

P2024-01 Sammanfattning

Fostrans- och utbildningssektorn vid Helsingfors stad råkade ut för ett allvarligt dataintrång under våren 2024. Angriparen kom åt uppgifter om många elever och anställda. På nätverksdisken fanns också uppgifter om andra personer, företag och samarbetspartners som på något sätt haft kontakt med staden.

Dataintrånget började i mitten av april 2024. Angriparen började undersöka nätverket och lyckades komma åt flera olika servrar. I slutet av april kopierade angriparen ungefär två terabyte (TB) data från nätverksdisken, i fyra omgångar. Man vet inte exakt hur mycket eller vilka uppgifter angriparen kopierat. I utredningen kom man fram till att angriparen fick tag på ungefär 750 000 dokument. I en del av dem fanns det känsliga personuppgifter.

Dataintrånget höll på länge för att organisationen inte övervakade nätverket tillräckligt bra. Man reagerade inte heller i tid på meddelanden om intrånget. När man var säker på att det var frågan om ett dataintrång, tog Helsingfors stad genast till åtgärder och lyckades stoppa intrånget.

Det var två saker som gjorde att angriparen kunde kopiera så mycket data. Hen kunde bryta sig in i systemet via en vpn-server som inte underhållits tillräckligt bra. Det hade också samlats mycket data på nätverksdisken under flera års tid. Det dåliga underhållet berodde på att man gjort förändringar i personalen och organisationen. Därför var det oklart vem som hade hand om vilka uppgifter. Det hade samlats mycket filer på nätverksdisken för att man hanterat informationen dåligt. Man hade inte heller kollat att de som använde disken följde de anvisningar som de fått.

Det finns många lagar om hur man ska hantera information, men de som ska hantera informationen känner ofta inte till lagarna. Det kan vara svårt att förstå lagar och nationella anvisningar, som också kan vara utspridda på olika ställen. Speciellt kommunerna har skyldigheter som kommer från flera olika myndigheter. Då är det svårt att ha koll på helheten.

Efter dataintrånget kom angriparen åt mycket material med personuppgifter. Angriparen kan senare använda uppgifterna på ett skadligt sätt, till exempel för identitetsstöld och bedrägeri. Under utredningen har man inte sett tecken på detta.

Hundratusentals personer drabbades av dataintrånget. Utredningen visade att det var svårt att ta reda på vilka alla offer var. Det gick bra att få tag på personalen som jobbar inom staden, men det var väldigt svårt att få tag på alla gamla anställda och gamla och nuvarande elever. Man försökte inte ens göra detta.

I utredningen ges fyra rekommendationer. De gäller mest Finansministeriet som ansvarar för att de följs tillsammans med Justitieministeriet, Kommunikationsministeriet, Utbildningsstyrelsen och Kommunförbundet.

1. Finansministeriet ansvarar, tillsammans med Justitieministeriet, för att lagarna om hur myndigheter hanterar information passar ihop och att det blir tydligt vem som övervakar och styr detta.
2. Finansministeriet och Kommunikationsministeriet ska ta reda på hur man kan bli bättre på att märka problem med datasäkerheten inom den offentliga sektorn i hela landet. De ska också se till att myndigheterna har tillräckliga möjligheter att hitta och åtgärda dessa problem.
3. Finansministeriet och Utbildningsstyrelsen ska se till att kommunerna och städerna gör tydliga och tillgängliga instruktioner om hur de ska meddela om dataintrång som sker. Då kan de som drabbats skydda sig mot följder av intrång och skydda sina personuppgifter.

4. Finansministeriet och Kommunförbundet ska hjälpa kommunerna i att hitta och lösa stora problem med datasäkerheten. De ska också hjälpa till med att förbättra säkerheten för information och data.