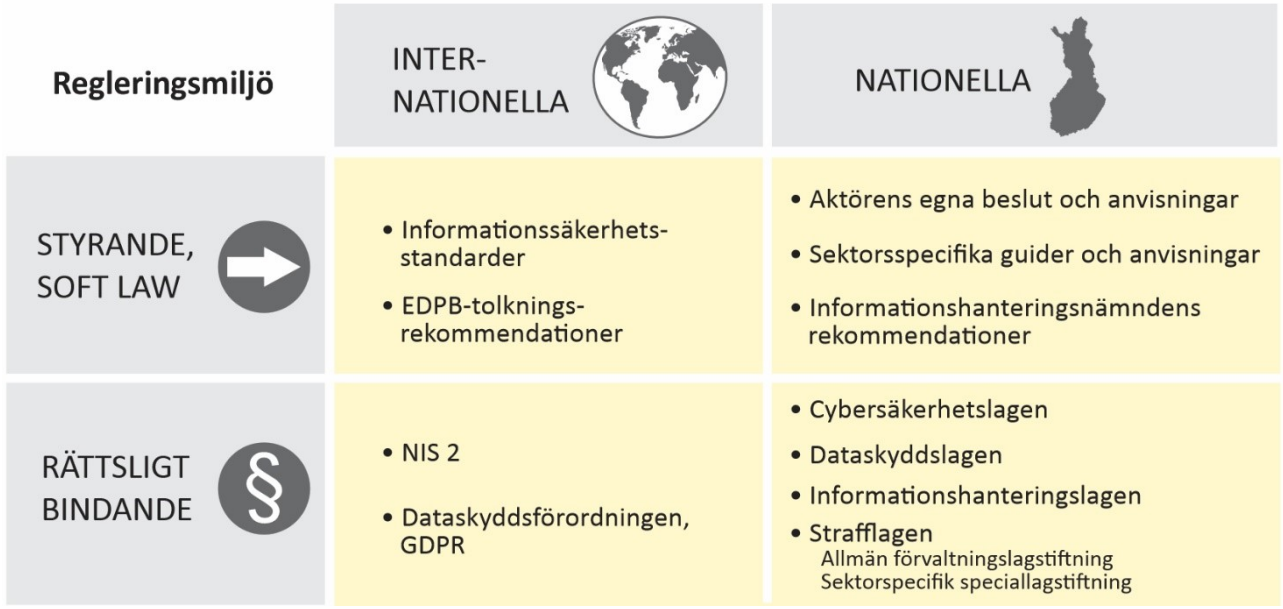
[56] (EU) 2016/679.
[57] 524/1999.
[58] 609/2019.

det om myndigheternas skyldigheter i fråga om informationshantering även i andra allmänna bestämmelser om förvaltning, bland annat i offentlighetslagen, arkivlagen och dataskyddsförordningen. Införandet av bestämmelsen har krävt betydande reformer av informationshanteringsenheterna.

I **lagen om offentlighet i myndigheternas verksamhet (offentlighetslagen)**[59] föreskrivs om myndigheternas skyldighet att främja offentlighet och öppenhet samt om de rättsliga förutsättningarna att begränsa dem. I 24 § i offentlighetslagen föreskrivs bland annat om sekretessbelagda uppgifter. Informationshanteringslagens organisatoriska tillämpningsområde regleras i offentlighetslagen.

I **arkivlagen**[60] föreskrivs om arkivbildarens skyldigheter. Enligt 7 § i arkivlagen har arkivfunktionens till uppgift att säkerställa att handlingar hålls tillgängliga och bevaras, att sköta den informationstjänst som hänför sig till dem, att bestämma handlingars förvaringsvärde och att gallra ut onödigt material. Vid arkiveringen ska tillgodoseendet av offentlighetsprincipen stödas genom att beakta enskilda personers och sammanslutningars rättsskydd samt dataskydd. Helsingfors stad är *arkivbildare* vars arkivfunktion enligt 9 § i arkivlagen ordnas av stadsstyrelsen.

Enligt 7 § i **förvaltningslagen** ska myndigheten sträva efter att ordna uträttandet av ärenden och behandlingen av ärenden så att den som vänder sig till förvaltningen får behörig service och att myndigheten kan sköta sin uppgift med gott resultat.



Figur 13. Regleringsmiljö för informationshantering, informationssäkerhet och dataskydd.

Krav på dataskydd

Dataskyddsförordningen ställer många slags krav på behandlingen av personuppgifter och många slags skyldigheter för den personuppgiftsansvarige. För det första ska det alltid finnas en grund för behandlingen enligt dataskyddsförordningen. Bestämmelser om allmänna grunder för behandling av personuppgifter finns i artikel 6 i dataskyddsförordningen, som kompletteras av 4 § i dataskyddslagen. För myndigheternas del är grunderna för

[59] 621/1999.
[60] 831/1994.

behandlingen i allmänhet fullgörandet av den personuppgiftsansvariges lagstadgade skyldighet, utförandet av en uppgift av allmänt intresse eller utövande av offentlig makt. Även samtycke, fullgörande av ett avtal och skydd av livsviktiga intressen är möjliga grunder för behandlingen.

Bestämmelser om behandling av särskilda kategorier av personuppgifter finns i artikel 9 i dataskyddsförordningen. Särskilda kategorier av personuppgifter är uppgift om till exempel etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse och hälsa. Till exempel en skolelevs religiösa övertygelse och hälsouppgifter hör således till kategorin särskilda personuppgifter.

Behandling av särskilda kategorier av personuppgifter är i regel förbjuden, men det finns flera undantag till detta. Behandling är tillåten till exempel när grunden för behandlingen är en uppgift som direkt föreskrivs för den personuppgiftsansvarige i lag, till exempel ordnande av småbarnspedagogik och grundläggande utbildning. I dataskyddslagen föreskrivs i fråga om särskilda grupper av personuppgifter att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga och särskilda åtgärder för att skydda den registrerades rättigheter. Sådana är till exempel

- åtgärder för att det i efterhand ska kunna säkerställas och bevisas vem som har registrerat, ändrat eller överfört personuppgifter,
- åtgärder för att höja kompetensen hos den personal som behandlar personuppgifter,
- utnämning av ett dataskyddsombud,
- den personuppgiftsansvariges och personuppgiftsbiträdets interna åtgärder för att förhindra tillträde till personuppgifter,
- pseudonymisering av personuppgifter,
- kryptering av personuppgifter,
- åtgärder för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna i anknytning till behandlingen av personuppgifterna, inbegripen förmåga att återställa tillgängligheten och tillgången till uppgifterna i rimlig tid vid en fysisk eller teknisk incident,
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet,
- särskilda förfaranderegler för att säkerställa att dataskyddsförordningen och denna lag iakttas när personuppgifter överförs eller behandlas för något annat ändamål,
- utförande av en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen,
- andra tekniska, förfarandemässiga och organisatoriska åtgärder.

Om behandling av personuppgifter som rör **fällande domar i brottmål samt lagöverträdelser som innefattar brottfällande domar** föreskrivs separat i artikel 10 i dataskyddsförordningen samt i 7 § i dataskyddslagen.

I artikel 5.1 i dataskyddsförordningen anges principerna för behandling av personuppgifter, som alltid ska följas när personuppgifter behandlas. Enligt punkt 2 ska den personuppgiftsansvarige ansvara för och kunna *visa* att dessa principer efterlevs (ansvarsskyldighet).

Enligt dataskyddsprinciperna ska personuppgifter

- behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade,
- samlas in och behandlas för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål,

- vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas,
- om nödvändigt uppdateras: inexakta och felaktiga personuppgifter ska raderas eller rättas utan dröjsmål,
- förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas,
- behandlas konfidentiellt och säkert.

I artikel 24 i **dataskyddsförordningen** föreskrivs om hur den personuppgiftsansvarige ska agera för att säkerställa och visa att behandlingen av personuppgifter sker lagenligt. Enligt punkt 1 i artikeln ska den personuppgiftsansvarige genomföra lämpliga *tekniska* och *organisatoriska* åtgärder för att *säkerställa* och kunna *visa* att behandlingen utförs i enlighet med dataskyddsförordningen. Hurdana tekniska och organisatoriska åtgärder som krävs bedöms med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter. I fråga om särskilda kategorier av personuppgifter förutsätts noggrannare processer och strängare säkerhetsåtgärder än för sådana personuppgifter som till exempel inte innehåller uppgifter som rör den registrerades privatliv. De åtgärder som krävs påverkas också till exempel av dataskyddsprinciperna enligt artikel 5.1 i dataskyddsförordningen.

Till *tekniska informationssäkerhetsåtgärder* hör till exempel övervakning av åtkomsten till enheter och system, förhindrande av olovlig användning av personuppgifter och system, registrering av händelser, övervakning av datatrafikens ursprung och routning, fastställande av systemens användarrättigheter, ändamålsenlig organisering av underhållsåtgärderna och skyddet av personuppgifter och system mot gärningar eller händelser som äventyrar informationssäkerheten, såsom virus och andra skadliga program. Vid behov ska informationssystemet skyddas till exempel så att redan olagliga försök att få åtkomst till personuppgifter utlöser ett larm till den personuppgiftsansvarige.

Till *organisatoriska åtgärder* hör till exempel organisationsarrangemang, fastställande av personalens uppgifter och ansvar samt anvisningar, utbildning och tillsyn. Den personuppgiftsansvarige ska till exempel se till att användarens rättigheter motsvarar användarens ställning och ansvar och att användaren endast får åtkomst till sådana personuppgifter som han eller hon behöver behandla för att kunna sköta sina arbetsuppgifter. Rätten att behandla personuppgifter ska vara mer begränsad ju känsligare eller sensitivare uppgifter det är fråga om. Vid behov ska man också skapa förfaranden, till exempel ett logginformationssystem, med hjälp av vilka man kan följa upp användningen av personuppgifterna och utlämnandet av personuppgifter.

Det räcker inte att de tekniska och organisatoriska åtgärderna vidtas en gång och glöms bort efter det, utan de vidtagna åtgärderna ska granskas regelbundet och uppdateras vid behov.

Den personuppgiftsansvariges *ansvarsskyldighet* grundar sig på både artikel 5.2 och artikel 24.1 i dataskyddsförordningen. För det första, ansvarsskyldigheten ”tvingar” den personuppgiftsansvarige att fundera över och skriva ner sina processer, varvid man eventuellt upptäcker brister som man hinner åtgärda innan den konkreta skadan inträffar. För det andra kan den personuppgiftsansvarige med hjälp av ansvarsskyldigheten visa att den aktivt har strävat efter att identifiera risker i anslutning till dataskyddet och vidtagit nödvändiga åtgärder för att skydda personuppgifterna. Underlåtenhet att fullgöra anvisningsskyldigheten strider mot dataskyddsförordningen även i det fall att ingen annan konkret dataskyddsförseelse skulle ha inträffat.

Med ansvarsskyldighet avses också *dokumenteringsskyldighet*, som i praktiken fullgörs genom att vissa åtgärder vidtas och dokumenteras. Ansvarsskyldighetens omfattning beror bland annat på organisationens storlek samt antalet personuppgifter och deras art. Anvisningsskyldigheten kan för sin del fullgöras till exempel med ett register över behandlingsåtgärderna, verksamhetsprinciperna för dataskyddet samt interna och externa anvisningar, informationspraxis, bedömningar av den rättsliga grunden för behandlingen, dokumentation av konsekvensbedömningar och förhandssamråd, dokumentation av informationssäkerhetsincidenter och den process som följer av dem, dokumentation i anslutning till dataskyddsombudets ställning och uppgifter, databehandlingsavtal, definition av gemensamt personuppgiftsansvarigas ansvarsområden samt dokumentation av utlämnande av personuppgifter till tredje länder.

Dataskyddsförordningen innehåller också bestämmelser om säkerheten vid behandling av personuppgifter. I artikel 25 i förordningen föreskrivs om *inbyggt dataskydd och dataskydd som standard* som syftar till att dataskyddet ska beaktas redan vid planeringen av informationssystem och behandling av personuppgifter och inte först när informationssystemet eller tjänsten är tekniskt färdig. Det är lättare att integrera dataskydds- och informationssäkerhetsåtgärderna i verksamheten i planeringsskedet än genom att i efterhand försöka anpassa det färdiga systemet eller verksamhetssättet i en mer informationssäker riktning.

Enligt bestämmelsen ska den personuppgiftsansvarige – med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter – både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder som dataskyddsprinciperna förutsätter. För att trygga principen om uppgiftsminimering föreskrivs uttryckligen att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Detta gäller både mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. I artikeln konstateras dessutom att den personuppgiftsansvarige i synnerhet ska säkerställa att personuppgifter i standardfallet inte görs tillgängliga för ett obegränsat antal fysiska personer.

Dataskydds- och informationssäkerhetsåtgärdernas tillräcklighet ska utvärderas kontinuerligt och de ska uppdateras till exempel när behandlingsåtgärderna förändras eller tekniken utvecklas. Den personuppgiftsansvarige ska också bedöma personuppgiftsbiträdenas åtgärder och sträva efter att säkerställa att deras åtgärder är lagenliga.

Med **informationssäkerhet** avses skydd av personuppgifter, tjänster, system och datakommunikation så att personuppgifterna endast är tillgängliga för dem som har rätt att använda dem, så att personuppgifterna inte kan ändras av andra än dem som har rätt att göra det och så att personuppgifterna och informationssystemen kan användas av dem som har rätt att använda dem. I artikel 32 i dataskyddsförordningen föreskrivs om *säkerhet i samband med behandlingen*. Enligt den ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Vid bedömningen av huruvida åtgärderna är lämpliga beaktas den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter

och friheter. Åtgärder som avses här kan till exempel vara pseudonymisering och kryptering av personuppgifter, förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna, förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident, ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

I praktiken kan åtgärderna till exempel genomföras genom att införa övervakning av åtkomsten till enheter och system, förhindrande av olovlig användning av personuppgifter och system, registrering av behandlingshändelser, övervakning av datatrafikens ursprung och routning, fastställande av systemens användarrättigheter, ändamålsenlig organisering av underhållsåtgärderna och skyddet av personuppgifter och system mot gärningar eller händelser som äventyrar informationssäkerheten, såsom hackning av personuppgifter, virus och andra skadliga program.

I bestämmelsen påminns dessutom om att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje person som utför arbete under deras överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att inte göra det. Detta förutsätter bland annat att personalen utbildas och ges anvisningar. Utfärdandet av anvisningar förutsätter å sin sida att den personuppgiftsansvarige vet vilka uppgifter som behandlas i dess verksamhet och varför samt att dataskydds- och informationssäkerhetsaspekterna har beaktats när behandlingen ordnades.

Bestämmelser om *konsekvensbedömning avseende dataskydd* finns i artikel 35 i dataskyddsförordningen. Enligt den ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter, om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Syftet med konsekvensbedömningen är att hjälpa till att identifiera, bedöma och hantera de risker som behandlingen av personuppgifter medför. Den hjälper dessutom den personuppgiftsansvarige att iaktta, dokumentera och påvisa kraven i dataskyddslagstiftningen. Bedömningen krävs särskilt bland annat i fall där en omfattande behandling gäller särskilda kategorier av personuppgifter som avses i artikel 9.1, till exempel uppgifter om religiös övertygelse och hälsotillstånd. Konsekvensbedömningen ska göras innan behandlingen inleds och vid behov ska den uppdateras

Dataombudsmannen har beskrivit hur risker uppkommer på följande figur (figur 14):

Figur 14. Uppkomsten av risker vid behandling av personuppgifter. (Bild: Dataombudsmannens byrå)[61]

I dataskyddsförordningen föreskrivs att den personuppgiftsansvarige ska *anmäla personuppgiftsincidenten* till tillsynsmyndigheten inom 72 timmar efter att ha fått vetskap om den och även underrätta de registrerade om det inträffade, om kränkningen sannolikt medför en stor risk för människors rättigheter och friheter. Syftet med anmälningarna är att utreda hur en personuppgiftsincident inträffar, men också att vidta försiktighetsåtgärder för att minska riskerna för missbruk av uppgifterna (artiklarna 33 och 34).

Bestämmelser om skyldigheten att utse ett *dataskyddsombud* finns i artikel 37 i dataskyddsförordningen. Enligt bestämmelsen ska Helsingfors stad utse ett dataskyddsombud.

Informationssäkerhetskrav enligt informationshanteringslagen

Informationshanteringslagen innehåller bestämmelser som gäller hela den offentliga förvaltningen om ordnande och beskrivning av informationshanteringen, informationslagrens interoperabilitet, genomförandet av informationssystemens interoperabilitet, genomförandet av tekniska gränssnitt och åtkomstförbindelser samt genomförandet av informationssäkerheten.

I 13 § i författningen ställs följande rättsliga krav på myndighetens informationssäkerhet:

- En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel. Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen.

[61] Dataombudsmannens byrå: Bedöm riskerna och planera åtgärderna för att genomföra dataskyddet. 26.2.2025 https://tietosuoja.fi/sv/bedom-riskerna

- De med tanke på skötseln av en myndighets uppgifter relevanta informationssystemens feltolerans och funktionella användbarhet ska regelbundet säkerställas genom tillräcklig testning.
- Myndigheten ska planera informationssystemen, informationslagrens strukturer och informationsbehandlingen i samband med dem på ett sådant sätt att handlingsoffentligheten utan svårighet kan genomföras.
- Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder.
- Angående bedömning av informationssäkerheten i myndigheters informationssystem och datakommunikation föreskrivs särskilt.

Kraven är principiella. De innehåller inga detaljerade bestämmelser om hur eller med vilka metoder informationssäkerheten ska tryggas.

Verktyget **Katakri 2020** för auditering av informationssäkerheten för myndigheter kan användas som hjälp vid bedömningen av organisationens förmåga att skydda myndighetens sekretessbelagda information. Den första Katakri, det vill säga de nationella kriterierna för säkerhetsauditering, färdigställdes redan 2009. Katakri är indelat i tre delområden:

- Inom delområdet för *säkerhetsledning* strävar man efter att säkerställa att organisationen har ett fungerande system för hantering av informationssäkerheten samt tillräckliga förfaranden för personalsäkerhet för att skydda säkerhetsklassificerade uppgifter.
- Inom delområdet för *fysisk säkerhet* beskrivs säkerhetskraven för den fysiska driftmiljön för säkerhetsklassificerade uppgifter.
- Inom delområdet för *teknisk informationssäkerhet* beskrivs de säkerhetskrav som ställs på den tekniska miljön för behandlingen av personuppgifter.
- **Cybermätaren**[62] är en mätare som utvecklats av Cybersäkerhetscentret och som grundar sig på internationella mätmodeller för cyberförmågor. Cybermätaren, som är skräddarsydd för företag och organisationer som är verksamma i Finland, hjälper företags, organisationers och även hela samhällets förmåga att avvärja cyberhot. Cybermätaren är ett konkret verktyg för företags- och organisationsledningen då verktyget hjälper dem att bättre kunna hantera cyberhot.

Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen[63] är informationshanteringsnämndens rekommendation om bedömningskriterier för informationssäkerheten inom den offentliga förvaltningen. Kriterierna för bedömning stödjer behoven av utveckling och bedömning av informationssäkerheten i hela den offentliga förvaltningen. De kan användas som hjälp vid bedömning av hur kraven på informationssäkerhet i informationshanteringslagen, säkerhetsklassificeringsförordningen och delvis i dataskyddsförordningen uppfylls. Dess del om dataskydd har utarbetats i samarbete med Dataombudsmannens byrå.

