(ترجمانی از زبان فنلندی)

P2024-01 خلاصه

در بهار سال 2024، یک هک یا نفوذ معلوماتی جدی بر روی خدمات تعلیم و تربیت شاروالی هلسینکی (KASKO) انجام شد. در نتیجه این هک معلوماتی، مقدار زیادی معلومات دانش آموزان و کارکنان به دست اشخاصی که این هک معلوماتی را انجام داده بودند افتاد. علاوه بر این، در اسناد و مدارک موجود در دیسک یا درایو شبکه، معلومات مربوط به اشخاص، شرکت ها و کمپنی ها و مؤسسه های دیگری که بطور غیر مستقیم یا مستقیم با شاروالی همکاری می کردند و ارتباط داشتند، وجود داشته است.

این هک معلوماتی در اواسط ماه آوریل 2024 شروع شد که بعد از آن، شخص هکر شروع به بررسی هدف های شبکه داخلی و گسترش دسترسی خود به سرورهای مختلف را نمود. در اواخر ماه آوریل، شخص هکر در چهار نوبت، مجموعاً تقریباً دو ترابایت معلومات از دیسک شبکه کاپی کرد. امکان تشخیص مقدار یا محتوای دقیق فایل ها وجود نداشته است. در تحقیقات، این ارزیابی نتیجه گیری شد که شخص هکر تقریباً 750000 مدرک و سند بدست آورد که بخشی از آنها شامل معلومات شخصی حساس بوده اند.

این هک معلوماتی مدت طولانی ادامه پیدا کرد، چون که نظارت بر شبکه سازمان دچار نقص بود و به آگهی های مشاهده شده سر وقت واکنش نشان داده نشد. بعد از این که از این هک معلوماتی اطمینان حاصل شد، شاروالی هلسینکی بلافاصله اقدامات کنترل و تصحیح را آغاز کرد که از طریق آنها، این هک متوقف گردید.

دو چیز کاپی کردن این مقدار عظیم معلومات را امکان پذیر نمود: هک کردن سیستم معلوماتی از طریق سرور اتصال از راه دور وی پی ان که از آن بطور ناقص نگهداری می شد انجام گردید و دیسک شبکه شامل معلومات بسیار زیادی بود که در مدت چندین سال در آن جمع آوری شده بودند. نگهداری ناقص ناشی از تغییرات کارکنان و سازمان بود که در نتیجه آنها، مسئولیت ها نامشخص شدند. به دلیل وجود نقص در مدیریت معلومات، فایل ها در دیسک شبکه جمع آوری شده بودند و نظارتی بر روی رعایت طرزالعمل های داده شده برای استفاده از دیسک وجود نداشت.

مدیریت معلومات شامل چندین قانون و آئین نامه می شود، ولی آشنایی اشخاصی که کار عملی انجام می دهند اغلب با این قوانین و آئین نامه ها دچار کمبود است. توضیحات مربوط به قانونگذاری و طرزالعمل های سراسری بخشاً دشوار و پراکنده هستند. بویژه شاروالی ها باید وظایفی که از طرف مسئولین اداری مختلف متعددی تعیین می شوند را رعایت کنند که در چنین مواردی مدیریت و کنترل کلیت دشوار می گردد.

در نتیجه این هک معلوماتی، مقدار زیادی اسناد و مدارکی که شامل معلومات اشخاص می شدند، به دست شخص هکر افتاد. از این معلومات ممکن است در آینده بتوان به مقاصد زیانبار، مانند سرقت هویتی و فریبکاری و شیادی استفاده نمود. در زمان تحقیقات، علائم و نشانه هایی در این مورد مشاهده نشد.

اشخاصی که قربانی این هک معلوماتی شده اند، صدها هزار نفر بودند. تحقیقات نشان داد که بررسی و مشخص کردن جامع همه اشخاص قربانی دشوار بود. در ارتباط با کارکنانی که برای شاروالی کار می کنند، دسترسی به این اشخاص بخوبی انجام شد، ولی دسترسی جامع به کارکنان و دانش آموزان قبلی و دانش آموزان فعلی عملاً بسیار دشوار بود و اصلاً تلاشی هم برای انجام آن صورت نگرفت.

در این تحقیقات چهار توصیه انجام می شود. این توصیه ها عمدتاً مربوط به وزارت مالیه می شوند که در همکاری با وزارت عدلیه، وزارت ترانسپورت و ارتباطات و وزارت معارف، همراه با اتحادیه شاروالی ها، مسئولیت اجرای آنها را بر عهده دارد.

1. وزارت مالیه در همکاری با وزارت عدلیه اطمینان حاصل کند که قانونگذاری مربوط به مدیریت معلومات بخش دولتی و حاکمیت عمومی هماهنگ گردد و ساختار نظارتی و راهبردی آن روشن و مشخص شود.
2. وزارت مالیه در همکاری با وزارت ترانسپورت و ارتباطات بررسی کند که چگونه می توان مشاهدات مربوط به نواقص و کمبودهای امنیت معلومات بخش دولتی و حاکمیت عمومی را بطور سراسری بهبود بخشید و اطمینان حاصل نمود که کارکنان و فعالین بخش دولتی و حاکمیت عمومی توانایی کافی برای مشاهده و اصلاح نواقص و کمبودهای امنیت معلومات را داشته باشند.
3. وزارت مالیه در همکاری با وزارت معارف اطمینان حاصل کند که شاروالی ها برای اطلاع رسانی در مورد هک های معلوماتی، طرزالعمل روشن و قابل دسترسی ایجاد کنند که با کمک آن اشخاص قربانی بتوانند از عواقب هک معلوماتی در امان باشند و از معلومات شخصی خود حفاظت کنند.
4. وزارت مالیه در همکاری با اتحادیه شاروالی ها در شناسایی و تشخیص و اصلاح نواقص و کمبودهای بحرانی امنیت معلومات به شاروالی ها کمک کند و برای مدیریت معلومات و امنیت معلومات، مدیریت ریسک طراحی و ایجاد کند.

(ترجمانی از زبان فنلندی)