خلاصه P2024-01

در بهار سال 2024 بخش آموزش و پرورش شهرداری هلسینکی Helsinki (KASKO) مورد یک حمله جدی سایبری قرار گرفت. در نتیجه این نفوذ حجم زیادی از اطلاعات مربوط به دانش‌آموزان و کارمندان به دست نفوذگر افتاد. علاوه بر این در اسناد موجود در فضای ذخیره سازی شبکه‌ای اطلاعات سایر افرادی که به طور مستقیم یا غیر مستقیم با شهرداری همکاری یا ارتباط داشته‌اند از جمله اشخاص حقیقی، شرکت‌ها و سایر نهادهی همکاری نیز وجود داشته است.

نفوذ سایبری در اواسط آوریل 2024 آغاز شد، پس از آن نفوذگر شروع به شناسایی اهداف در شبکه داخلی کرد و دسترسی خود را به سرورهای مختلف گسترش داد. در پایان ماه آوریل، نفوذگر در چهار مرحله مجموعاً حدود دو ترابایت اطلاعات را از فضای ذخیره سازی شبکه‌ای کپی کرد. تعداد دقیق فایل‌ها یا محتوای آنها قابل شناسایی نبوده است. در جریان تحقیقات، برآورد شده است که نفوذگر حدود 000 750 سند را به دست آورده است که بخشی از آن‌ها حاوی اطلاعات شخصی حساس بوده‌اند.

نفوذ سایبری برای مدت طولانی ادامه داشته است، زیرا نظارت بر شبکه در سازمان ناکارآمد بوده و به هشدارهای دریافت شده به موقع واکنشی نشان داده نشده است. پس از آن که وقوع نفوذ تأیید شده است، شهرداری هلسینکی Helsinki بلافاصله اقدامات مدیریتی و اصلاحی را آغاز کرد که با کمک آن ها حمله متوقف گردید.

کپی حجم وسیعی از اطلاعات به دو عامل امکان پذیر شده است: نفوذ به سامانه اطلاعاتی از طریق یک سرور اتصال از راه دور (VPN) با نگهداری نامناسب صورت گرفته است؛ در طول سال ها حجم زیادی اطلاعات روی فضای ذخیره سازی شبکه جمع شده بوده است. نگهداری نامناسب به دلیل تغییرات در نیروی انسانی و سازمان رخ داده است که منجر به نامشخص شدن مسئولیتها شود. فایل ها روی فضای ذخیره سازی شبکه انباشته شدند، زیرا مدیریت اطلاعات ناقص بوده و رعایت دستورالعمل های استفاده از دیسک به درستی نظارت نمی شده است.

قوانین و مقررات متعددی در رابطه با مدیریت اطلاعات وجود دارد، اما آگاهی از آنها در بین متخصصان اغلب نا کافی می باشد. قوانین و دستورالعمل‌های ملی تا حدودی نا مشخص و پراکنده هستند. بخش شهرداری به طور ویژه مشمول تعهداتی است که توسط چندین نهاد دولتی مختلف اعمال می‌شود که این موضوع مدیریت کلی را دشوار می‌کند.

در نتیجه نفوذ سایبری، مقدار زیادی از اطلاعات شخصی به دست نفوذگر افتاده است. این اطلاعات ممکن است بعداً برای اهداف مخرب مانند سرقت هویت و کلاهبرداری استفاده شود. در طول تحقیقات، هیچ نشانه‌ای مبنی بر وقوع این موارد مشاهده نشده است.

صدها هزار نفر قربانی نفوذ سایبری شدند. تحقیقات نشان داده است که شناسایی کامل همه قربانیان دشوار بوده است. ارتباط با کارمندان شاغل در شهرداری به خوبی انجام گرفته است، اما شناسایی و تماس با کارمندان سابق، دانش‌آموزان سابق و فعلی عملاً بسیار دشوار بوده و حتی تلاش خاصی برای این کار صورت نگرفته است.

این تحقیق چهار توصیه ارائه می دهد. این دستورالعمل ها عمدتاً خطاب به وزارت دارایی هستند که مسئول اجرای آنها با همکاری وزارت دادگستری، وزارت حمل و نقل و ارتباطات، اداره ملی آموزش و پرورش و انجمن مقامات محلی و منطقه‌ای می باشد.

1. وزارت دارایی، با همکاری وزارت دادگستری، هماهنگی قوانین مربوط به مدیریت اطلاعات در ادارات دولتی و شفاف سازی ساختارهای نظارتی و کنترلی آن را تضمین خواهد کرد.

2. وزارت دارایی، با همکاری وزارت حمل و نقل و ارتباطات، بررسی خواهد کرد که چگونه می توان تشخیص آسیب پذیری های امنیت اطلاعات در مدیریت عمومی را در سطح کشور بهبود بخشید و اطمینان حاصل کند که نهادهای عمومی از قابلیت های کافی برای شناسایی و اصلاح آسیب پذیری های امنیت اطلاعات برخوردارند.

3. وزارت دارایی فنلاند با همکاری اداره ملی آموزش و پرورش اطمینان حاصل می‌کند که شهرداری ها و شهرها دستورالعملی روشن و قابل دسترس برای اطلاع رسانی در مورد موارد نفوذ سایبری تهیه کنند، تا قربانیان بتوانند در برابر پیامدهای این نفوذهای سایبری از خود محافظت کرده و از اطلاعات شخصی خود مراقبت نمایند.

4. وزارت دارایی، با همکاری انجمن شهرداری ها، از شهرداری ها در شناسایی و رفع کمبودهای حیاتی امنیت اطلاعات حمایت می‌کند و همچنین مدیریت اطلاعات و مدیریت ریسک امنیت اطلاعات را توسعه می‌دهد.