ISO/IEC 27001 är den mest erkända internationella standarden för hanteringssystem för informationssäkerhet. I den fastställs kraven på inrättande, genomförande, underhåll, uppföljning och förbättring av organisationens system för hantering av informationssäkerheten. Den hjälper organisationerna att utarbeta en policy för hantering av

[62] Cybermätaren https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/lagesbild-och-natverksledarskap/cybermataren

[63] Julkri; Finansministeriets publikationer 2023:46.

informationssäkerheten samt genomföra nödvändiga tillsynsåtgärder och ställa upp tydliga mål för att förbättra informationssäkerheten.

I 15 § i **informationshanteringslagen** föreskrivs om tryggande av säkerheten i fråga om informationsmaterial. Detta innebär att informationsmaterialens oföränderlighet har verifierats tillräckligt väl, informationsmaterialen har skyddats mot tekniska och fysiska skador, informationsmaterialens ursprung, uppdatering och felfrihet har verifierats, informationsmaterialens tillgänglighet och användbarhet har verifierats, informationsmaterialens tillgänglighet begränsas endast om tillgången till informationen eller rätten att behandla informationen har begränsats särskilt i lag, informationsmaterialen kan arkiveras till behövliga delar. Lagen förutsätter också att informationsmaterial behandlas och förvaras i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet.

Enligt 16 § i informationshanteringslagen förutsätts att den systemansvariga myndigheten ska definiera användarrättigheterna för informationssystem. Användarrättigheterna ska definieras och uppdateras utifrån användarens uppgiftsrelaterade användningsbehov.

Enligt 17 § i informationshanteringslagen ska en myndighet ombesörja att logginformation insamlas om användning av dess informationssystem och om utlämnande av information från dem, om användningen förutsätter identifiering eller annan registrering. Syftet med logginformationen är uppföljning av användningen och utlämnandet av information från informationssystem samt utredning av tekniska systemfel.

Informationshantering och informationens livscykel

Enligt 5 § i informationshanteringslagen ska informationshanteringsenheten upprätthålla en *informationshanteringsmodell* som definierar och beskriver informationshanteringen i dess verksamhetsmiljö. Informationshanteringsmodellen ska upprätthållas för planering och genomförande av tjänster, ärendebehandling och hantering av informationsmaterial, för genomförande av rättigheter och begränsningar i fråga om tillgången till information, för att minska överlappande insamling av information, för genomförande av interoperabilitet mellan informationssystem och informationslager samt för upprätthållande av informationssäkerhet.

Enligt 26 § i informationshanteringslagen ska informationshanteringsenheten förse de ärenden som myndigheten ska behandla eller som tilldelats myndigheten med en ärendekod som gör det möjligt att identifiera de uppgifter som rör ärendet. Bestämmelsen hänför sig uttryckligen till behandlingen av förvaltningsärenden, som i det fall som utreds är till exempel beslutsfattande som gäller personalen, antagning av elever, beslutsfattande som gäller stöd till elever och beslutsfattande som gäller betalningsskyldighet.

I 27 § i informationshanteringslagen föreskrivs om informationsmaterial som bildas i samband med tjänsteproduktion på annat sätt än i de egentliga processerna för handläggning av ärenden (tjänsternas informationshantering). Denna bestämmelse omfattar allt annat informationsmaterial som myndigheten utarbetat eller bildat och som inte behandlas i det logiska ärenderegistret. Det material som var föremål för dataintrånget har i huvudsak omfattats av denna bestämmelse.

En informationshanteringsenhet ska ordna hanteringen av informationsmaterial som uppkommer i andra sammanhang än ärendebehandling så att handlingar som har samband med informationsmaterialet kan sökas med hjälp av en kod som anger informationsmängden, så att informationen utan svårighet kan ges till behöriga personer. Myndigheten ska registrera handlingar och övrig information som uppkommer i samband med tjänsteproduktion så att det i efterhand är möjligt att konstatera att de uppkommit i samband med produktion av

tjänster. Innan informationshanteringslagen stiftades fanns det i Finland ingen motsvarande bestämmelse om informationshantering i samband med tjänster[64]. Informationshanteringsnämnden har gett en preciserande rekommendation om informationshanteringen i samband med tjänster och utvecklingen av den (se s. 60).

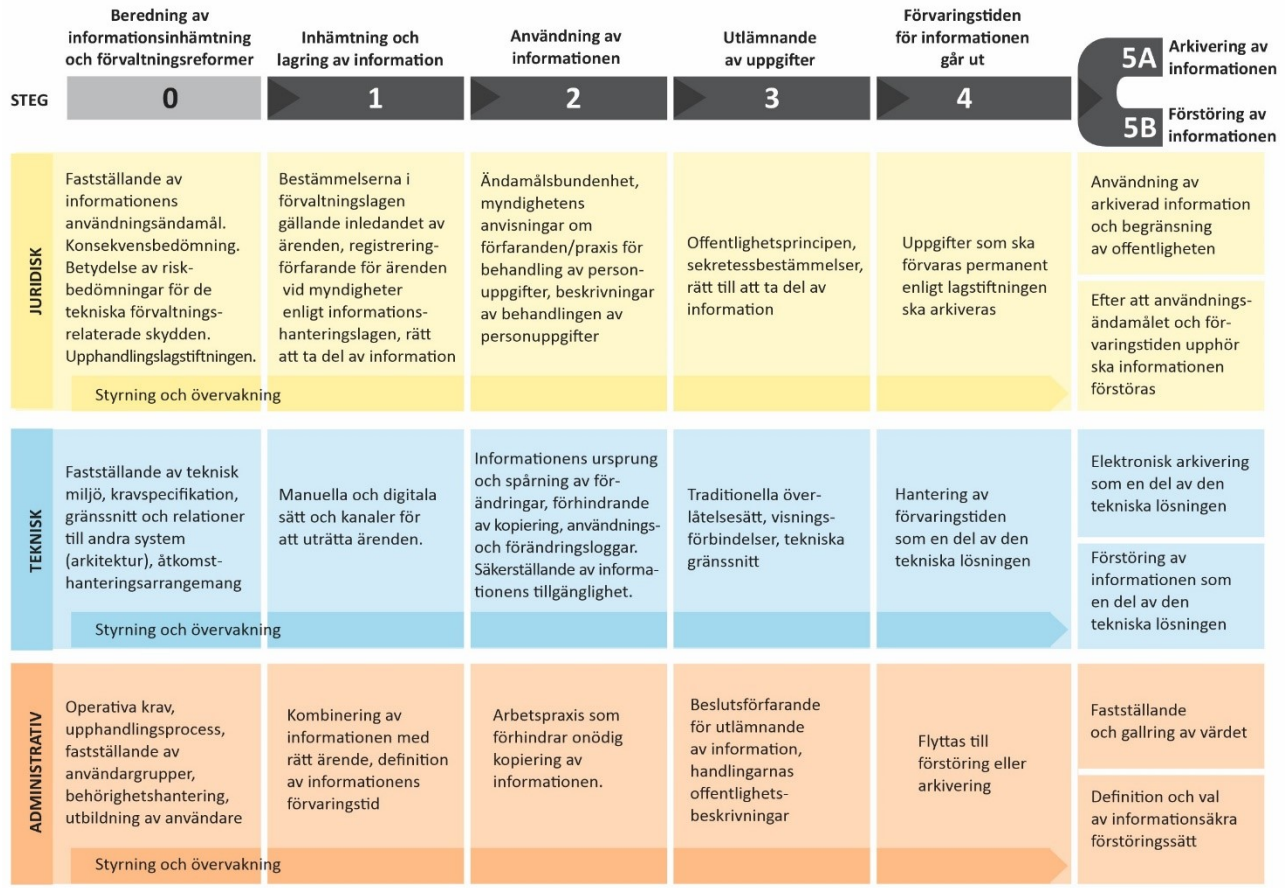
Enligt 21 § i informationshanteringslagen ska den registeransvarige bestämma en förvaringstid för varje informationsmaterial. Efter att förvaringstiden har gått ut ska uppgifterna förstöras. De uppgifter som enligt lag ska arkiveras eller som på andra grunder anses vara nödvändiga att förvaras arkiveras enligt arkivlagen.

Det finns inga uttryckliga bestämmelser om namnen på eller innehållet i utbildningens personregister, med undantag av elevhälsoregistret, som regleras i lagen om elev- och studerandevård[65]. Vid informationsbehandlingen inom utbildningen iakttas således i stor utsträckning den allmänna regleringen av informationshantering, dataskydd och offentlighet.

Enligt arkivlagen har arkivfunktionens till uppgift att säkerställa att handlingar hålls tillgängliga och bevaras, att sköta den informationstjänst som hänför sig till dem, att bestämma handlingars förvaringsvärde och att gallra ut onödigt material. För arkivbildningen upprätthålls en plan för informationsstyrning (s.k. TOS). Planen för informationsstyrning är en planeringshelhet som är kopplad till informationshanteringsmodellen.

Uppgifterna ska förstöras efter att den förvaringstid som fastställts för uppgifterna har löpt ut eller behovet av att använda uppgifterna annars har upphört. De allmänna anvisningarna om förvaringstiderna grundar sig bland annat på anvisningarna om förvaringstid.[66]

[64] RP 284/2018 rd. Regeringens proposition till Riksdagen med förslag till informationshanteringslag.
[65] 1287/2013.
[66] Kunnallisten asiakirjojen säilytysajat. Määräykset ja suositukset. Opetustoimi 12. 25.2.2025 https://www.kuntaliitto.fi/julkaisut/2002/1349-kunnallisten-asiakirjojen-sailytysajat-maaraykset-ja-suositukset-opetustoimi-12



Figur 15. Juridiska, administrativa och tekniska aspekter under informationens livscykel.

Uppgifternas offentlighet och sekretess

I **offentlighetslagen** föreskrivs om uppgifternas offentlighet och sekretess. Utgångspunkten för offentlighetslagen är uppgifternas offentlighet och myndighetens skyldighet att främja offentligheten. I 24 § i offentlighetslagen föreskrivs om de kategorier av uppgifter vars ärenden är sekretessbelagda och rätten att få dessa uppgifter är begränsad.

Enligt 24 § 1 mom. 30 punkten i offentlighetslagen är sekretessbelagda ärenden bland annat

- handlingar som gäller elevvård eller befriande av en elev från undervisning,
- elevers och examinanders provprestationer samt
- sådana av en läroanstalt utfärdade betyg och andra handlingar som innehåller uppgifter om verbala bedömningar av en elevs personliga egenskaper,
- liksom även handlingar av vilka det framgår hur de som av studentexamensnämnden har förordnats att bedöma provsvaren har fördelat sina uppgifter mellan olika skolor, tills ett år har förflutit från examensomgången.

Enligt 32 punkten i samma moment är också handlingar som innehåller uppgifter om en persons politiska övertygelse eller uppgifter om åsikter som personen har uttalat privat eller uppgifter om någons levnadssätt, deltagande i föreningsverksamhet eller fritidssysselsättningar, familjeliv eller andra med dem jämförbara personliga förhållanden sekretessbelagda.

Undervisningsväsendet har i speciallagstiftningen vissa bestämmelser om sekretessbelagda uppgifter om elev- och studerandevården samt om informationsutbytet mellan skolans personal.[67]

Ställningen hos offret för dataintrånget, skydd av uppgifter och ersättning för skador

Offret för dataintrånget har med stöd av artikel 82 i dataskyddsförordningen rätt att av *den personuppgiftsansvarige eller personuppgiftsbiträdet* få ersättning för skada som orsakats av brott mot dataskyddsförordningen. En förutsättning för ersättningsansvaret är att 1) skadan har orsakats antingen den registrerade eller någon annan person, 2) behandlingen av personuppgifter har stridit mot dataskyddsförordningen och 3) det finns ett orsakssamband mellan behandlingen av personuppgifter och skadan som strider mot dataskyddsförordningen. Grunden för skadeståndsansvaret bestäms enligt artikel 82 i dataskyddsförordningen, medan nationell lag tillämpas på bedömningen av ersättningsbeloppet; vanligen skadeståndslagen.[68] Det kan till exempel vara fråga om en situation där den personuppgiftsansvarige har skyddat registret så dåligt att det har varit möjligt att göra ett dataintrång.

Om det är fråga om en skada som orsakats av någon annan än den personuppgiftsansvarige eller personuppgiftsbiträdet, kan skadestånd yrkas med stöd av skadeståndslagen. En ren förmögenhetsskada, dvs. en ekonomisk skada som inte har samband med en person- eller sakskada, ersätts enligt 5 kap. 1 § i skadeståndslagen när skadan har orsakats genom en straffbar gärning eller vid myndighetsutövning eller om det i andra fall finns synnerligen vägande skäl. Lidande ersätts enligt 5 kap. 6 § i skadeståndslagen bland annat när det har orsakats genom en straffbar gärning som kränker friheten, friden, hedern eller privatlivet. Om ett dataintrång leder till en personskada ersätts den på grund av vållande enligt 5 kap. 2 § i skadeståndslagen.

Materiell skada som ersätts är till exempel inkomstbortfall som eventuellt orsakats av dataintrång och kostnader för anskaffning av kreditförbud. Immateriell skada är till exempel psykiskt lidande samt en akut stressreaktion som uppträder som en tillfällig olägenhet. Ett dataintrång kan i vissa fall också leda till en psykisk sjukdom som klassificeras som personskada, till exempel depression eller panikstörning. Då ersätts till exempel sjukvårdskostnader, inkomstbortfall samt lidande och/eller bestående eller tillfälligt men till följd av sjukdom.

Europeiska unionens domstol har ansett att även rädslan för eventuellt framtida missbruk av personuppgifter ska ersättas med stöd av artikel 82 i dataskyddsförordningen, förutsatt att rädslan inte är helt hypotetisk.[69] I *fallet VB mot Natsionalna agentsia za prihodite*[70] konstaterade Europeiska unionens domstolen att dataskyddsförordningen inte särskiljer situationerna i fråga om huruvida överträdelser av den orsakar lidande på grund av att personens personuppgifter har missbrukats redan vid tidpunkten för framställande av ersättningsanspråk eller på grund av att personen i fråga är rädd för framtida missbruk. Ordalydelsen i förordningen utesluter inte att uttrycket ”immateriell skada” utgörs av rädsla för att tredje parter missbrukar personuppgifterna till följd av överträdelser av förordningen. Den skadelidande ska dock visa att rädslan har gett upphov till negativa följder. Offret för dataintrånget kan orsakas betydande lidande på grund av att han eller hon är rädd för att uppgifterna senare kommer fram i något överraskande sammanhang, till och med offentligt, till exempel på en webbplats.

---

[67] Bestämmelserna är bland annat 40 § i lagen om grundläggande utbildning (628/1998), 32 § i gymnasielagen (629/1998), 109 § i lagen om yrkesutbildning (531/2017).
[68] 412/1974.
[69] Till exempel Österreichische Post, C-300/21 och GP mot juris GmbH, C-741/21.
[70] C-340/21.

Ett särdrag hos dataintrångsskador är att skadesituationen inte kan återställas med skadestånd så att den motsvarar situationen före skadan, eftersom det är möjligt att missbruka uppgifterna i ett senare skede.

Statskontoret kan med stöd av brottsskadelagen betala kostnader för personskador samt ersättning för sveda och värk och för tillfälliga och bestående men. Lidande ersätts med statliga medel endast i vissa allvarliga fall och därför kan ersättning för lidande inte beviljas på grund av dataintrång eller spridning av information som kränker privatlivet. Ersättning för lidande kan beviljas på basis av utpressning eller försök till utpressning. Allmänt taget är ersättningsskyddet i brottsskadelagen mer begränsat än ersättningsrätten enligt skadeståndslagen, men det ger offret ett visst minimiskydd som är till nytta om gärningsmannen är insolvent.

Utöver risken för rättegångskostnader i samband med straff- och ersättningsrättegångar ska man också beakta att rättegångar och material i anslutning till dem i princip är offentliga. Lagen om offentlighet vid rättegång i allmänna domstolar[71] gör det till exempel möjligt att hemlighålla målsägandens identitet i ett brottmål som gäller särskilt känsliga uppgifter om dennes privatliv samt att hemlighålla en handling som innehåller känsliga uppgifter om privatlivet eller hälsotillståndet. Trots detta kan det hända att uppgifter läcker ut eller att alla uppgifter som en part föreslår vara sekretessbelagda inte beläggsmed sekretess. Därför kan rädslan för ytterligare offentlighet i ärendet i vissa fall leda till att offret för dataintrånget inte vill yrka på straff eller skadestånd som han eller hon skulle ha rätt till.

Personbeteckning är ett sätt att identifiera en människa som är avsedd att vara bestående. Offren för dataintrång är ofta rädda för att deras personbeteckning används till exempel för identitetsstöld eller bedrägeri. Rädslan är förståelig även om personbeteckningen i sig inte ska användas som ett inloggningsverktyg utan endast som ett verktyg för identifiering av en person – att en personbeteckning uppges är ju ingen garanti för att det är fråga om den person som avses med personbeteckningen.

Enligt lagen om befolkningsdatasystemet och de certifikattjänster som tillhandahålls av Myndigheten för digitalisering och befolkningsdata[72] kan personbeteckningen ändras endast under strikta förutsättningar, som uppfylls om

- personens födelsedatum eller kön har antecknats fel i beteckningen
- en person fastställer sitt kön som ett annat
- någon annan upprepade gånger har missbrukat en persons personbeteckning och detta har orsakat stora ekonomiska eller andra olägenheter
- en människas hälsa eller säkerhet är utsatt för ett uppenbart och bestående hot.

Efter dataintrånget mot Vastaamo (2020) utreddes behovet av att ändra bestämmelserna om ändring av personbeteckningen, eftersom personbeteckningarna inte kunde ändras på förhand för att skydda individer efter kränkningarna av informationssäkerheten eller dataintrånget. I ärendet kom man dock fram till att det inte fanns skäl att lindra förutsättningarna för att ändra personbeteckningen. En ändring av personbeteckningen skulle orsaka många slags besvär och kostnader för människan på grund av behovet av att ändra och uppdatera handlingar, kunduppgifter och register.

---

[71] 370/2007.
[72] 661/2009.

Missbruk av personbeteckning som identifieringsverktyg kan förebyggas bland annat genom att öka olika aktörers medvetenhet om att personbeteckningen inte ensam ska användas som identifieringsverktyg samt genom att styra aktörerna till att använda stark autentisering, såsom mobilcertifikat eller bankkoder. I 29 § i dataskyddslagen föreskrivs följande om användning av personbeteckning vid identifiering: ”Enbart personbeteckningen eller en kombination av personbeteckningen och den registrerades namn får inte användas för utredning av den registrerades identitet med hjälp av uppgifter som den registrerade har uppgett eller lämnat eller med hjälp av handlingar som den registrerade har visat upp (*identifiering*)”.

Informationsskyldighet och myndighetens anmälningsskyldighet gentemot offren för dataintrånget

Enligt artikel 34 i dataskyddsförordningen är den personuppgiftsansvarige skyldig att underrätta den registrerade om dennes uppgifter har blivit föremål för en kränkning av informationssäkerheten – såsom ett dataintrång – om informationssäkerhetsincidenten sannolikt medför en hög risk för människors rättigheter och friheter. Informationen ska i första hand ges personligen och utan obefogat dröjsmål.

Informationen ska innehålla en tydlig och klar beskrivning av vilka uppgifter personuppgiftsincidenten gäller. Dessutom ska informationen omfatta uppgifter om den aktör som kan ge mer information samt beskriva eventuella konsekvenser av incidenten. Den personuppgiftsansvarige ska också presentera åtgärder genom vilka man har strävat efter att mildra eller ännu kan mildra konsekvenserna av personuppgiftsincidenten. Syftet med anmälningsskyldigheten är att säkerställa att de som utsatts för kränkningen får den information som behövs för att skydda sina personuppgifter och vidta lämpliga åtgärder.

I situationer där det skulle krävas oskäligt besvär att nå de registrerade kan informationen också genomföras som en allmän delgivning. Även då ska kommunikationen vara lika effektiv, heltäckande och tillgänglig som vid personlig delgivning.[73]

Myndighetens anmälningsskyldighet begränsas dock inte enbart till informationsskyldigheten enligt dataskyddsförordningen. Anmälningsskyldigheten måste förstås som en mer omfattande uppgift i anslutning till skyldigheten att trygga de grundläggande fri- och rättigheterna enligt 22.1 § i grundlagen. Uppgiften omfattar myndighetens förpliktelse att på eget initiativ informera om sådana ärenden som de behandlar och som har en vittsyftande inverkan eller annars är betydande.[74] Justitiekanslern vid statsrådet har utvärderat hur denna förpliktelse har fullgjorts bland annat i anslutning till förfarandet för införande av befogenheter under undantagsförhållanden under coronaviruspandemin. Justitiekanslern fäste uppmärksamhet vid att i synnerhet i exceptionella krissituationer är tydlig och informativ information av väsentlig betydelse och att myndigheten har en särskild skyldighet att sörja för medborgarnas tillgång till informationen.

Informationens betydelse framhävs av att myndigheternas meddelanden i en snabbt uppkommen situation kan vara medborgarnas enda informationskälla. Då är relevanta och juridiskt exakta uttryck som används i informationen av väsentlig betydelse.[75]

Bestämmelser om informationsskyldigheten finns i 20 § 2 mom. i offentlighetslagen[76], enligt vilken en myndighet skall informera om sin verksamhet och sina tjänster samt om de

[73] Dataskyddsförordningen artikel 34.1c.
[74] Regeringens proposition med förslag till Finlands grundlag 309/1993 rd, s. 62.
[75] OKV/740/70/2021 och OKV/61/10/2020.
[76] 621/1999.

rättigheter och skyldigheter som enskilda människor och sammanslutningar har i ärenden som anknyter till dess verksamhetsområde. Till informationsskyldigheten hör också kravet på gott språkbruk i 9 § i förvaltningslagen, enligt vilket myndigheten ska använda ett sakligt och begripligt språk. Vidare tryggas de språkliga rättigheterna i myndigheternas kommunikation i 23 § i språklagen[77].

Straffbestämmelser

I 38 kap. i **strafflagen** finns brottsrekvisit för bland annat systemstörning (7 a §) och grov systemstörning (7 b §), dataintrång (8 §) och grovt dataintrång (8 a §), avkodningssystemsbrott (8 b §) samt dataskyddsbrott (9 §). Åklagaren får inte väcka åtal för kränkning av kommunikationshemlighet, grov kränkning av kommunikationshemlighet, systemstörning, dataintrång eller avkodningssystemsbrott, om inte målsäganden anmäler brottet till åtal eller gärningsmannen när brottet begicks var anställd hos en inrättning som utövar allmän post- eller televerksamhet eller om inte ett synnerligen viktigt allmänt intresse kräver att åtal väcks (10 § 2 mom.). Åklagaren ska höra dataombudsmannen innan åtal väcks för dataintrång, grovt dataintrång eller dataskyddsbrott, om brottet i fråga riktar sig mot ett personregister. När domstolen behandlar ett mål som gäller ett sådant brott ska den ge dataombudsmannen tillfälle att bli hörd (30 § 3 mom.). Även juridiska personer kan ha straffansvar för dataintrång, grovt dataintrång, systemstörning och grov systemstörning.

I lagstiftningen föreskrivs inte om **samarbete mellan myndigheter** vid dataintrång eller cybersäkerhetshändelser på samma sätt som vid vanliga olycks- eller brottshändelser där det allmänna ledningsansvaret vanligtvis fördelas mellan räddnings- eller polismyndigheten. Myndighetsansvaret för cybersäkerhet och utredning av incidenter och hot mot informationssäkerheten har i Finland decentraliserats mellan olika myndigheter. Varje myndighet har en egen roll i utredningen av störningar i cybermiljön.

Statsrådet fattade den 10 juni 2021 ett principbeslut där det bestäms om åtgärder för att förbättra informationssäkerheten och dataskyddet inom kritiska samhällssektorer efter dataintrånget i Vastaamo. Intrånget mot Vastaamos patientdatasystem skedde åren 2018–2019 och intrånget blev allmänt känt den 21 oktober 2020, när gärningsmannen först började utpressa företaget och sedan dess klienter när utpressningen avföretaget misslyckades.

Vid dataintrånget stals person- och hälsouppgifter för uppskattningsvis 33 000 klienter vid psykoterapicentret. Principbeslutet grundar sig på en promemoria från en tväradministrativ arbetsgrupp som leddes av kommunikationsministeriet och beslutet fattades under statsminister Marins regeringsperiod.[78] I principbeslutet definieras 37 åtgärder på samhällsnivå för att förbättra dataskyddet och informationssäkerheten samt för att bekämpa och utreda dataintrång inom kritiska samhällssektorer. Ungefär en tredjedel av dessa åtgärder har bedömts omfatta lagstiftningsändringar.

Kommunikationsministeriet svarar för främjandet och uppföljningen av principbeslutet. I beslutet definieras inte tydligt vilka de kritiska samhällssektorerna är, men i punkten om verkställande åtgärder låter man förstå att det är fråga om de sektorer som definieras i NIS-direktivet. Undervisningsväsendet hör inte till dessa.

Centrala utvecklingsobjekt i principbeslutet är bland annat att förbättra samarbetet, informationsutbytet och handräckningen mellan myndigheterna, möjliggöra en tjänst för kartläggning av informationssäkerheten (Hyöky) och en tjänst för att upptäcka dataintrång (Havaro) för

[77] 423/2003.

[78] Statsrådets principbeslut om en förbättring av informationssäkerheten och dataskyddet inom kritiska samhällssektorer. 1.3.2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

alla kritiska sektorer, ge lagstadgade informationssäkerhetskrav för alla sektorer, skyldighet att regelbundet genomföra kvalitetsrevision av informationssäkerheten för kritiska funktioner samt inrätta en ärendehanterings- och kommunikationstjänst för kränkningar av informationssäkerheten.

I beredningsskedet av principbeslutet gav Helsingfors stadskansli den 7 april 2021 ett utlåtande där det konstateras att stora organisationer, såsom de största städerna, har möjlighet att skaffa tillräcklig expertis inom alla nödvändiga delområden inom digital säkerhet, såsom dataskydd och cybersäkerhet och att det är viktigt att Cybersäkerhetscentrets tjänst för kartläggning av informationssäkerheten utnyttjas i utredningen av informationssäkerhetens och dataskyddets nivå i Finlands 15 största kommuner.

Statsrådets principbeslut är till sin karaktär politiska riktlinjer som inte har någon direkt juridisk styrande effekt. Principbesluten beskriver dock sådant som har identifierats kräva åtgärder av statsrådet. Statsrådets principbeslut är regeringsspecifika. Vid regeringsskiftet har den nya regeringen fattat ett separat beslut om vilka principbeslut den förbinder sig till i sin verksamhet. Statsminister Oros regering fattade ett sådant beslut den 21 mars 2024.[79] Principbeslutet som syftar till att förbättra dataskyddet och informationssäkerheten har inkluderats som en del av styrningen och riktlinjerna för Orpos regerings verksamhet.

Samtidigt har man ansett att principbeslutens styrande effekt försvagas av det stora antalet beslut, det oenhetliga sättet att utarbeta dem samt deras eventuella lösryckthet från regeringsprogrammet.

Uppföljningen av principbeslutet har hört till kommunikationsministeriet, som utifrån de anmälningar som de ansvariga instanserna gjort har sammanställt sammandrag för den ministergrupp som följt ärendet.

Lagstiftningsåtgärderna i principbeslutet har framskridit långsamt eller regleringslösningarna har ändrats efter att principbeslutet utarbetades. Betydande ändringar i regleringen av sektorn har införts i cybersäkerhetslagen, som trädde i kraft den 8 april 2025. Regleringslösningarna och bestämmelsernas innehåll har delvis påverkats av till exempel det nationella genomförandet av nätverks- och informationssäkerhetsdirektivet NIS2, vilket är en del av verkställandet av cybersäkerhetslagen.

Förslaget i principbeslutet om att samarbetet mellan myndigheterna vid dataintrång ska effektiviseras enligt samma principer som vid andra allvarliga olyckor eller störningssituationer framgår åtminstone inte omedelbart av de pågående författningsprojekten. Regeringens proposition om utveckling av denna åtgärd förföll när riksdagen avslutade debatten den 4 april 2023.[80]

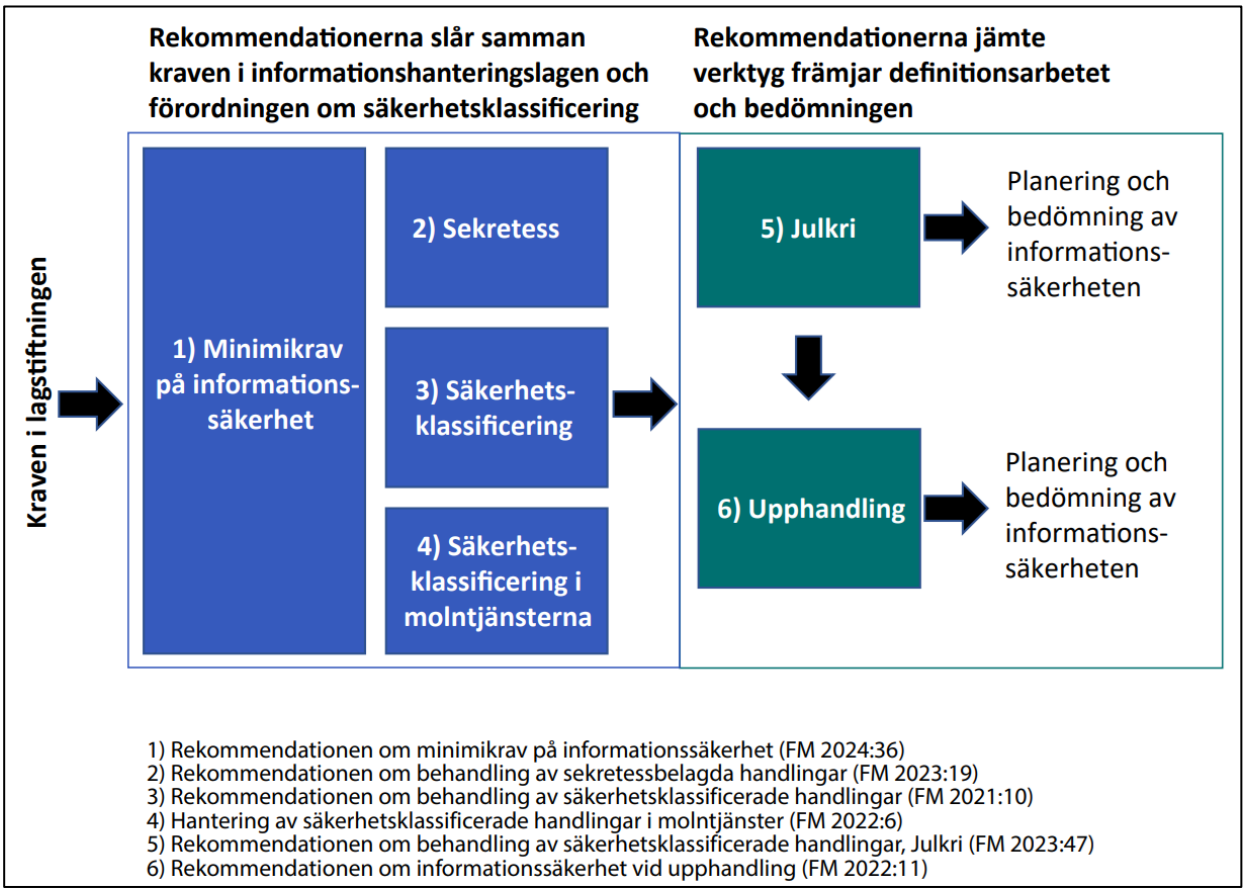
Informationshanteringsnämnden för den offentliga förvaltningen har gett sex rekommendationer för att förbättra informationssäkerheten inom den offentliga förvaltningen. Dessutom innehåller flera andra rekommendationer informationssäkerhetsaspekter. Rekommendationen om minimikrav på informationssäkerhet gavs den 11 mars 2024. Rekommendationen är omfattande och i den presenteras grunderna för minimiinnehållet i informationssäkerhetskravet enligt informationshanteringslagen för den offentliga förvaltningen. Rekommendationerna om informationssäkerhet och bästa praxis delas också av flera andra aktörer, vilket gör att man inte får en enhetlig bild av de rekommenderade lösningarna.

---

[79] SRK: Beslut om giltigheten av separata styrdokument som det beslutats om vid statsrådets allmänna sammanträde. 26.2.2025 https://valtioneuvosto.fi/paatokset/paatos?decisionId=1079

[80] RP 243/2022. 25.2.2025 https://www.eduskunta.fi/SV/vaski/KasittelytiedotValtiopaivaasia/Sidor/RP_243+2022.aspx

Rekommendationen och kriterierna som stöd för bedömningen av informationssäkerheten inom den offentliga förvaltningen gavs den 12 juni 2023. Rekommendationen är ett samordnat verktyg för informationssäkerhetsauditering för myndigheter (Katakri) och säkerhetskriterier för molntjänster (Pitukri).



Figur 16. Informationshanteringsnämndens rekommendationer om informationssäkerhet (FIGUR: Finansministeriet 2024)[81]

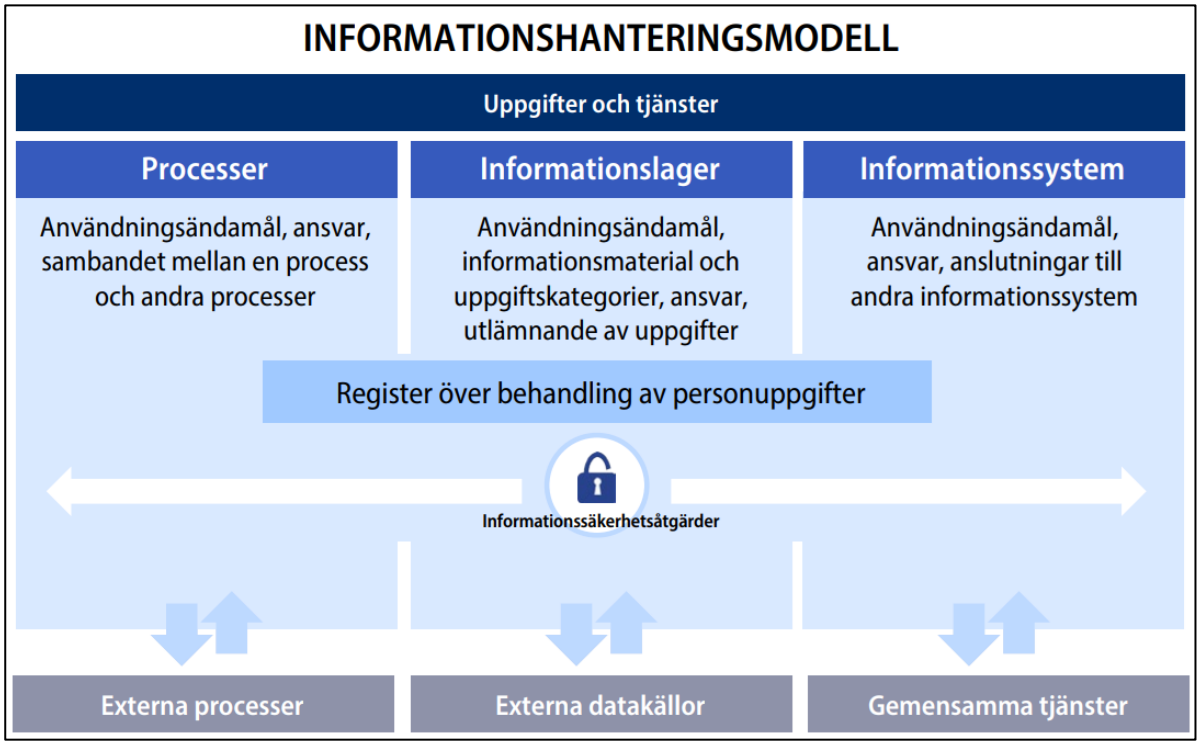
Informationshanteringsnämnden har publicerat en rekommendation om informationshanteringsmodellen. Syftet med rekommendationen är att förtydliga bestämmelserna i informationshanteringslagen om innehållet i informationshanteringsmodellen.

Enligt rekommendationen är informationshanteringsmodellen ett verktyg för informationshanteringsenheter för att förstå och hantera sin verksamhetsmiljö samt säkerställa att kraven på informationshantering uppfylls. De uppgifter som presenteras i informationshanteringsmodellen utgör grunden när en beskrivning i syfte att genomföra handlingsoffentligheten enligt 28 § i informationshanteringslagen produceras för informationshanteringsenhetens kunder.

Enligt rekommendationen kan informationshanteringsmodellen erbjuda grundläggande information om nuläget för organisationens informationshantering samt om de lösningar med vilka den genomför sin informationshantering. När informationshanteringsmodellen

81 Rekommendation om minimikrav på informationssäkerhet, sida 10. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165487/VM_2024_19.pdf

kombineras med eller länkas till informationshanteringsenhetens separata styrmetoder för informationshantering (till exempel arkivbildning, informationsstyrning, kvalitetshantering) kan modellen också utnyttjas i hanteringen av informationens livscykel. De förvaringstider för informationslager och informationsmaterial som avses i informationshanteringsmodellen samt information om arkivering och förstöring av uppgifter bildar en helhetsbild av livscykeln för den information som hanteras vid informationshanteringsenheten. På motsvarande sätt kan de verksamhetsprocesser som presenteras i informationshanteringsmodellen länkas till metadata som styr behandlingen av uppgifter i processens olika skeden.



Figur 17. Informationshanteringsmodellens innehåll.[82] (Figur: Finansministeriet 2024)

Informationshanteringsnämnden har publicerat en rekommendation om informationshantering i samband med produktionen av tjänster. Rekommendationen behandlar det myndighetsmaterial som inte ingår i den egentliga ärendehanteringen. Rekommendationen stöder fullgörandet av skyldigheten enligt 27 § i informationshanteringslagen. I rekommendationen beskrivs metoder för att genomföra åtgärder för specificering av uppgifter och livscykelhantering.[83]

Dataombudsmannens och andra laganvändares avgöranden publiceras i tjänsten Finlex. Avgörandena bildar ett fallmaterial vars rättsnormer kan användas för att avgöra dataskyddsfrågor.

Som en del av sitt uppdrag stöder dataombudsmannen fullgörandet av dataskyddsskyldigheten genom att publicera olika handböcker om centrala dataskyddsfrågor. Inom undervisning och utbildning har man bland annat utarbetat en guide om utbyte av information mellan

[82] Rekommendation för en informationshanteringsmodell, sida 10. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165497/VM_2024_22.pdf
[83] Rekommendation om metadata för myndigheternas handlingar i samband med tjänsteproduktion 16.3.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164194/VM_2022_42.pdf?sequence=1&isAllowed=y

hem och skola.[84] Många guider från dataombudsmannens byrå är utarbetade innan dataskyddsförordningen trädde i kraft och deras innehåll har inte uppdaterats i dataskyddsförordningen. Detta försämrar handböckernas användbarhet.

Största delen av utbildningsväsendets guider om dataskydd är Utbildningsstyrelsens publikationer. Guiderna har utarbetats i samarbete med dataombudsmannen.

Biträdande dataombudsmannen lade 2021 fram ett initiativ till Utbildningsstyrelsen om behandlingen av personuppgifter i applikationer som används vid anordnande av undervisning.[85] Det har dock inte färdigställts några riksomfattande anvisningar i ärendet.

Finlands cybersäkerhetsstrategi[86] för 2024–2035 publicerades i oktober 2024. Strategin har uppdaterats så att den motsvarar den förändrade verksamhetsmiljön och stärker cybersäkerhetens ställning som en del av den övergripande säkerheten. Strategin grundar sig på fyra centrala pelare:

1. Kompetens, teknologi och FUI: Målet är att stärka cybersäkerhetskompetensen på alla samhällsnivåer, främja ett innovativt cyberekosystem samt utnyttja ny teknik, såsom artificiell intelligens och kvantteknik.
2. Beredskap: Strategin betonar förebyggande verksamhet för att bekämpa cyberhot och reagera på dem, särskilt för att skydda kritisk infrastruktur och trygga samhällets funktionssäkerhet.
3. Samarbete: Här betonas betydelsen av nationellt och internationellt samarbete, inklusive nära samarbete med EU och Nato, samt partnerskap mellan den offentliga och privata sektorn för att bekämpa cyberhot.
4. Reaktion och motåtgärder: Strategin utvecklar beredskapen att reagera snabbt vid cyberattacker, inklusive att stärka cyberförsvarsförmågan och bekämpa cyberbrottslighet.

Målet med strategin är att Finland ska vara en föregångare inom cybersäkerhet före 2035, där den digitala miljön är säker och tillförlitlig för alla användare. Strategin uppdateras vart femte år. Genomförandeplanen följs upp och utvärderas regelbundet.

Genomförandeplanen för cybersäkerhetsstrategin publicerades den 4 december 2024.[87] Den består av 44 utvecklingsåtgärder som utarbetats under strategins fyra grundpelare. För varje åtgärd har uppställts ett mål, en tidtabell och finansiering, en konsekvensbedömning och en konsekvensanalys samt motsvarande organisation(er) och aktör(er).

Myndigheten för digitalisering och befolkningsdata (MDB) har enligt lagen i uppgift att för informationshanteringsnämnden producera sakkunnigtjänster[88] i syfte att utveckla förfarandena för informationshantering och informationssäkerhet. En central uppgift är att delta i arbetet av nämndens sektioner och i beredningen av rekommendationer samt stödja

---

[84] Dataombudsmannens byrå: Oppilaiden henkilötietojen käsittely kodin ja koulun yhteistyössä. 26.2.2025 https://tietosuoja.fi/documents/6927448/10594424/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4/5169bbf4-c5de-d073-c247-a10a462ca5fb/Oppilaan+henkil%C3%B6tietojen+k%C3%A4sittely+kodin+ja+koulun+v%C3%A4lisess%C3%A4+yhteisty%C3%B6ss%C3%A4.pdf

[85] Dataombudsmannens byrå: Biträdande dataombudsmannen har lagt fram ett initiativ till Utbildningsstyrelsen om behandlingen av personuppgifter i applikationer som används vid anordnande av undervisning. 26.2.2025 https://tietosuoja.fi/-/apulaistietosuojavaltuutettu-on-tehnyt-opetushallitukselle-aloitteen-opetuksessa-kaytettavien-sovellusten-henkilotietojen-kasittelysta?languageId=sv_SE

[86] Strategi för cybersäkerheten i Finland 2024–2035. 26.2.2025 https://julkaisut.valtioneuvosto.fi/handle/10024/165861

[87] Genomförandeplan för Finlands cybersäkerhetsstrategi (på finska). 28.2.2025 https://api.hankeikkuna.fi/asiakirjat/b9b35c4c-2719-4cfb-89fa-4388c855e2f0/c4785613-4037-43b5-b1cc-22d9b82c0d69/KIRJE_20241204070347.PDF

[88] Sakkunnigtjänster för informationshanteringsnämnden. 2.3.2025 https://dvv.fi/sv/sakkunnigtjanster-for-informationshanteringsnamnden

genomförandet av nämndens uppgifter till exempel med att delta i organiseringen av olika evenemang.

Dessutom ansvarar myndigheten för verksamheten i ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI)[89] och de arbetsgrupper som den tillsatt för att utveckla riskhanteringen, verksamhetens kontinuitet, beredskapen, cyber- och informationssäkerheten samt dataskyddet.

VAHTI-ledningsgrupperna och VAHTI-arbetsgrupperna har som mål att stöda och koordinera utvecklingen av den digitala säkerheten inom den offentliga förvaltningen samt samarbetet. De strävar efter att stärka den digitala säkerhetens observationsförmåga och förmågor, svara på olika hot och dela en aktuell lägesbild i samarbete med andra myndigheter. Dessutom främjar de säkert införande av ny teknik inom den offentliga förvaltningen samt stöder en kostnadseffektiv utveckling inom cyber- och digital säkerhet.

VAHTI-lednings- och arbetsgruppernas centrala uppgifter är:

- Bygga upp och stärka samarbetsnätverk för att utveckla den offentliga förvaltningens serviceproduktion och säkerhet inom den digitala säkerhetens olika delområden.
- Följa utvecklingen av cyberhot och digital säkerhet samt främja spridningen av aktuell hotinformation till aktörer inom den offentliga förvaltningen i samarbete med andra myndigheter.
- Publicera god praxis, stödmaterial och annat material och ordna seminarier och evenemang för att främja den digitala säkerheten inom den offentliga förvaltningen.
- Stöda utvecklingen av kompetensen, medvetenheten, attityderna och kulturen kring digital säkerhet i organisationer inom den offentliga förvaltningen.
- Producera en aktuell helhetsbild och utredningar av den offentliga förvaltningens cybersäkerhet och digitala säkerhet och dess utvecklingsbehov.

Under 2019–2023 genomförde Myndigheten för digitalisering och befolkningsdata ett JUDO-projekt som finansierades av finansministeriet och där man utvecklade olika tjänster för digital säkerhet. Med hjälp av tjänsten för helhetsbild av den digitala säkerheten[90] inom den offentliga förvaltningen kan organisationerna jämföra nivån på sin egen administrativa digitala säkerhet med andra aktörer. Dessutom erbjuder utbildningarna Digital säkerhet i livet och spelet[91] med samma namn avgiftsfria utbildningar för personal och sakkunniga. Applikationen är tillgänglig för iOS- och Android-enheter.

Taisto-övningar om digital säkerhet har ordnats årligen sedan 2018.[92] Under sju år har över 2 200 övningsteam deltagit i dessa antingen halv- eller heldagsövningar, varav största delen har varit organisationer inom den offentliga förvaltningen samt över 14 000 representanter för ledningen eller sakkunniga.

[89] Myndigheten för digitalisering och befolkningsdata, VAHTI. 26.2.2025 https://dvv.fi/sv/vahti-natverket

[90] Tjänsten för helhetsbild av den digitala säkerheten. 26.2.2025 https://www.suomi.fi/service/tjansten-for-helhetsbild-av-den-digitala-sakerheten-myndigheten-for-digitalisering-och-befolkningsdata/1b38df61-ca48-41b4-a238-da5ab1baaf27

[91] Utbildningshelheten Digital säkerhet i livet. 26.2.2025 https://dvv.fi/sv/digital-sakerhet-i-livet

[92] Taisto-övningen är en möjlighet att testa och utveckla er organisations digitala säkerhet. 26.2.2025 https://dvv.fi/sv/taisto-ovningar

Under 2024 inledde Myndigheten för digitalisering och befolkningsdata webbtjänsten Databanken för digital säkerhet[93] som en del av den nya plattformen Suomi.fi för tjänsteutvecklare. I databanken finns centralt material om digital säkerhet, såsom lagstiftningsskyldigheter och andra skyldigheter samt tillgängligt offentligt stödmaterial. Som en del av denna helhet har det också publicerats en handbok för hantering av digitala risker.[94]

Anvisningar för personer som fallit offer för dataintrång samt andra stödtjänster

Dataintrånget mot Vastaamo visade hur viktig roll olika anvisningar samt andra stödtjänster är för personer som utsatts för dataintrång, deras närstående och organisationen. Under de senaste fem åren efter händelsen har situationen förbättrats betydligt och anvisningarna har förenhetligats. Allt fler organisationer erbjuder numera avgiftsfria stödtjänster. Dessutom erbjuder kommersiella aktörer avgiftsbelagda informationssäkerhetstjänster för medborgare som använder internetuppkoppling och smarta enheter.

Myndigheten för digitalisering och befolkningsdata har utarbetat guider för personer som fallit offer för dataintrång. Guiden *”Mina personuppgifter har stulits eller läckt ut”*[95] på webbplatsen Suomi.fi ger anvisningar och råd till personer vars personuppgifter har hamnat i fel händer till följd av dataintrång, informationsläckage eller identitetsstöld. Den hjälper till att identifiera tecken på missbruk, förhindra skadlig användning av uppgifter, införa nödvändiga förbud och åtgärda följderna av situationen. I maj 2024 hade guiden sammanlagt 138 000 besökare, i juni 25 000 och i slutet av 2024 sammanlagt 67 000 besökare. Guiden har uppdaterats på basis av personuppgiftsincidenter 2024 och i fråga om nya skyddsmetoder.

Suomi.fi-webbplatsens guide *”Information har stulits eller läckt ut från min organisation”*[96] ger anvisningar till organisationer vid dataintrång eller informationsläckage. Den ger råd om hur man ska agera i en akut situation, hur man förhindrar ytterligare skador och uppmanar att anmäla till myndigheterna. Dessutom behandlar guiden åtgärder i efterhand, såsom förbättring av informationssäkerheten och uppdatering av processerna. Webbplatsen har haft cirka 7 500 besökare under 2024.

Suomi.fi-webbplatsens guide *”Beredskap för störnings- och krissituationer”*[97] ger information och anvisningar om hur man förbereder sig för olika störningar och kriser, såsom elavbrott, stormar och storolyckor. Webbplatsen har haft 950 000 besökare i november–december.

Cybersäkerhetscentret har samlat anvisningar och guider för privatpersoner och arbetsplatser om informationssäkerhetskompetens[98] samt praktiska råd för personer som fallit offer för identitetsstöld.[99] På webbplatsen förklaras vad identitetsstöld är och hur brottslingar kan missbruka personuppgifter. Webbplatsen ger råd om hur man kan skydda sig mot ekonomiska skador, göra en brottsanmälan, införa ett frivilligt kreditförbud och skydda kontonumret. Dessutom ger den anvisningar om hur man kan förhindra missbruk av uppgifter och var man kan få hjälp i en krissituation.

---

[93] Suomi.fi för tjänsteutvecklare: Databanken för digital säkerhet. 26.2.2025 https://kehittajille.suomi.fi/tjanster/digital-sakerhet

[94] Suomi.fi för tjänsteutvecklare: Databanken för digital säkerhet. 27.2.2025 https://kehittajille.suomi.fi/guider/riskhantering

[95] Suomi.fi: Mina personuppgifter har stulits eller läckt ut. 26.2.2025 https://www.suomi.fi/guider/informationslacka

[96] Suomi.fi: Information har stulits eller läckt ut från min organisation. 26.2.2025 https://www.suomi.fi/guider/dataintrang

[97] Suomi.fi: Beredskap för störnings- och krissituationer. 26.2.2025 https://www.suomi.fi/guider/beredskap

[98] Cybersäkerhetscentret: Anvisningar och guider för privatpersoner. 26.2.2025 https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/anvisningar-och-guider-privatpersoner

[99] Cybersäkerhetscentret: Råd för dem som drabbats av identitetsstöld eller dataläckage 26.2.2025 https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/rad-dem-som-drabbats-av-identitetsstold-eller-datalackage

Efter dataintrånget mot Helsingfors stad publicerade **Konsumentförbundet** artikeln ”Ohjeita tietomurron kohteeksi joutuneille” på sin webbplats.[100] Artikeln behandlar läckta uppgifter såsom person- och adressuppgifter, användarnamn och e-postadresser samt ger råd, såsom att kontrollera sin egen e-post och banktrafik för ovanliga händelser. Dessutom rekommenderas att man byter lösenord och använder starka, individuella lösenord i olika tjänster. Artikeln ger också anvisningar om hur man ska gå till väga om uppgifterna missbrukas.

Brottsofferjouren (RIKU) har på sin webbplats publicerat råd för personer som fallit offer för dataintrång eller dataläckage.[101] På webbplatsen betonas att det är viktigt att följa myndigheternas instruktioner om det som skett och vidta nödvändiga spärråtgärder för att personuppgifterna inte ska användas för bedrägerier. RIKU erbjuder också samtalshjälp. Tjänsterna är avgiftsfria.

Mieli rf[102] erbjuder medborgarna flera tjänster särskilt för att stödja den psykiska hälsan. Om man faller offer för ett dataintrång är det möjligt att använda bland annat kristelefonens tjänster eller det stöd som kriscentren erbjuder.

Sekasin-chatt[103] är en riksomfattande stödtjänst riktad till 12–29-åringar, där man kan tala om vad som helst man grubblar på anonymt och i förtroende. Sekasin Kollektiivi är en sammanslutning som koordineras av MIELI Psykisk Hälsa Finland rf, Finlands Röda Kors, Setlementförbundet och SOS Barnbyn och som arbetar för att främja de ungas psykiska välbefinnande och hjälpa till i kriser.

KyberVPK[104] är ett finländskt hackerkollektiv som grundades för att hjälpa producenter av kritiska funktioner i kampen mot attacker och återhämta sig från dem. Enligt behoven hos den organisation som ber om hjälp kan kollektivet hjälpa till att förebygga informationssäkerhetsproblem, testa miljöns säkerhet, lösa informationssäkerhetsincidenter tillsammans eller till exempel hjälpa till att ta i bruk systemen på ett säkert sätt. Detta frivilligarbete och den avgiftsfria verksamheten har anlitats inom bland annat social- och hälsovården, kommuner, läroanstalter och andra organisationer eller företag som producerar kritiska tjänster och funktioner.

2.10 Övriga utredningar

Elisa Santa Monicas utredningsrapport om dataintrånget: Helsingfors stad ingick den 2 maj 2024 ett avtal med Elisa Santa Monica om utredningshjälp gällande dataintrånget. Som en del av uppdraget kartlades angriparens agerande i intranätet och Helsingfors stad stöddes i bekämpningen av angreppet. Uppdraget utvidgades den 7 maj 2024 till att omfatta hela utredningen av personuppgiftsincidenten samt kontinuerligt stöd för fostrans- och utbildningssektorns informationssäkerhetstillsyn. Företaget producerade den 7 oktober 2024 en omfattande utredningsrapport med bilagor, där man också har utnyttjat den forensik som utomstående informationssäkerhetsföretag riktat mot nätverksenheter samt loggrapporter för brandväggar och servrar.

---

[100] Konsumentförbundet: Ohjeita tietomurron kohteeksi joutuneille. 26.2.2025 https://www.kuluttajaliitto.fi/materiaalit/ohjeita-tietomurron-kohteeksi-joutuneille/

[101] Brottsofferjouren: Dataintrång – råd till offer för dataintrång eller dataläckage. 26.2.2025 https://www.riku.fi/sv/gor-sa-har-om-dina-uppgifter-har-lackt-ut-pa-natet-dataintranget-mot-psykoterapicentret-vastaamo/

[102] Mieli rf. 26.2.2025 https://mieli.fi/sv/

[103] Sekasin-chatt. 26.2.2025 https://sekasin.fi/se/

[104] KyberVPK. 26.2.2025 https://kybervpk.fi/sv/

Den allmänna kommentaren[105] från **FN:s kommitté för barnets rättigheter** behandlar inte direkt dataskydd eller informationssäkerhet, men den allmänna andan och målen i konventionen betonar barnets rätt till integritet och säkerhet, vilket också omfattar dataskydd och informationssäkerhet.

Dataombudsmannens byrå[106] har sammanställt information om barnens dataskyddsrättigheter. Dataombudsmannen betonar att varje barn och ung person har rätt till dataskydd. Personuppgifter är till exempel namn, adress, födelsedatum, telefonnummer, fotografier och videor samt uppgifter om läkarbesök. Barnen har också rätt att veta var och varför deras uppgifter behandlas samt rätt att radera eller ändra sina uppgifter. Dataombudsmannens byrå säkerställer att barnets bästa beaktas vid behandlingen av personuppgifter.

Den **nationella barnstrategin**[107] lyfter fram barnets skydd och rätt till integritet i digitala tjänster. Detta perspektiv är en del av det bredare målet att skapa ett barn- och familjevänligt samhälle där barnens rättigheter tillgodoses inom alla livsområden.

Centralförbundet för Barnskydd har publicerat webbpublikationen ”Barnet på nätet – Synvinklar på barnets rättigheter och dataskyddet i en digital miljö”[108], som behandlar barns rättigheter och dataskydd på internet. Det centrala budskapet är att barnens särskilda behov och rättigheter ska beaktas vid behandlingen av personuppgifter. Barn har samma dataskyddsrättigheter som vuxna, men de behöver särskilt skydd, såsom vårdnadshavarens samtycke för barn under 16 år. Den nämnda åldersgränsen är den åldersgräns som avses i artikel 8 i EU:s dataskyddsförordning som en medlemsstat kan avvika från i sin lagstiftning, dock så att åldersgränsen är minst 13 år. Finland har utnyttjat prövningsmarginalen. Enligt 5 § i dataskyddslagen (1050/2018) är åldersgränsen för tillhandahållande av informationssamhällets tjänster till barn (minst) 13 år. Dessutom betonas att barnen ska erbjudas tydlig och begriplig information om behandlingen av deras personuppgifter.

Helsingfors stads interna kontroll genomförde en utredning av dataintrånget på uppdrag av kanslichefen. Utredningen blev klar den 15 augusti 2024 och kompletterades med en tilläggsutredning 25 november 2024. I sammandraget konstateras bland annat att efter att funktionerna ändrades förblev VPN-routern kvar under fostrans- och utbildningssektorns ansvar och att underhållet av den försummades. Systematisk konfigurationshantering tillämpades inte och VPN-enheten ersattes inte tillräckligt snabbt med en alternativ tjänst. Man hade inte inlett något projekt för att övergå till centraliserade datorsalar vid fostrans- och utbildningssektorn och förändringen genomfördes främst som expertarbete i samband med andra arbetsuppgifter. Förändringen ansågs inte vara brådskande och det fanns ingen aktiv uppföljning av brandväggens larm. Reaktionen på dataintrånget skedde med fördröjning. Larm om avvikande observationer kom redan cirka fem dagar innan dataintrånget upptäcktes och man reagerade på det.

Antalet andra attacker i anslutning till dataintrång i den digitala världen har enligt Cybersäkerhetscentrets årsrapport antingen ökat något (försök till dataintrång, dataläckage)

[105] United Nations (2001) Convention on the Rights of the Child. 26.2.2025 https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/CRC_General_Comment_1_en.pdf
[106] Dataombudsmannens byrå. Barnets dataskyddsrättigheter 28.1.2025 https://tietosuoja.fi/sv/barns-dataskydd
[107] Barnstrategin. 26.2.2025 https:// lapsistrategia.fi/
[108] Centralförbundet för Barnskydd (2019): Barnet på nätet – Synvinklar på barnets rättigheter och dataskyddet i en digital miljö. 26.2.2025 https://www.lskl.fi/wp-content/uploads/Lapsi-verkossa.pdf

eller minskat något (dataintrång)[109]. Enligt statistik från Finanssiala ry[110] har bedrägerierna som kommit till bankernas kännedom fortsatt att öka under hela 2020-talet.

Dataintrånget mot Helsingfors stad är hittills det mest betydande i finländska förhållanden, eftersom det omfattade cirka 300 000 personer. Dataintrånget gällde såväl grundläggande personuppgifter som vissa personers personbeteckning och andra känsliga uppgifter.

Nätbrottsligheten har under det senaste decenniet blivit en alltmer professionell och global affärsverksamhet. Nätbrottslingar har grundat tjänster av typen CaaS (Crime-as-a-Service) som erbjuder alla nödvändiga verktyg och andra tjänster med nyckel i handen-principen och med 24/7-kundstöd. Angriparen kan be en lämplig kriminell aktör att kartlägga potentiella objekt, därefter söka den sårbarhet som behövs och skapa nödvändigt fotfäste, varefter angriparen kan inleda önskad attack, till exempel utpressning med den information som stulits.

I Microsofts årliga rapport Digital Defense 2024[111] konstateras att nätbrottsligheten enligt World Economic Forum orsakade skador på över 1 000 miljarder dollar 2023. Konsumenternas förluster uppgick till 8,8 miljarder dollar, vilket var en ökning med 30 procent jämfört med 2022.

Dataintrång eller överbelastningsattacker mot den offentliga förvaltningen 2018–2024 har sammanställts i följande tabell (tabell 2):

Tabell 2: Dataintrång i den offentliga förvaltningen och andra betydande aktörer 2018–2024.

Organisation	Tidpunkt	Fall
Lahtis stad	2/2018	Brytningsprogrammet Cryptominer i Provincias nätverk.
Lahtis stad	6/2019	Skadeprogrammet spred sig till tusen arbetsstationer, utrednings- och rensningskostnaderna uppgick till en miljon euro.
Kumo stad	8/2019	Utpressningsprogrammet låste filerna. Återhämtningen tog ett par veckor.
Björneborgs stad	8/2019	Utpressningsprogrammet observerades i tid (undervisningsnätverket).
Sjundeå kommun	9/2019	Dataintrång och nätfiskemeddelanden i kommunens namn till följd av det.
Åbo stad	4/2021	Dataintrång i utbildningsväsendets nätverk. Utpressningsprogrammet observerades i tid.
Savonia yrkeshögskola	2/2022	I dataintrånget stals studerandenas personuppgifter och de publicerades på det mörka nätet.

[109] Kyberturvallisuus Suomessa 17.3.2025 https://kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuus-Suomessa.pdf

[110] Huijaukset rajussa kasvussa vuonna 2024 – pankit saivat pysäytettyä huijattuja maksuja yli 44 miljoonan euron arvosta. 28.2.2025 https://www.finanssiala.fi/uutiset/huijaukset-rajussa-kasvussa-vuonna-2024-pankit-saivat-pysaytettya-huijattuja-maksuja-yli-44-miljoonan-euron-arvosta/

[111] Microsoft Digital Defense Report 2024 28.2.2025 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Mellersta Nylands utbildningssamkommun	11/2022	Utpressningsgruppen Lockbit stoppade Mellersta Nylands utbildningssamkommuns IT-miljö för nästan en månad. Kostnader 100 000 euro. Ett penningkrav har aldrig framställts och uppgifterna har inte läckt ut.
Säkylä stad	12/2022	En extern tjänsteproducents fel lämnade ett hål i nätet. Fallet har inte beskrivits närmare i offentligheten.
Helsingforsregionens trafik	12/2022	Ett betydande antal överbelastningsattacker, bakom flera stod en prorysk aktivistgrupp som heter NoName. Samma grupp påstod sig ha angripit även andra organisationer inom den offentliga förvaltningen under 2022–2024.
Rautavaara kommun	10/2023	Utpressningsprogram i förvaltningsnätverket, angriparen hann kryptera en del av filerna.
Tietoevry Oyj	1/2024	Akira slog till mot Tietoevrys datacentral i Sverige och förstörde även säkerhetskopiorna. Fallet orsakade stora skador för webbutiker och många svenska kommuner.
Helsingfors stad	4/2024	Dataintrång mot fostrans- och utbildningssektorns nätverk vid Helsingfors stad, varvid den okända angriparen kunde kopiera uppskattningsvis 750 000 dokument.
Transport- och kommunikationsverket Traficom	5/2024	Missbruk genom vilket en utomstående aktör kunde ladda ner uppgifter om 65 000 fordonsägare eller -innehavare. Samma metod användes också mot Skatteförvaltningens positiva kreditupplysningsregister. I detta fall gjordes ett dataintrång mot kreditgivarens programvara, vilket ledde till att det ställdes obehöriga förfrågningar om utdrag ur det positiva kreditupplysningsregistret.
Nordea	9/2024	Flera mycket allvarliga överbelastningsattacker (DDoS) mot banken Nordea, som avsevärt störde nätbankens funktion och bankens identifieringstjänst.
Vincit Oyj	12/2024	Ett dataintrång som gjorts via hemdatorn för en anställd vid IT-bolaget Vincit och som gav angriparen tillgång till tio kundföretags informationssystem. Angriparen stal ett stort antal personuppgifter från Valio.

En **utredning av nivån på informationssäkerheten och dataskyddet i de 15 största kommunerna** genomfördes efter dataintrånget mot Vastaamo i fråga om statsförvaltningens nationella behov av att utveckla informationssäkerheten och dataskyddet. Utredningen var en del av statsrådets principbeslut om att förbättra informationssäkerheten och dataskyddet inom kritiska samhällssektorer (nedan Titukri)[112]. Titukri upphörde att gälla genom statsrådets beslut den 10 oktober 2024.

Som en åtgärd i principbeslutet (åtgärd 29) ville man skapa en mer heltäckande situationsförståelse av nivån på informationssäkerheten och dataskyddet hos de 15 till invånarmängden största kommunerna i Finland samt de aktörer som svarade för den kritiska infrastrukturen i deras område. I fråga om kritisk infrastruktur var aktörer inom social- och hälsovården samt energi- och vattentjänsterna av intresse. Antalet organisationer som identifierats enligt de angivna kriterierna var 66, varav 41 deltog i utredningen.

[112] LVM/2021/44.

Finansministeriet och Cybersäkerhetscentret ansvarade för genomförandet av utredningen. Finansministeriet ansvarade för den övergripande styrningen av utredningsprojektet.

Cybersäkerhetscentret ansvarade för insamlingen av energibolagens och vattenverkens material och kommunernas kartläggning av angreppsytan samt deltog i styrningen av utredningsarbetet samt i planeringen, kommenteringen och skrivandet av rapporten. Myndigheten för digitalisering och befolkningsdata stödde finansministeriet genom att ansvara för insamlingen av kommunernas och välfärdsområdenas material samt deltog i planeringen och skrivandet av rapporten. Två konsultbolag stödde de instanser som ansvarade för utredningen – en i insamlingen av material och en i utarbetandet av rapporten.

Utredningen är säkerhetsklassificerad och avsedd för utveckling av verksamheten hos de ansvariga myndigheterna och i de organisationer som varit föremål för utredningen. I utredningsbeskrivningen lyfts dock fram utvecklingsförslag som på en allmän nivå beskriver fenomenet utan att avslöja sådant som omfattas av sekretessen.

I utredningens centrala resultat konstateras bland annat på kommunal nivå:

- Kommunerna ska stödjas i identifieringen av central egendom som ska skyddas.
- Riskhanteringen i leveranskedjorna är bristfällig, vilket bland annat avser beredskapen för bolagiserade eller utkontrakterade tjänster.

På riksnivå:

- Man bör fästa uppmärksamhet vid att befintliga metoder och utredningar används på bred front i utvecklingen av verksamheten (cybermognadsutredningar, enkät om digital säkerhet).
- De tjänster som används kan utvidgas så att kommunerna kan använda dem bättre än tidigare (särskilt Hyöky-tjänsten).
- Verktyg och metoder som förebygger, utvecklar och mäter verksamheten bör användas och utvecklas i ett mer omfattande myndighetssamarbete.
- Skyldigheten att använda tjänster genom nationell lagstiftning bör bedömas.

Undervisningsväsendet var inte föremål för utredningen, eftersom det inte betraktas som en kritisk samhällssektor vid verkställandet av ovan nämnda principbeslut. I beredningsskedet av principbeslutet konstateras i Utbildningsstyrelsens utlåtande (3.3.2021) att Utbildningsstyrelsen i beslutsutkastet utöver de sektorer som föreslås bli föremål för utredningen även föreslår att nivån på informationssäkerheten och dataskyddet i de 15 största kommunerna i Finland utreds inom undervisningsväsendet. Vidare konstateras i utlåtandet att undervisningsväsendet har många uppgifter om minderåriga barn samt i allt högre grad särskilda personuppgifter (såsom uppgifter om behovet av särskilt stöd), så det är viktigt att sörja för informationssäkerheten och dataskyddet.

Kommunförbundet har utarbetat olika utredningar och guider för att främja cybersäkerheten inom kommunalförvaltningen. Rapporten *”9 utmaningar inom digital säkerhet enligt kommunledningen”*, som publicerades 2021, sammanställer kommunledningens uppfattningar om läget för digital säkerhet i kommunerna. I rapporten konstateras bland annat:

- Kommunerna saknar en verksamhetsmodell för digital säkerhet som styr ledningen och genomförandet av digital säkerhet i kommunerna.
- Förmågan att reagera på plötsliga attacker är bristfällig.
- Kompetensen koncentreras för mycket, ämnesområdets innehåll är ofta teknologiskt och svårbegripligt.

- Kraven på digital säkerhet försämrar ofta smidigheten och användbarheten.

Enligt utredningen behövs mer omfattande kompetens om digital säkerhet i kommunerna och all kompetens kan inte koncentreras till enskilda kommuner. Därför är Kommunförbundets och andra samarbetsparters stöd viktigt för kommunerna.

Kommunförbundet har också utarbetat en minneslista *"Digital säkerhet: checklista för kommundirektörer"*. I minneslistan finns en kort förteckning över de viktigaste ansvaren som ska fördelas och de myndigheter som ger stöd i problemsituationer.[113] På minneslistan framförs dock inte till exempel att det ofta krävs specialkompetens för att bekämpa och utreda attacker mot datanät och att denna kompetens främst finns hos företag som producerar informationssäkerhetstjänster.

Kommunförbundet publicerade 2023 en *mall för förvaltningsstadga*[114] för kommunen. Förvaltningsstadgan är kommunens interna regelverk som definierar kommunens ledning och förvaltning och som förutsätts i kommunallagen. I 9 kap. i mallen för förvaltningsstadga presenteras grunderna för organiseringen av ansvaret för informationshanteringen och informationssäkerheten i kommunen.

Utredningen om bekämpning av IT-relaterad brottslighet är inrikesministeriets publikation från 2017. I utredningen presenteras åtgärdsförslag som gäller bland annat utveckling av bekämpningen av nätbrott, förbättring av utbildningen i bekämpning, utveckling av lägesbildsverksamheten gällande nätbrottslighet samt revidering av lagstiftningen. Genomförandet av åtgärdsförslagen i utredningen var inte längre under aktiv uppföljning, så utredningsgruppen bad ministeriets polisavdelning utarbeta ett sammandrag av hur åtgärderna framskrider.

Av polisavdelningens sammandrag framgår att de centrala åtgärdsförslagen har framskridit. Reformer har gjorts särskilt inom samarbetsstrukturerna och utbildningen. Bland annat i Polisyrkeshögskolans undervisningsutbud har man utvecklat utbildningen i anslutning till utredning av ämnesområdet.

Lagstiftningen har också utvecklats eller håller på att utvecklas. I åtgärdsförslagen som gällde lagstiftningen hade man lyft fram trycket på skyldigheten att inleda förundersökning av nätbrottslighet. Åtgärdsförslaget löd enligt följande:

> *"Tillsammans med justitieministeriet bedöms behovet av att ändra bestämmelserna om polisens förundersökning och vid behov bereds lagändringar så att utredningsresurserna kan riktas på behörigt sätt med beaktande av arten av brott som riktar sig mot datanätsmiljöer och målsägandens ställning."*

I polisavdelningens sammandrag framförs att fallen Vastaamo och WinCapita visar att det i Finland inte finns någon mekanism för att kollektivt tillgodose brottsoffrens rättigheter. Det utmanar myndigheternas förmåga att behandla fall med ett stort antal målsägande. Den finländska straffprocessen och dess processregler kan inte hantera ett stort antal målsägande och deras privaträttsliga yrkanden.

En **utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet** är ett gemensamt utredningsprojekt enligt inrikesministeriets och försvarsministeriets riktlinjer för den inre säkerheten och försvarsredogörelserna av den 15 februari 2022 samt det tidigare statsrådets principbeslut av den 10 juni 2021 för att bedöma myndigheternas

---

[113] Kommunförbundet: Digital säkerhet: checklista för kommundirektörer. 26.2.2025 https://www.kommunforbundet.fi/sites/default/files/media/file/2022-03-18-digisakerhet-minneslista.pdf

[114] Kommunförbundet: Mall för förvaltningsstadga för kommunen. 26.2.2025 https://www.kommunforbundet.fi/publikationer/2023/2242-mall-forvaltningsstadga-kommunen

verksamhetsförutsättningar i fråga om tryggandet av den nationella cybersäkerheten, bekämpandet av cyberbrottslighet, cyberförsvaret och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället, med beaktande av den kontinuerliga utvecklingen av den nationella och internationella hotmiljön.[115] Syftet med utredningen var att utarbeta utvecklingsförslag med hjälp av vilka man kan förbättra myndigheternas verksamhetsförutsättningar.

Enligt utredningen har myndigheterna i den verkliga världen i allmänhet tydliga uppgifter i hanteringen av olika hotfulla situationer och ansvarsområdena och samarbetsskyldigheterna mellan myndigheterna är fastställda. I fråga om cyberverksamhetsmiljön saknar lagstiftningen i Finland tillräckliga bestämmelser om samordning och samarbete mellan myndigheter på olika nivåer, och lagstiftningen beaktar inte i tillräcklig utsträckning cyberverksamhetsmiljöns särdrag i bekämpning av cyberhot och informationsutbyte.

Skyddet av cyberverksamhetsmiljön har fördelats på flera olika förvaltningsområden och hela cyberverksamhetsmiljön har inte anvisats och kan inte anvisas till något enskilt förvaltningsområde. För att kunna reagera på hoten krävs ett nära samarbete mellan förvaltningsområdena både på strategisk och operativ nivå. Genom att ytterligare intensifiera samarbetet kan man säkerställa att rätt myndighet vidtar åtgärder i rätt tid, dock utan att äventyra en annan myndighets uppgifter och att bästa kompetens anlitas i verksamheten.

Enligt utredningen har myndigheterna i nuläget inte tillräckliga verksamhetsförutsättningar för att effektivt förbereda sig för och bekämpa de allvarligaste cyberhoten som äventyrar den nationella cybersäkerheten och försvaret. För att förbättra verksamhetsförutsättningarna har man identifierat behov av utvecklingsåtgärder inom sju centrala delområden: cybersäkerhetens strategiska målbild, samarbete och myndighetsprocesser, lägesbild, informationsutbyte, påverkan och motåtgärder, informationshämtning och skydd av myndighetsnätverk.

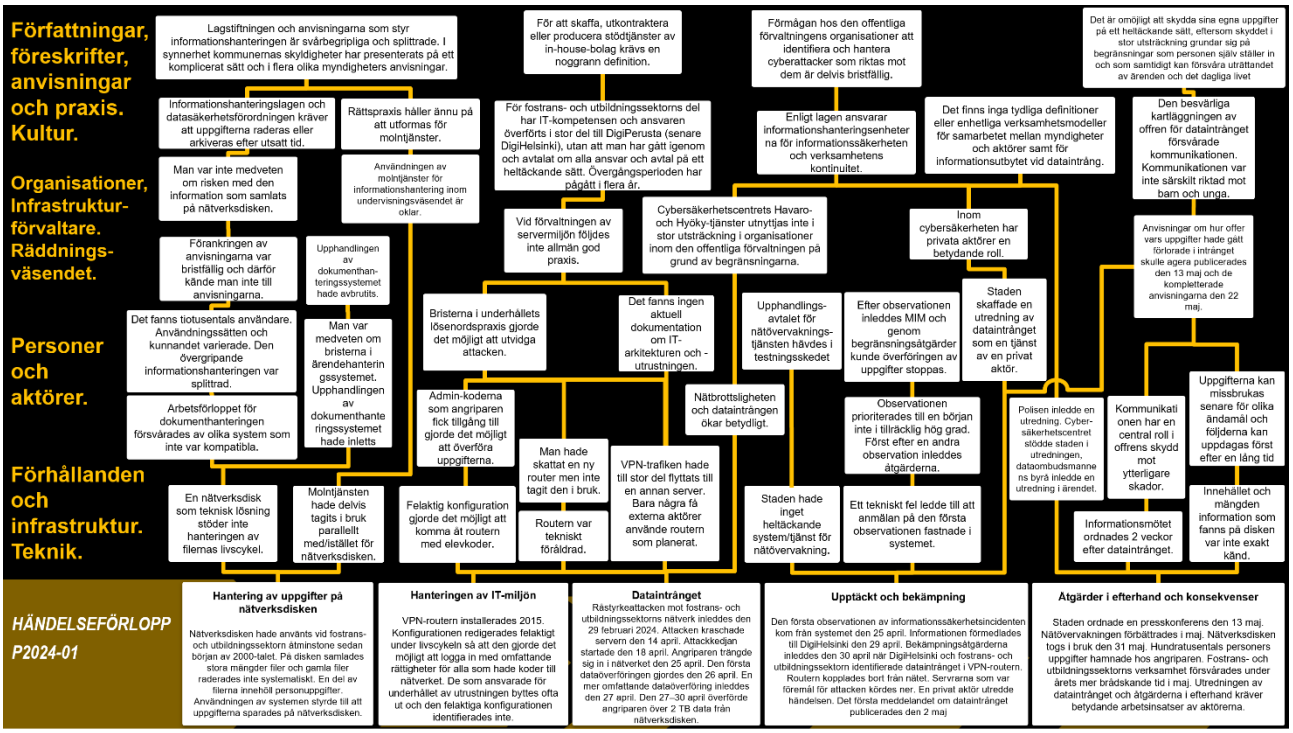
Utöver behovet av att intensifiera myndighetssamarbetet är det skäl att beakta att många kritiska samhällsfunktioner ägs i hög grad av den privata sektorn och att dessa aktörers cybersäkerhetsberedskap varierar betydligt. Cybersäkerhetscentrets CERT-funktion (Computer Emergency Response Team) hjälper vid behov aktörerna i det första skedet av att utreda personuppgiftsincidenter, men en mer omfattande utredning och fortsatta åtgärder genomförs till exempel med hjälp av tjänster inom den privata sektorn.

[115] Statsrådet (2023): Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet. 26.2.2025 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164793/VN_2023_31.pdf

3 ANALYS

Vid analysen av händelsen har man använt sig av Accimap-metoden som vidareutvecklats av Olycksutredningscentralen.[116] Strukturering av analystexten grundar sig på Accimap-diagrammet som utarbetats i utredningen, där händelsen beskrivs som en händelsekedja i schemats nedre del. De faktorer som ligger bakom händelsekedjan avvecklas i diagrammet på olika analysnivåer.

3.1 Analys av händelsen



Figur 18. P2024-01 ACCIMAP-analysdiagram.

3.2 Hantering av uppgifter på nätverksdisken

Inom Helsingfors stads fostrans- och utbildningssektor tog man i början av 2000-talet i bruk en nätverksdisk där man mycket fritt kunde spara filer. Alla anställda vid fostrans- och utbildningssektors hade tillgång till disken och den hade tiotusentals användare under årens lopp. På disken samlades under åren över fyra miljoner filer, av vilka en del innehöll känsliga uppgifter som hör till särskilda kategorier av personuppgifter. Innehållet på disken hade inte gåtts igenom systematiskt på flera år och gamla filer raderades inte. Nätverksdiskar har länge varit allmän teknik, men som en teknisk lösning stöder de inte systematisk informationshantering eller informationens livscykelmodell.

På nätverksdisken var man tvungen att spara material som stöder verksamheten och gäller beredningen av beslutsfattandet, vilket också utnyttjades i de officiella ärendehanteringssystem som användes. Detta berodde på Helsingfors stads många informationssystem som inte hade integrerats i en enhetlig ärendehanteringshelhet.

---

116 Rasmussen, J. & Svedung, I. (2000) *Proactive Risk Management in a Dynamic Society*. Karlstad, Sweden: Swedish Rescue Services Agency.

Helsingfors stad hade anvisningar för personalen om informationshantering och användning av IT-miljön. Anvisningarna var delvis utspridda i stadens dokumenthanteringssystem. Ett centralt problem var att personalen vid fostrans- och utbildningssektorn kände till anvisningarna dåligt, så deras inverkan på den praktiska verksamheten var liten.

Helsingfors stad hade identifierat brister i sina dokumenthanteringssystem och inlett en offentlig upphandling i anslutning till detta. Marknadsdomstolen upphävde dock upphandlingen på grund av ett formfel.

Helsingfors stad hade delvis övergått till att använda molntjänster i stället för nätverksdiskar. Fostrans- och utbildningssektorn hade dock fortsatt att använda nätverksdiskar i en stor del av sin organisation. Införandet av molntjänster inom kommunsektorn har bromsats upp av oklarheter om de rättsliga förutsättningarna och begränsningarna gällande deras användning. Även rättspraxisen håller ännu bara på att ta form.

Användarrättigheterna till nätverksdisken hade definierats enligt organisation och funktion, säkerhetskopieringen hade ordnats på samma sätt, men man var inte medveten om riskerna förknippade med det stora antalet filer som hade samlats på disken eller dess läckage.

Informationshanteringen är förknippad med många lagar, anvisningar och flera myndigheter. Ämnet är uppsplittrat i flera lagar och det är svårt att bilda en uppfattning av helheten. Informationshanteringslagen och EU:s allmänna dataskyddsförordning föreskriver att uppgifter som lagrats ska raderas eller arkiveras inom den tid som organisationen fastställt för dem.

3.3 Hantering av IT-miljön

Dataintrånget gällde en VPN-router som togs i bruk 2014. Fjärrförbindelserna till fostrans- och utbildningssektorns nätverk hade i huvudsak redan överförts till andra VPN-routrar, så ASA 5515-routern som utsattes för intrånget användes främst av externa aktörer. Enheten var tekniskt föråldrad och på grund av att uppdateringar saknades var informationssäkerheten inte uppdaterad. En ersättande enhet hade skaffats för routern, men den hade inte tagits i bruk.

Den mest avgörande faktorn för att dataintrånget lyckades var en felaktig konfiguration som gjorde det möjligt att få åtkomst till systemet med elevkoder och gav omfattande rättigheter att använda intranätet. Tidpunkten när inställningarnas ändrades eller vem som gjorde ändringarna kunde inte fastställas i utredningen. Vem som ansvarade för underhållet av enheten hade bytts flera gånger och det var oklart även vid tidpunkten för dataintrånget.

De underhållskoder som angriparen kom över i intranätet och bristerna i lösenordspraxis gjorde det lättare att utvidga dataintrånget till nya servrar. I hanteringen av datakommunikations- och servermiljön iakttogs som helhet inte god praxis för IT-sektorn.

Helsingfors stads IT-tjänster hade omorganiserats under de senaste fem åren. De hade först koncentrerats till Digitaalinen perusta och senare till bolaget DigiHelsinki. Fostrans- och utbildningssektorn som sektor hade i huvudsak fortsatt att upprätthålla en egen informationsteknisk helhet. Inom den hade det dock skett många organisations- och personförändringar som ledde till att fostrans- och utbildningssektorns ansvar för underhållet av informationstekniken delvis var oklart. Inom kommunsektorn har man allmänt identifierat utmaningarna med att skaffa externa tjänster, lägga ut dem på entreprenad och använda in-house-bolag i serviceproduktionen.

3.4 Dataintrånget

Dataintrånget hade förberetts med en råstyrkeattack samt med en skanning av miljön i slutet av februari och i mars 2024. Den 14 april 2024 riktades en attack mot fostrans- och utbildningssektorns VPN-router genom att utnyttja en känd sårbarhet, vilket kraschade routern. Orsaken till kraschen undersöktes dock inte, även om undersökningen skulle ha avslöjat att enheten fortfarande var i användning och inte uppdaterats samt att enhetens loggning inte fungerade på grund av att diskutrymmet på den separata loggservern var fullt.

Det egentliga dataintrånget inleddes den 18 april 2024. Angriparen loggade in i fostrans- och utbildningssektorns nätverk via routern den 25 april 2024, då den första filöverföringen från nätverket gjordes. De viktigaste filöverföringarna gjordes 27–30 april 2024, då sammanlagt cirka två terabyte (cirka 750 000 filer) exporterades.

Dataintrången har i allmänhet ökat under de senaste åren. Cybersäkerhetscentret producerar en lägesbild för samhället och organisationerna med hjälp av Havaro- och Hyöky-tjänsterna. Helsingfors stad har varit kund hos Hyöky sedan slutet av 2023, men den sårbara routern hade utelämnats från de kontroller som tjänsten gjorde.

De tjänster som Cybersäkerhetscentret producerar utnyttjas i liten utsträckning i organisationer inom den offentliga sektorn, eftersom Cybersäkerhetscentret inte har haft resurser att utveckla och upprätthålla dessa tjänster för denna målgrupp.

Nätbrottslighet utgör ett betydande hot mot den offentliga förvaltningen, som förfogar över stora mängder information som samlats in om medborgarna. Därför kan offentliga organisationer vara attraktiva mål för dataintrång. Oftast grundar sig behandlingen av personuppgifter inom den offentliga förvaltningen på skötseln av en lagstadgad uppgift och därför är de registrerades möjligheter att begränsa och övervaka användningen av sina egna uppgifter begränsade. På grund av underställda ställningen hos förvaltningens kund uppstår en betonad skyldighet för den offentliga förvaltningen att skydda de registrerades uppgifter.

Organisationsledningens ansvar för informationssäkerheten och dataskyddet är entydigt.

3.5 Upptäckt och bekämpning

Programvara för bekämpning av skadlig programvara gav larm den 25 april 2024, men informationen förmedlades till fostrans- och utbildningssektorn först den 29 april 2024. Inte heller då identifierades genast hur kritiska informationssäkerhetslarmen var, så bekämpningsåtgärderna kunde inledas först den 30 april 2024.

Fostrans- och utbildningssektorn och DigiHelsinki identifierade VPN-routern som var källan till dataintrånget. Routern lösgjordes från nätet och de övriga servrarna som var föremål för attacken kördes ner. Fördröjningen mellan den första observationen och att bekämpningsåtgärderna inleddes påverkades av tekniska och processfel i systemet för servicebegäran samt brister i informationsgången mellan aktörerna.

Om man hade använt en omfattande logghantering och ett kontrollrum för informationssäkerhet skulle attacken sannolikt ha identifierats redan i beredningsskedet och den skulle inte ha framskridit till dataintrånget. Nätövervakningen i realtid skulle ha observerat de exceptionellt stora dataöverföringarna som ägde rum nattetid från intranätet till internet. Helsingfors stad stod i beråd att upphandla ett omfattande system för nätövervakning, men upphandlingen av systemet hade avbrutits eftersom beställaren inte var nöjd med resultaten från ibruktagningstestet.

Eftersom stadens egna resurser och kompetens ansågs vara otillräckliga köptes tjänster av ett utomstående företag för att utreda och hantera dataintrånget. Privata aktörer har kritiska resurser för informationssäkerheten och myndigheternas tillgängliga resurser är begränsade. Aktörer inom den offentliga sektorn har inte möjlighet att i någon stor utsträckning stödja aktörer vid dataintrång eller andra krissituationer som gäller informationssäkerheten. Samarbetet mellan myndigheterna är i dessa situationer delvis ostrukturerat och stöder inte alltid hanteringen av störningssituationer.

Helsingfors stad grundade flera arbetsgrupper som sammanträdde regelbundet och ofta för att hantera krissituationen. Staden började delge information offentligt med ett pressmeddelande den 2 maj 2024. Den ursprungliga lägesbilden av det inträffade, dess följder och konsekvenser för olika målgrupper preciserades i takt med att utredningsarbetet av dataintrånget framskred.

Vid dataintrång fokuseras uppmärksamheten lätt på händelsens tekniska detaljer, såsom sårbarheter i systemen och informationssäkerhetsåtgärder. Kommunikationens roll är dock lika kritisk – den påverkar direkt offrens möjlighet att skydda sig mot ytterligare skador. En klar, snabb och konsekvent kommunikation hjälper till att hantera situationen, förebygga felaktig information och säkerställa att de berörda får det stöd och de anvisningar de behöver.

3.6 Åtgärder i efterhand och konsekvenser

Informationsmötet ordnades 11 dagar senare den 13 maj 2024. På mötet gavs anvisningar och man berättade att situationen och dess omfattning utreds ytterligare. I meddelandet av den 21 maj 2024 berättades att målgrupperna som var offer för dataintrånget har utvidgats.

I kommunikationen kan man inte vänta på de slutliga resultaten av utredningsarbetet, utan det är viktigt att i ett tidigt skede ge en allmän bild och berätta om skyddsåtgärderna för offren för dataintrånget. Även om man vid dataintrång är tvungen att agera på bristfällig information, bygger öppenhet upp förtroende och gör det möjligt att undvika att det uppstår ett informationsvakuum och att spekulationer sprids.

Helsingfors stad riktade snabbt kommunikationen till stadens anställda och vårdnadshavare. För att stöda den personliga och interaktiva kommunikationen öppnades ett servicenummer för offren för dataintrånget och berörda parter, såsom vårdnadshavarna. Kommunikationen riktades dock inte till olika åldersgrupper, såsom barn och unga enligt deras åldersnivå, och man beaktade inte barns och ungas behov till exempel med klarspråk (även minoritetsspråkgrupper), visuellt innehåll eller de kommunikationskanaler de använder. Till exempel finns det ett heltäckande och effektivt sätt att nå minderåriga enligt skolklass, eftersom det gör det möjligt att informera eleverna direkt på ett sätt som är lämpligt för deras åldersnivå och samtidigt erbjuder dem möjlighet till frågor och handledning.

Helsingfors stad meddelade den 18 juni 2024 att dataintrånget mot staden inte har blivit större. Staden meddelade den 12 juli 2024 att en utredningsgrupp som utnämnts av statsrådet inleder en utredning om ett dataintrång som riktats mot Helsingfors stad. Nästa gång staden informerade om dataintrånget var den 17 december 2024.

Enligt artikel 34 i dataskyddsförordningen (GDPR) ska information till offer för personuppgiftsincidenter i första hand ges personligen och utan obefogat dröjsmål, om kränkningen sannolikt medför en hög risk för den registrerades rättigheter eller friheter.

Helsingfors stad riktade snabbt sin interna kommunikation till stadens anställda. Stadens anställda kunde snabbt nås via den personliga kommunikationen, eftersom man kände till deras e-postadresser och man utan dröjsmål kunde meddela dem om dataintrånget både på stadens

intranät och med ett personligt e-postmeddelande. För att stöda den personliga och interaktiva kommunikationen öppnades ett servicenummer för offren för dataintrånget och berörda parter.

Det visade sig vara betydligt besvärligare att nå tidigare och nuvarande elever, deras vårdnadshavare och andra som uträttat ärenden med staden. Att informera alla registrerade personligt upplevdes som omöjligt och man gjorde inga försök. Även om dataskyddsförordningen tillåter allmän delgivning när det är orimligt att nå enskilda personer garanterar detta inte automatiskt att informationen är effektiv eller heltäckande.

Att falla offer för dataintrång kan orsaka många slags hälsorisker, psykisk belastning och att känslan av trygghet rubbas. Stulen information kan utnyttjas för kriminella ändamål, såsom identitetsstöld, ekonomiskt bedrägeri, utpressning och bedrägerier samt för att skada ryktet även flera år senare. Konsekvenserna av missbruk framträder inte nödvändigtvis genast.

Minderåriga har inte nödvändigtvis förmåga eller kunskap att skydda sina egna uppgifter. De kan också vara okunniga om vikten av dataskydd. De vet inte nödvändigtvis hur uppgifterna kan användas för brottsliga ändamål och förstår inte alltid vikten av att skydda sig. Dessutom kan skyddsåtgärder, såsom kreditförbud eller begäran om radering av uppgifter, vara komplicerade ur en minderårigs synvinkel och de kräver åtgärder av vårdnadshavaren. På motsvarande sätt kan de vara utmanande också för personer som inte talar finska, svenska eller engelska.

Det är viktigt att de unga och deras vårdnadshavare erbjuds klara och tillgängliga anvisningar om beredskap för dataintrång och minimering av deras konsekvenser. Dessutom kan man via utbildning och mediefostran hjälpa unga att förstå hur deras personuppgifter kan utnyttjas och hur de kan skydda sig bättre.

Innan denna redogörelse färdigställdes har det inte observerats några tecken på att personuppgifter skulle ha spridits i det mörka nätet eller utnyttjats för identitetsstöld. Det går dock inte att utesluta att personuppgifter utnyttjas i framtiden.

4 SLUTSATSER

Slutsatserna innehåller orsakerna till händelsen. Med orsak avses olika faktorer som ligger bakom händelsen och direkta och indirekta faktorer som påverkar den.

1. På nätverksdisken samlades under årens lopp olika uppgifter och raderingen av onödiga uppgifter gjordes på människors eget initiativ att radera uppgifter och ordna filer, vilket inte var systematiskt eller övervakat.

   Slutsats: *Att hanteringen av informationens livscykel grundar sig på de hanteringsåtgärder som användarna själva genomför ökar risken för en situation där behandlingen av personuppgifter och informationshanteringen som helhet blir okontrollerbar.*

2. Informationshanteringslagen och dataskyddsförordningen är sinsemellan samordnade, men tillsammans med andra författningar inom den offentliga förvaltningen, såsom förvaltningslagen, offentlighetslagen, arkivlagen och speciallagstiftningen, framstår informationshanteringshelheten som svårbegriplig och olika lagar innehåller flera liknande utvärderings- och planeringsskyldigheter.

   Slutsats: *Informationshanteringen inom den offentliga förvaltningen är förknippad med flera författningar som utfärdats vid olika tidpunkter och som inte bildar en tydligt samordnad helhet. Därför är det svårt för de som ansvarar för informationshanteringen att uppfatta kravhelheten och det leder till en varierande tillämpning av dessa.*

3. Informationshanteringen, informationssäkerheten och dataskyddet inom den offentliga förvaltningen styrs av flera olika myndigheter. Myndigheterna utför handledning självständigt utifrån sin egen uppgift.

   Slutsats: *När flera myndigheter styr informationshanteringen är den styrning som informationshanteringsenheterna får splittrad och i praktiken varierar tillämpningen av författningar och anvisningar. Myndigheternas arbete består av styrning, men tillsynen över aktörerna är ringa.*

4. IT-brottslighet är ett växande kriminalitetsområde och de olägenheter den orsakar är betydande. Den offentliga förvaltningen är på grund av informationens art och mängd i dess besittning ett intressant objekt för brottslingar.

   Slutsats: *Den offentliga sektorns förmåga att svara på hot som orsakas av nätbrott är för närvarande bristfällig, eftersom metoder för att observera attacker och sårbarheter inte tillämpas på ett heltäckande sätt. Genom att identifiera och korrigera attacker och sårbarheter är det möjligt att förhindra dataintrång och skydda personuppgifter.*

5. Den föråldrade VPN-routern förblev i bruk även om största delen av användarna hade övergått till att använda en ny VPN-router. Ingen hade ett tydligt ansvar för enheten, så underhållet av den var minimalt och begränsades endast till det obligatoriska förnyandet av certifikatet.

   Slutsats: *När det sker ändringar i tekniken och organisationen förblir IT-utrustningens underhåll dåligt, vilket innebär en risk för dataintrång.*

6. Beredningen av dataintrånget skulle ha kunnat observeras flera veckor tidigare genom omfattande webbövervakning. Försök att utvidga intrånget mot det intranätet orsakade larm, men man reagerade inte i tillräcklig grad på dem.

Slutsats: *Att ett dataintrång lyckas beror sällan på ett fel eller en försummelse. Nätövervakningen är en central del av en informationssäker hantering av IT-miljön. Avsaknaden av logginformation fördröjer utredningen av skador, stör rensningsarbetet och försvårar beredskapen inför framtida attacker.*

7. Vid dataintrång ligger ansvaret för att utreda ärendet och avvärja angreppet hos den organisation som utsatts för attacken. Staden inledde åtgärder för att bekämpa dataintrånget tillsammans med det datasäkerhetsbolag som staden anlitat. Även myndigheter deltog i bekämpningsåtgärder och andra utredningsåtgärder.

   Slutsats: *Inom den offentliga sektorn är utredningen och hanteringen av dataintrång beroende av sakkunskapen hos den privata sektorns aktörer och deras tillgänglighet. Det finns ingen verksamhetsmodell för att inleda samarbete, utbyta information och samordna åtgärder.*

8. Helsingfors stad inledde den interna kommunikationen om dataintrånget omedelbart, men den externa kommunikationen med fördröjning. Stadens anställda nåddes snabbt via personlig kommunikation. Däremot var det svårare att rikta kommunikationen till tidigare och nuvarande elever samt deras vårdnadshavare och stadens övriga kunder.

   Slutsats: *Det kan vara svårt att nå offren för dataintrånget. Allmän delgivning är viktig, men i sig räcker det inte för att säkerställa att kommunikationen är tillgänglig. Förutseende kommunikationsplanering och information via flera kanaler är viktigt för att offren för dataintrånget ska kunna skydda sig.*

9. Informationen till barn och unga var bristfällig och beaktade inte i tillräcklig grad olika ålders- och specialgruppers behov, såsom att rikta kommunikationen enligt åldersnivå.

   Slutsats: *Minderåriga offer för dataintrång kan inte nödvändigtvis skydda sina personuppgifter själva. Därför är det viktigt att rikta kommunikationen till barn, unga och vårdnadshavare, och att genomförandet är besvärligt får inte utgöra ett hinder för detta.*

10. I Finland är det möjligt att begränsa användningen och utlämnandet av egna personuppgifter i offentliga informationssystem. Detta görs med inställningar som personen själv konfigurerar och som begränsar användningen av dennes egna personuppgifter men som kan inte helt förhindra utnyttjandet av uppgifterna för kriminella ändamål.

    Slutsats: *Det är omöjligt att skydda sina egna personuppgifter på ett heltäckande sätt och det grundar sig i stor utsträckning på de begränsningar som personen själv konfigurerat, som samtidigt kan försvåra uträttandet av ärenden och det dagliga livet. Offer för dataintrång utsätts för långvarig risk för senare missbruk av deras egna uppgifter.*

5 SÄKERHETSREKOMMENDATIONER

5.1 Samordning av lagstiftningen om informationshantering

Bestämmelser som ska beaktas i informationshanteringen inom den offentliga förvaltningen har utfärdats vid olika tidpunkter. När informationshanteringslagen stiftades beaktades de centrala kraven i den allmänna dataskyddsförordningen, och dessa bestämmelser kan anses vara samordnade med varandra. Det förekommer fortfarande bestämmelser om informationshantering även i annan lagstiftning. Det finns bestämmelser i speciallagar och i den allmänna förvaltningslagstiftningen, såsom arkivlagen och offentlighetslagen. Dessa har inte samordnats på ett heltäckande sätt från början till slutet av informationens livscykel och särskilt bestämmelserna och föreskrifterna om arkivering är gamla. Även de tekniska lösningarna har utvecklats i mycket hög grad, vilket ökar behovet av att se över lagstiftningen.

Fördelningen av tillsyns- och styrningsuppgifterna mellan flera olika myndigheter orsakar för sin del också svårigheter i att få till stånd enhetliga styrande materialet och för dem som tillämpar materialet.

Utredningsgruppen rekommenderar att

finansministeriet i samarbete med justitieministeriet ser till att lagstiftningen om informationshantering inom den offentliga förvaltningen samordnas och att dess tillsyns- och styrningsstrukturer förtydligas. [2025-S4]

Bestämmelserna förutsätter bland annat överlappande planerings- och bedömningsskyldigheter, såsom användning av informationshanteringsmodellen, konsekvensbedömning och riskbedömning. Uppmärksamhet ska också fästas vid verkställandet av lagstiftningen, styrningen av dess tillämpning och stödet till dem som tillämpar lagstiftningen i olika tolkningsfrågor. Praktiska tillämpningsproblem har bland annat orsakats av genomförandet av informationshanteringen i tjänsterna och användningen av molntjänster i behandlingen av personuppgifter.

5.2 Utveckling av observation av informationssäkerhetsbrister inom den offentliga förvaltningen

Att på förhand upptäcka brister i informationssäkerheten inom den offentliga förvaltningen är ett effektivt sätt att förhindra att sårbarheter utnyttjas och på så sätt förebygga dataintrång. Den ökade IT-brottsligheten förutsätter att informationssäkerhetsåtgärderna utvecklas på bred front och i flera lager. Detta innebär att det är viktigt att kontinuerligt uppdatera och förbättra informationssäkerhetspraxisen samt utnyttja de senaste teknikerna och metoderna. Dessutom är det viktigt att utbilda personalen i informationssäkerhetsfrågor och säkerställa att alla organisationsnivåer är medvetna om eventuella hot och kan agera för att bekämpa dem. På så sätt kan man skapa ett heltäckande och effektivt informationssäkerhetssystem som skyddar den offentliga förvaltningens information och resurser.

Utredningsgruppen rekommenderar att

finansministeriet i samarbete med kommunikationsministeriet utreder på vilket sätt observationen av informationssäkerhetsbrister inom den offentliga förvaltningen kan förbättras på riksnivå och säkerställer att de offentliga aktörerna har tillräcklig förmåga att upptäcka och åtgärda informationssäkerhetsbrister. [2025-S5]

Den nuvarande tjänsten Hyöky används inte i stor utsträckning bland aktörer inom den offentliga förvaltningen. Det behövs dock en tjänst för identifiering av informationssäkerhetsbrister som är lätt att använda och som alla offentliga organisationer kan ta i bruk. På så sätt kan informationssäkerheten inom den offentliga förvaltningen förbättras på ett övergripande sätt.

5.3 Utveckling av kommunikationsanvisningarna vid dataintrång

Kommunikation är en del av beredskapen för dataintrång. Detta förutsätter uppdaterade anvisningar för kommunikation. När ett dataintrång inträffar är det viktigt att kommunicera på ett snabbt, klart, tillgängligt och konsekvent sätt. Detta minskar osäkerheten, förebygger spridningen av felaktig information och säkerställer att offren får det stöd de behöver. Dessutom ska anvisningar och stöd erbjudas dem vars uppgifter har äventyrats. Informationen om dataintrång ska vara flerkanalig, lämplig och anpassad för åldersnivån samt tillgänglig för att informationen ska nå dem som fallit offer för dataintrånget på ett heltäckande och begripligt sätt. Om dataintrånget inte kommuniceras klart och konsekvent kan det uppstå flera risker. Osäkerheten ökar när de berörda inte vet vad som har hänt och hur det påverkar dem, vilket kan orsaka onödig oro och stress.

Utredningsgruppen rekommenderar att

finansministeriet i samarbete med Utbildningsstyrelsen ser till att kommunerna och städerna utvecklar klara och tillgängliga anvisningar för kommunikation om dataintrång. Med hjälp av anvisningarna kan offren skydda sig mot dataintrångens konsekvenser och skydda sina egna personuppgifter. [2025-S6]

I utvecklingen av kommunikationen bör man eftersträva ett omfattande samarbete särskilt med undervisnings- och kulturministeriet och Cybersäkerhetscentret. I det praktiska genomförandet lönar det sig att utnyttja de kanaler som de unga använder, såsom sociala medier och meddelandetjänster, samt information till vårdnadshavarna via journalistiska medier, e-post, brevpost och officiella webbplatser. Dessutom är skolklassen ett effektivt sätt att nå minderåriga, eftersom detta sätt möjliggör handledning och behandling av frågor på ett sätt som är lämpligt för åldersnivån.

5.4 Identifiering och åtgärdande av kommunernas kritiska informationssäkerhetsbrister

Säkerställandet av informationssäkerheten och förebyggandet av dataintrång förutsätter förebyggande, omedelbara och kontinuerliga åtgärder av kommunerna för att förbättra riskhanteringen i anslutning till behandling och lagring av personuppgifter.

Identifiering och hantering av risker i anslutning till behandling och lagring av personuppgifter är centrala åtgärder för att säkerställa uppgifternas tillförlitlighet och informationssäkerhet i offentliga tjänster.

En regelbunden riskanalys hjälper till att identifiera och åtgärda eventuella problem i tid.

Utredningsgruppen rekommenderar att

finansministeriet i samarbete med Kommunförbundet stöder kommunerna i identifieringen och åtgärdandet av kritiska informationssäkerhetsbrister samt utvecklar riskhanteringen inom informationshanteringen och datasäkerheten. [2025-S7]

Organisationerna ska identifiera var de har lagrat personuppgifter. Objekt som ska granskas omedelbart är de lagringsplatser som organisationen använder, såsom nätverksdiskar, chattjänster, e-post och molntjänster. Dessutom ska informationssäkerheten för fjärrförbindelser kontrolleras.

Det är bra att inkludera välfärdsområdena och andra intressentgrupper i utvecklingsarbetet.

5.5 Genomförda åtgärder

Helsingfors stads handlingsprogram inleddes efter dataintrånget genom beslut av kanslichefen. I samband med beslutet utreddes bristerna i ärendehanteringen och informationssäkerheten enligt verksamhetsområde korrigerande åtgärder anvisades. Åtgärderna har prioriterats i en genomförandeordning enligt hur viktiga de är. I åtgärderna har man beaktat faktorer som möjliggjort dataintrånget, till exempel informationssäkerhetsutbildning för personalen, fjärrförbindelsepraxis, lagringsplatser för personuppgifter samt fastställande av ansvar för radering av uppgifter. Utvecklingsprogrammet omfattar en regelbunden rapporteringsskyldighet gentemot kanslichefen per delåröversikt.[117]

Helsingfors stad fattade ett upphandlingsbeslut om ytterligare åtgärder för informationssäkerhet från DigiHelsinki Oy den 12 augusti 2024. Åtgärderna gäller förbättring av informationssäkerhetsbrister som observerades vid dataintrånget. Värdet på den extra upphandlingen var 2,6 miljoner euro.[118]

NIS 2-direktivet är Europeiska unionens cybersäkerhetsdirektiv och dess mål är att stärka EU:s gemensamma och medlemsstaternas nationella cybersäkerhetsnivå särskilt inom kritiska sektorer. Den fastställer minimiåtgärder för hantering av cybersäkerhetsrisker samt rapporteringsskyldigheter vid betydande incidenter. Direktivet antogs i november 2022 och dess medlemsstater ska införliva det i den nationella lagstiftningen senast den 17 oktober 2024. Lagarna som verkställer NIS 2-direktivet gavs till riksdagen den 23 maj 2024 och de godkändes i riksdagen i mars 2025 och trädde i kraft den 8 april 2025. Bestämmelser om skyldigheter för den offentliga förvaltningen enligt NIS 2-direktivet finns i det nya 4 a kap. i lagen om informationshantering inom den offentliga förvaltningen. För andra organisationers del regleras skyldigheten i den nya cybersäkerhetslagen. Lagarna trädde i kraft den 8 april 2025. Transport- och kommunikationsverket är den tillsynsmyndighet inom den offentliga

[117] Kanslichefens åtgärdsprogram (Helsingfors stad 3.9.2024).

[118] Upphandling, ytterligare åtgärder för informationssäkerhet från DigiHelsinki Oy, stadskansliet. 28.2.2025 https://paatokset.hel.fi/fi/asia/hel-2024-011885?paatos=484a470a-21d9-4e44-a0c2-b4ce754116e1

förvaltningen som avses i cybersäkerhetslagen [124/2025]. Dessutom bör man beakta att kommunerna inte omfattas av tillämpningsområdet för cybersäkerhetslagen förutom genom de tjänster de eventuellt tillhandahåller. Den nya cybersäkerhetslagen och ändringarna i informationshanteringslagen som trädde i kraft våren 2025 medför nya skyldigheter även för aktörer inom den offentliga sektorn. Transport- och kommunikationsverket fungerar som tillsynsmyndighet för aktörerna inom den offentliga sektorn och strävar i sin nya roll efter att förtydliga sektorns styrnings- och tillsynsstrukturer.

Direktiv om kritiska entiteters motståndskraft mot störningar (CER, Critical Entities Resilience Directive)[119] trädde i kraft den 14 december 2022 och medlemsstaterna ska införliva dess krav i sin nationella lagstiftning senast den 17 oktober 2024. Syftet med CER-direktivet är att förbättra säkerställandet av motståndskraften i fråga om ömsesidigt beroende tjänster som är kritiska med tanke på samhällets funktionsförmåga samt att upprätthålla samhällets ekonomiska funktioner. CER-direktivet genomförs genom att det stiftas en allmän lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft. I lagen föreslås bestämmelser om en nationell strategi för kritisk infrastruktur och kritiska aktörers motståndskraft och en anknytande nationell riskbedömning, om den allmänna styrningen och samordningen av verksamheten, om ett samstämmigt ramverk för bedömning av kritiska aktörer och om en enhetlig ram för att stärka kritiska aktörers motståndskraft mot hot av olika slag. Direktivet medför nya uppgifter för det samordnande ministeriet, sektorministerierna och myndigheterna. Direktivet medför en ny uppgift att genom enhetliga förfaranden identifiera kritiska aktörer samt uppgifter i anslutning till tillsynen. Sektorsspecifika tillsynsmyndigheter föreslås vara behöriga att utöva tillsyn över de kritiska aktörerna. De centrala skyldigheterna som gäller kritiska aktörer gäller riskbedömning, plan för störningstålighet och säkerställande av störningstolerans samt förfaranden för avvikelser.

Cyberresiliensförordningen[120] (CRA, Cyber Resilience Act) (EU) 2024/2847 är en EU-förordning vars syfte är att förbättra cybersäkerheten för digitala enheter och programvaror på EU:s marknad så att produkterna har färre sårbarheter. Författningen ställer minimikrav på cybersäkerhet för apparater med digitala element och programvara, vilka direkt eller indirekt kan anslutas till en annan enhet eller ett nät. Sådana produkter är till exempel säkerhetskameror, tv-apparater, leksaker, hushållsroutrar, brandväggar samt olika programvaror, såsom operativsystem och webbläsare.

Tillverkarna ansvarar för sina produkters cybersäkerhet under produkternas hela livscykel. De ska säkerställa att produkterna har planerats, utvecklats och tillverkats i enlighet med de väsentliga cybersäkerhetskraven i författningen. Dessa krav gäller bland annat säkra standardinställningar, automatiska säkerhetsuppdateringar, förhindrande av obehörig åtkomst samt konfidentiell behandling av data. Dessutom ska tillverkarna tydligt ange stödperiodens längd för sina produkter och aktivt rapportera om utnyttjade sårbarheter samt allvarliga informationssäkerhetsincidenter till Europeiska unionens cybersäkerhetsbyrå (ENISA) och de nationella CSIRT-enheterna.

---

[119] CER-direktivet, regeringens proposition RP 205/2024. 28.2.2025 https://www.edus-kunta.fi/SV/vaski/HallituksenEsitys/Sidor/RP_205+2024.aspx

[120] Cyberresiliensförordningen (Cyber Resilience Act, CRA). 28.2.2025 https://www.kyberturvallisuuskeskus.fi/sv/toimin-tamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra#76938-0

KÄLLFÖRTECKNING

Utredningsgruppen har fått skriftligt undersökningsmaterial och utfört höranden med stöd av lagen om säkerhetsutredning av olyckor och vissa andra händelser (525/2011). Man kontaktade 26 organisationer. Genom höranden och preliminära samtal inhämtades information från cirka 60 personer. Följande organisationer har lämnat uppgifter till utredningsgruppen:

1. Myndigheten för digitalisering och befolkningsdata
2. DigiHelsinki Oy
3. Dustin Finland Oy
4. Elisa Santa Monica Oy
5. Fujitsu Finland Oy
6. Helsingfors stad
7. Polisen i Helsingfors
8. Helsingfors universitet
9. Centralkriminalpolisen
10. Erfarenhetsexperter
11. Kommunförbundet
12. Barnombudsmannens byrå
13. Kommunikationsministeriet
14. Transport- och kommunikationsverket, Cybersäkerhetscentret
15. Försvarshögskolan
16. Undervisnings- och kulturministeriet
17. Utbildningsstyrelsen
18. Palo Alto Networks
19. Inrikesministeriet
20. Skyddspolisen
21. Telia Cygate
22. Informationshanteringsnämnden
23. Dataombudsmannens byrå
24. Statens cybersäkerhetsdirektörs byrå, Kommunikationsministeriet
25. Finansministeriet
26. Brottsofferjouren

SAMMANDRAG AV UTLÅTANDENA OM UTKASTET TILL UTREDNINGSRAPPORT

Utkastet till utredningsrapport har varit på remiss hos finansministeriet, kommunikationsministeriet, justitieministeriet, undervisnings- och kulturministeriet, inrikesministeriet, Cybersäkerhetscentret vid Traficom, Utbildningsstyrelsen, Helsingfors stad, Skyddspolisen, Centralkriminalpolisen, polisinrättningen i Helsingfors, Myndigheten för digitalisering och befolkningsdata, Dataombudsmannens byrå, informationshanteringsnämnden, Kommunförbundet, Barnombudsmannens byrå, Elisa Santa Monica Oy samt Telia-Cygatella.

Utlåtanden av privatpersoner publiceras inte i enlighet med lagen om säkerhetsutredning av olyckor och vissa andra händelser.

Finansministeriet konstaterar i sitt utlåtande att utredningsrapporten exceptionellt bra och detaljerat behandlar dataintrånget inom fostrans- och utbildningssektorn vid Helsingfors stad och orsakerna till detta. Finansministeriet konstaterar att rekommendationerna i utredningsrapporten gäller lagstiftningen och anvisningarna, men av rapporten framgår dock inte att lagstiftningens tillstånd de facto skulle ha påverkat dataintrånget. Finansministeriet föreslår att man till rekommendationerna i utredningsrapporten fogar anvisningar som gör det möjligt att undvika de brister som uppdagats i utredningen till exempel i servicehanteringen, leverantörshanteringen och egendomsförvaltningen. Finansministeriet anser det också vara bra att en undersökning som denna undersökningsrekommendation görs för alla betydande dataintrång.

Finansministeriet konstaterar att utredningen inte gäller hela kommunsektorn och att det inte är möjligt att genom en analys av händelserna i en kommun dra slutsatser som kan tillämpas på alla kommuner. I fråga om säkerhetsrekommendationerna i utredningsrapporten lyfter finansministeriet fram att det är utmanande att påverka sättet och tidtabellen för beredningen av de författningar som andra ministerier ansvarar för. Därför är det problematiskt att ansvaret för samordningen i en del av åtgärderna i rekommendationen i första hand åläggs finansministeriet. Dessutom påminner finansministeriet om att regleringen av informationshanteringen också ingår i de speciallagar som andra ministerier ansvarar för och som alltid bereds av det ministerium som ansvarar för regleringen i fråga. Finansministeriet framför i sitt utlåtande att det kan främja samordningen med olika metoder, såsom utlåtanden och anvisningar, men det är det ministerium som ansvarar för regleringen som i sista hand ansvarar för samordningen.

Finansministeriet konstaterar att det med stöd av den allmänna uppgiften att följa upp kommunernas verksamhet och ekonomi inte har rätt att få information om ordnandet av den enskilda kommunens interna kontroll och riskhantering eller om dess tillräcklighet, inklusive ansvar för informationssäkerheten och upptäckt av brister. Finansministeriet konstaterar att det således inte kan vara ministeriernas uppgift att skapa en lägesbild över enskilda kommuner eller ett system för att upptäcka brister som omfattar hela kommunsektorn. Dessutom framför finansministeriet i sitt utlåtande att kommunerna i enlighet med sin självstyrelse själva ansvarar för ordnandet av informationshanteringen och informationssäkerheten samt kommunikationen i enlighet med kommunallagen (410/2015). Ministeriet konstaterar också att kommunen sköter de uppgifter som den åtagit sig med stöd av självstyrelsen och ordnar de uppgifter som särskilt föreskrivs för den i lag.

Finansministeriet betonar att upptäckten och åtgärdandet av brister i informationssäkerheten samt utvecklingen av riskhanteringen inom informationshanteringen och dataskyddet är en

del av kommunens interna kontroll och riskhantering och därmed en sak som varje kommuns kommunstyrelse ansvarar för. Finansministeriet konstaterar också att ministerierna inte kan ha ansvar för att utveckla riskhanteringen inom informationshanteringen och dataskyddet eller till exempel för att säkerställa tillräckliga förmågor i alla kommuner. Detsamma gäller säkerställandet av tillräcklig kommunikation.

Enligt finansministeriets uppfattning ska kommunernas eget ansvar för ordnandet av informationshanteringen inte förbigås enbart på grund av att det med tanke på uppföljningen av genomförandet av säkerhetsrekommendationen är lättare att ge rekommendationen till ministerierna. Finansministeriet lyfter också fram att inga rekommendationer alls har getts till kommunerna eller till kommunernas revision. Finansministeriet konstaterar att behovet av att identifiera och korrigera informationssäkerhetsbrister kan variera mellan organisationer och därför är det varje organisations eget ansvar. Enligt finansministeriet kan även välfärdsområdena ha behov av en rekommendation som gäller kommunerna.

Enligt **kommunikationsministeriets** utlåtande beskriver utredningsrapporten tydligt hur situationen framskrider, händelserna under situationen och de åtgärder som vidtagits under den. Utredningsrapporten beskriver de faktorer som lett till händelsen och följderna av den så att andra organisationer kan utnyttja utredningsobservationerna för att utveckla sin egen verksamhet i en säkrare riktning och på så sätt förebygga nya skador.

Dessutom konstaterar kommunikationsministeriet att nivån på cybersäkerheten i hög grad också påverkas av de resurser som olika organisationer använder för cybersäkerhet och dessutom förutsätter utvecklingen av myndigheternas verksamhet och tjänster resursfördelning. I utredningsrapporten har man inte lyft fram de åtstramade statliga finansernas betydelse särskilt för den offentliga förvaltningen och de cybersäkerhetstjänster som produceras i och med den. Kommunikationsministeriet betonar att upptäckandet av brister i informationssäkerheten och andra tjänster som produceras för att förbättra cybersäkerheten kräver kontinuerlig resursfördelning.

Kommunikationsministeriet konstaterar att rekommendationerna för närvarande i huvudsak ges till ministerierna och för att liknande olyckor och tillbud i fortsättningen ska kunna undvikas i såväl kommuner, företag som andra organisationer bör man överväga att ge rekommendationerna även till dessa för att stärka den förebyggande beredskapen.

Transport- och kommunikationsverket lyfter fram att säkerställandet av kontinuiteten i de tjänster som Cybersäkerhetscentret vid Transport- och kommunikationsverket producerar och utvidgningen av användningen av tjänster, såsom Cybermätaren och Hyöky, till större målgrupper samt tryggandet av HAVARO-tjänstens funktion och kontinuitet också har beaktats i Finlands cybersäkerhetsstrategi 2025–2035 och dess genomförandeplan, men att dessa åtgärder ändå har konstaterats kräva tilläggsresurser i strategin.

Kommunikationsministeriet lyfter i sitt utlåtande fram att det är viktigt att utnyttja de erfarenheter som erhållits under utredningen av dataintrånget mot Helsingfors stad samt den färdiga utredningsrapporten som stöd för lagberedningen och regeringsprogrammet för att beakta skrivningen. I lagberedningen bör man fundera på olika alternativ för cybersäkerhet. Med tanke på säkerhetsutredningar av allvarliga riktade störningar beaktas att det redan nu är möjligt att utreda exceptionella händelser.

Undervisnings- och kulturministeriet konstaterar i sitt utlåtande att utredningsrapporten har utarbetats väl och detaljerat. Redogörelsen innehåller väsentlig och värdefull information om orsakerna till och konsekvenserna av dataintrånget mot Helsingfors stad samt om förfarandena för hantering av incidenter. Enligt undervisnings- och kulturministeriet innehåller

redogörelsen också värdefulla lärdomar för organisationerna om utvecklingen av cybersäkerheten, riskhanteringen och hanteringen av undantagssituationer. Innehållet bidrar också till planeringen av eventuella fortsatta åtgärder inom undervisnings- och kulturministeriets förvaltningsområde.

Undervisnings- och kulturministeriet konstaterar att utkastet till utredningsrapporten ur en substanssynvinkel inte innehåller sådan explicit information som skulle äventyra genomförandet av skyddsarrangemangen eller annars inte passar in i en offentlig handling. Undervisnings- och kulturministeriet konstaterar dock att undersökningsrapporten innehåller mycket detaljerade beskrivningar som kan orsaka ytterligare betydande olägenheter för Helsingfors stads rykte samt påverka hur Helsingfors stad i fortsättningen blir föremål eller väljs ut för olika riktade cyberattacker. Enligt undervisnings- och kulturministeriets uppfattning kan dokumentet i dess offentliga version innehålla en mer allmän och kortare beskrivning eller ett sammandrag av händelseförloppet och de faktorer som lett till det framgångsrika dataintrånget.

Undervisnings- och kulturministeriet konstaterar i punkt 5.1 i rekommendationerna att det utöver det föreslagna kan förekomma praktiska tillämpningsproblem i situationer där personuppgifter behandlas mellan olika förvaltningsområden. Exempel på elevhälsotjänster där man behandlar uppgifter som hör till särskilda kategorier av personuppgifter i genomförandet av både välfärdsområdenas och undervisningsväsendets lagstadgade uppgifter. Lagen om ändring av lagen om elev- och studerandevård (377/2022) har skapat varierande tolknings- och genomförandepraxis, men har också gjort undervisningsväsendets informationssäkerhets- och informationshanteringsmiljö mer komplicerad.

I punkt 5.3 i rekommendationerna konstaterar undervisnings- och kulturministeriet att förslaget om ett mer omfattande samarbete särskilt med undervisnings- och kulturministeriet samt Cybersäkerhetscentret bör understödas. Motsvarande samarbete är också möjligt i fråga om sådana åtgärder som syftar till att förebygga dataintrång eller främja beredskapen för dem. Tydliga ansvar samt verksamhetssätten för kommunikation och rapportering är en väsentlig del av skapandet av en fungerande tväradministrativ lägesbild samt hanteringen av incidenter.

Transport- och kommunikationsverket Traficom har strukturerat sitt utlåtande i fyra helheter, som är de lagstadgade uppgifterna för Cybersäkerhetscentret vid Traficom, Cybersäkerhetscentrets åtgärder i fallet, Cybersäkerhetscentrets cybertjänster samt kommentarer om slutsatserna och säkerhetsrekommendationerna.

Traficom påpekar att dess lagstadgade uppgifter i anslutning till cybersäkerheten endast delvis beskrivs i utkastet till utredningsrapport och i sitt utlåtande redogör man närmare för de lagstadgade uppgifterna samt Traficoms och andra myndigheters inbördes verksamhet och samarbete vid olika cyberincidenter. Dessutom lyfter Traficom fram att samarbetet mellan de myndigheter som utreder informationssäkerhetsincidenter är fungerande och rutinmässigt, men att detta samarbete bör vidareutvecklas och övas.

I sitt utlåtande betonar Traficom att det utöver Cybersäkerhetscentrets operativa cybersäkerhetsuppgifter finns skäl att i utredningsrapporten även beakta de tillsynsuppgifter som hänför sig till cybersäkerheten som finns i 303.1 § i lagen om tjänster inom elektronisk kommunikation (917/2014). Dessutom lyfter Traficom fram att den fungerar som tillsynsmyndighet inom flera sektorer i enlighet med 26 § 1 mom. 1 punkten i den nationella cybersäkerhetslagen, som grundar sig på NIS2-/cybersäkerhetsdirektivet, och 18 h § i informationshanteringslagen.

Traficom konstaterar också att utredningsrapporten ger en felaktig bild av vissa cybersäkerhetstjänster som Cybersäkerhetscentret erbjuder den offentliga sektorn och som preciseras i utlåtandet.

I anslutning till de slutsatser som framförts lyfter Traficom fram att tillsynsmyndighetens uppgifter betonar både proaktivt styrande åtgärder och tillsyn i efterhand. Den proaktiva styrningen har de bästa möjligheterna att med tillsynsmyndighetens tillgängliga resurser nå de organisationer som är föremål för tillsynen. Enligt Traficom är proaktiv styrning ett effektivt tillsynsmedel inom cybersäkerheten. De åtgärder som styr tillsynen utesluter dock inte utnyttjandet av andra tillsynsverktyg. Traficom konstaterar att om tillsynsmyndigheterna hade mångdubbla resurser jämfört med nuläget, kunde man inom olika sektorer fundera på grundläggande förändringar även i tillsynen som genomförs i efterhand och till exempel i inspektionsverksamheten för de organisationer som omfattas av tillsynen. Tillsyns- och styrningsuppgifterna inom cybersäkerhet har i regel tilldelats mycket knappa resurser vid olika myndigheter i Finland.

Traficom instämmer i sitt utlåtande i uppfattningen att även den offentliga sektorns cybersäkerhet och förmåga att svara på hot om olika nätbrott bör utvecklas under de kommande åren. Enligt Traficom förutsätter detta i synnerhet resurser för åtgärder som utvecklar cybersäkerheten och personalen, utbildning och utnyttjande av nödvändiga tekniska metoder. Enligt Traficoms bedömning kan det finnas skäl att satsa betydligt på den offentliga sektorns förmåga att svara på allvarliga statliga hot, men också på hot som orsakas av cyberbrottslingar. Enligt Traficom kan detta till exempel omfatta särskilda satsningar på metoder för att upptäcka och reagera på attacker och sårbarheter, såsom Cybersäkerhetscentrets HAVARO- och Hyöky-tjänster.

Enligt Traficom ansvarar organisationer själv i sista hand för att upprätthålla och utveckla sin egen informationssäkerhet och cybersäkerhet även inom den offentliga sektorn. Traficom betonar att även de processer och metoder för cybersäkerhet som används inom den offentliga sektorn ska granskas på nytt i och med ändringarna i den nya cybersäkerhetslagen och informationshanteringslagen.

Traficom påminner att den nya cybersäkerhetslagen och ändringarna i informationshanteringslagen medför nya skyldigheter även för aktörer inom den offentliga sektorn.

Traficom understöder den föreslagna säkerhetsrekommendationen (rekommendation 5.2), eftersom utvecklingen av förmågan att upptäcka informationssäkerhetsbrister inom den offentliga förvaltningen med tanke på förbättringen av Finlands nationella cybersäkerhet kan anses vara en central åtgärd för ett cybersäkert Finland.

Utbildningsstyrelsen preciserar i sitt utlåtande uppgifterna om de handböcker och anvisningar som den publicerat. Utbildningsstyrelsen betonar att den inte har behörighet att dra upp riktlinjer för tolkningen av dataskyddslagstiftningen, så omfattningen av dess handböcker och stödmaterial beror på den tillgängliga rättspraxisen och tillsynsmyndigheternas avgöranden. Utbildningsstyrelsen föreslår att Utbildningsstyrelsens roll i rekommendationen formuleras så att den motsvarar ämbetsverkets uppgift till exempel så att Utbildningsstyrelsen stöder anordnare av fostran, undervisning och utbildning att utveckla tydliga och tillgängliga anvisningar i kommunikationen i anslutning till dataintrångsfall.

Myndigheten för digitalisering och befolkningsdata konstaterar i sitt utlåtande att det för närvarande finns tillräckligt med bestämmelser för att upprätthålla informationssäkerheten och att den grundläggande lagstiftningen i ärendet är i sin ordning. Enligt dem gäller utmaningarna att känna till bestämmelserna och att resurserna uppfyller kraven till fullo. Enligt

Myndigheten för digitalisering och befolkningsdata är det viktigare att stöda och handleda aktörerna i att uppfylla kraven i författningarna än att öka tillsynen.

Dataombudsmannen fäster i sitt utlåtande uppmärksamhet vid exaktheten i användningen av vissa begrepp och juridiska detaljer och ber att de preciseras. I utlåtandet framförs att alla åtgärder som dataombudsmannens byrå vidtagit i fallet inte framgår av redogörelsen. Dataombudsmannens byrå fäster också uppmärksamhet vid att dataombudsmannen genomför regelbunden tillsynsverksamhet, men att genomförandet av den skulle förutsätta att byrån får mera resurser.

Barnombudsmannen konstaterar i sitt utlåtande att utredningsrapporten är tydlig och detaljerad och ger en utmärkt bild av dataintrånget, utredningen av det, kommunikationen samt slutsatserna och rekommendationerna. Enligt barnombudsmannen finns det i utredningsrapporten ett väl identifierat behov av att informera barn och unga enligt deras ålder om dataintrånget och hur man skyddar sig mot följderna av det samt om skyddet av de egna personuppgifterna. Barnombudsmannen preciserar att det i Finland enligt 5 § i dataskyddslagen (1050/2018) är åldersgränsen för tillhandahållande av informationssamhällets tjänster till barn minst 13 år.

Helsingfors stad anser i sitt utlåtande att utredningen av händelserna i dataintrånget och slutsatserna av det är nyttiga, eftersom uppgifterna i fortsättningen kan användas som stöd för utvecklingen av informationssäkerheten, informationshanteringen och dataskyddet. Helsingfors stad anser att utredningsrapporten har utarbetats på ett förtjänstfullt sätt och att den är omfattande.

Helsingfors stad ansåg att dataintrånget var professionellt, välplanerat och effektivt. Helsingfors stad uppskattar att cirka 150 000 elever och vårdnadshavare samt alla 38 000 anställda vid staden blev offer för dataintrånget.

I sitt utlåtande motiverar Helsingfors stad den valda informationslinjen. I det inledande skedet bedömdes det vara omöjligt att informera alla registrerade personligen, så för informationen tillämpades allmän delgivning vilket dataskyddsförordningen möjliggör. Helsingfors stad meddelade dataombudsmannen sitt avgörande och skickade denne information om de informationsåtgärder som vidtagits. Helsingfors stad betonar att den regelbundet bedömde möjligheterna att informera personligen under dataintrånget och utredningarna i efterhand, men eftersom man inte kunde klarlägga de läckta uppgifterna med tillräcklig noggrannhet ansågs det att det inte fanns tillräckliga förutsättningar för att informera personligen. Dataombudsmannen gav inte heller anvisningar om att agera annorlunda.

Helsingfors stad konstaterar att med beaktande av att utredningen inte är helt färdig anser staden att den externa kommunikationen inte skulle ha kunnat genomföras enligt en snabbare tidtabell. Helsingfors stad framför i sitt utlåtande åsikten att man i praktiken hade gett anvisningar om radering av föråldrade filer på nätdisken, men att iakttagandet av dem inte övervakades.

Enligt Helsingfors stad splittras anskaffningen och utvecklingen av de informationssystem som tjänsterna kräver av såväl de specifika författningarna som den behörighet som tilldelas kommunens olika behöriga tjänsteinnehavare. Ledningen av en modern och datasäker IKT-arkitektur förutsätter att beslutsfattandet om tekniken och kärndatasystemen centraliseras. Därför är det också svårt för de som ansvarar för informationshanteringen att uppfatta kravhelheten och det leder till en varierande tillämpning av dessa.

Helsingfors stad anser att rekommendationerna är nödvändiga, även om de är ganska omfattande, vilket kan göra genomförandet och hanteringen av dem krävande. Helsingfors stad anser att målet att utveckla proaktiv upptäckt och åtgärdande av informationssäkerhetsbrister är motiverat.

Helsingfors stad anser att avsnittet om utveckling av kommunikationsanvisningarna är problematisk, eftersom utvecklingen av kommunens kommunikation enligt 121 § i grundlagen ankommer på kommunerna själva. Myndigheterna kan stöda kommunens uppgift men inte sköta den. Att Kommunförbundet stöder identifieringen och åtgärdandet av informationssäkerhetsbrister samt utvecklingen av informationshanteringen och dataskyddet anser staden vara en mycket bra idé.

I anslutning till skolornas datasäkerhet påminner Helsingfors stad om att elevantalet är stort och att eleverna fortfarande är minderåriga i grundskolan, vilket utgör en betydande utmaning för skolmiljöernas datasäkerhet i synnerhet i större kommuner. Enligt staden har man i utredningsrapporten inte i tillräcklig utsträckning beaktat det perspektivet att utvecklingen av elevernas och studerandenas informationssäkerhetsfärdigheter inte endast handlar om att uppnå målen i läroplanen utan också om att upprätthålla informationssäkerheten i organisationens egna system. Helsingfors stad konstaterar att Utbildningsstyrelsen bör beakta utvecklingen av barnens digitala kompetens i läroplanen samt utarbeta anvisningar om hur informationssäkerheten beaktas i situationer där svaga digitala färdigheter hos eleverna utgör en risk för miljön.

Helsingfors stad konstaterar att skadeståndsfrågorna i anslutning till det omfattande dataintrånget är betydande, eftersom såväl direkt skada som en motiverad rädsla för att personuppgifter eventuellt läcks ut eller kommer att missbrukas kan berättiga till ersättningar. Immateriella skador är lika värdefulla som materiella skador. Därför kan även en liten informationssäkerhetsbrist eller försummelse leda till omfattande och dyra skador. Det är viktigt att skadorna ersätts med stöd av lagen på basis av orsakssamband och påvisad skada så att regleringen eller ersättningspraxisen inte blir övermäktig.

Helsingfors stad föreslår i sitt utlåtande dessutom små preciseringar i händelseförloppet och detaljerna.

DigiHelsinki Oy konstaterar i sitt utlåtande att den har producerat brandväggstjänster enligt tjänstebeskrivningen i ramavtalet och att tjänsten inte innehöll övervakning av datasäkerhetslarm. Enligt utlåtandet hörde ASA 5515 som används i dataintrång inte i något skede till DigiHelsinki och företaget hade inte synlighet till antingen apparaten eller fostrans- och utbildningssektorns intranät. DigiHelsinki hade konkurrensutsatt installationstjästen för kommunikationsutrustningen och enligt det förmedlat certifikatens jouruppdraget, som fostrans- och utbildningssektorn hade beställt, till Dustin Oy för att utföra. DigiHelsinki ansåg att ägandet och underhållet av ASA 5515 hörde till fostrans- och utbildningssektorn. DigiHelsinki också för fram i sitt utlåtande preciseringar gällande hantering av larm från programvara för bekämpning av skadlig programvara och ticketerna.

Kommunförbundet anser i sitt utlåtande att det är nyttigt att dataintrånget mot Helsingfors stad har utretts och att man i samband med det har identifierat säkerhetsrekommendationer för att förebygga motsvarande händelser. Kommunförbundet anser att det är särskilt förtjänstfullt att rapporten i detalj beskriver dataintrångets framskridande och orsakerna till det lyckade dataintrånget. Enligt Kommunförbundet kan beskrivningen utnyttjas som stöd för utvecklingen av kommunernas informationssäkerhet och dataskydd. Kommunförbundet föreslår att man utifrån beskrivningen direkt kan fastställa en detaljerad lista över utvecklingsobjekt för varje organisation.

Kommunförbundet anser att rekommendationerna i rapportutkastet är viktiga. Rekommendationerna anses dock till många delar vara omfattande och allmänna, varvid deras genomförbarhet ifrågasätts. Kommunförbundet betonar i sitt utlåtande betydelsen av god informationshantering för att åtgärderna i anslutning till dataskydd och informationssäkerhet ska vara effektiva och rikta sig mot rätt saker. Förbundet konstaterar att det finns mycket lagstiftning och olika anvisningar, men att de är utspridda och att kommunerna får väldigt lite stöd i tillämpningen direkt från myndigheterna.

Enligt Kommunförbundet borde man fundera på till vilka delar den senaste tidens ökade förståelse av kommunernas roll som en del av den nationella beredskapen samt hur kritiska kommunernas personuppgiftslager är borde synas i de nationella strategierna, verksamhetsplanerna och finansieringsbesluten för cybersäkerheten. Enligt Kommunförbundet är informationshanteringens nuläge inte nödvändigtvis så problematiskt som rapporten låter förstå.

Kommunförbundet lyfter fram att ingen aktör bedömer hur 4 kap. i informationshanteringslagen, dvs. informationssäkerhetskraven, uppfylls. Kommunförbundet anser att det är viktigt att lösa problemet med ovan nämnda lagstiftning och verkställandet av den, så att utvärderingen av verkställandet av 4 kap. i informationshanteringslagen kan inledas och genomföras på lång sikt.

Centralkriminalpolisen föreslår en teknisk korrigering av sin egen organisation i utredningsrapporten. I övrigt hade den inget att uttala sig om.

Justitieministeriet hade inget att uttala sig om i fråga om utredningsrapporten.