حمله سایبری به شهرداری هلسینکی HELSINKI نشان می‌دهد که مقابله با چنین حملاتی نیازمند رویکردی جدید و متفاوت در زمینه آمادگی، ارتباطات و پیشگیری در بخش دولتی است

در ژوئیه 2024، شورای دولت گروه تحقیقاتی مستقلی را در چارچوب مرکز تحقیقات سوانح فنلاند (OTKES) منصوب کرد تا به بررسی حمله سایبری بپردازد که در بهار 2024 شهرداری هلسینکی Helsinki را هدف قرار داد. برآورد می‌شود که حدود 300 000 نفر قربانی این حمله سایبری شده‌اند، که این حمله را به بزرگ ترین حمله سایبری اطلاعاتی در تاریخ فنلاند تبدیل می‌کند. گروه تحقیقاتی بررسی‌های ایمنی را به پایان رسانده و گزارش نهایی تحقیقاتی خود را در تاریخ[1] 17.6.2025 به شورای دولت ارائه کرده است.

جرایم سایبری حوزه‌ای رو به رشد از فعالیت‌های مجرمانه هستند و آسیب های ناشی از آن‌ها، به ویژه در شرایط کنونیِ تهدیدات ترکیبی، قابل توجه و چشمگیری می باشد. بخش دولتی به دلیل کیفیت و حجم بالای اطلاعاتی که در اختیار دارد، هدفی جذاب برای مجرمان به شمار می‌آید. با این حال، بخش عمومی هنوز در مقابله با تهدیدات ناشی از جرایم سایبری نیازمند توسعه و بهبود است، چرا که روش‌های شناسایی حملات و آسیب پذیری‌ها به اندازه کافی به‌طور گسترده مورد استفاده قرار نگرفته‌اند.

مدیریت اطلاعات، امنیت سایبری و حفاظت از داده‌های بخش دولتی توسط چندین نهاد نظارتی مختلف هدایت می‌شود. این نهادها به طور مستقل و بر اساس وظایف خاص خود اقدام به نظارت و راهبری می‌کنند. راهبری ارائه شده به واحدهای مدیریت داده‌ها پراکنده غیر تمرکز و در عمل، اجرای قوانین و دستورالعمل‌ها ناپیوسته و متفاوت است. علاوه بر این، فعالیت های انجام شده توسط نهادهای نظارتی بیشتر جنبه هدایت دارند و نظارت بر عملکرد فعالان کمتر صورت می‌گیرد. با این حال، مدیریت چرخه عمر اطلاعات از اهمیت بالایی در زمینه امنیت اطلاعات و حفاظت از داده‌ها برخوردار است. توانمندی های بخش دولتی برای مقابله با تهدیدات سایبری را می‌توان با توسعه و گسترش روش‌های شناسایی حملات و آسیب پذیری‌ها تقویت کرد.

"آمادگی برای رویدادهایی مانند نفوذهای سایبری و مقابله با آنها ما را از جهات مختلف در موقعیتی جدید قرار می‌دهد: در فنلاند، همکاری بین نهادهای دولتی به‌طور سنتی امری معمول و رایج بوده است. در رویدادهای سایبری، اقدامات مقابله‌ای به صورت پراکنده و غیر متمرکز انجام می‌شود. در عین حال، بررسی و مدیریت موارد نفوذ سایبری تا حد زیادی به تخصص و دسترسی فعالان بخش خصوصی وابسته است. به عنوان مثال، مکانیسم همکاری مشابه [2]فعالیت‌های جستجو و نجات (SAR) برای موارد نفوذ سایبری تعریف نشده است. بسیاری از مسئولیت‌ها نیز بر عهده خود قربانیان باقی می‌ماند. می گوید هانا تییرینکی Hanna Tiirinki، رئیس گروه تحقیق.

"تعریف قربانی نیز نیازمند بازنگری است. ما تقریباً بدون اینکه متوجه باشیم، هر روز از پایگاه‌های داده و خدمات مختلفی استفاده می‌کنیم. در اختیار مدیریت محلی، اطلاعات شخصی متنوعی از ما وجود دارد. در حوادث سایبری، مهاجم ممکن است حجم زیادی از داده‌ها را برای استفاده در آینده ذخیره کند. آنچه که آسیب پذیری اصلی برای قربانیان ایجاد می‌کند، ترکیب این داده‌ها با یکدیگر است. «در حملات سایبری همواره باید این خطر را در نظر گرفت که داده‌ها ممکن است در آینده برای مقاصد زیان‌بار، مانند سرقت هویت یا کلاهبرداری، مورد استفاده قرار گیرند – و برای مثال، جوانان لزوماً درک روشنی از این ندارند که ممکن است چه بر سر اطلاعات آنها بیاید زمانی که به سن قانونی می‌رسند"، تییرینکی Tiirinki اضافه می‌کند.

قانون ملی امنیت سایبری در تاریخ 8.4.2025 به اجرا درآمد. اجرای ملی دستورالعمل امنیت شبکه و اطلاعات (NIS2) بخشی از اجرای این قانون امنیت سایبری است. با این حال، در فنلاند، شهرداری‌ها و شهرها دارای خودگردانی گسترده‌ای هستند و دستورالعمل NIS2 شامل حال آنها نمی‌شود.

تییرینکی Tiirinki اضافه می‌کند: *" دستورالعمل NIS2 در فنلاند شامل سطح مدیریت محلی نمی‌شود. با توصیه هایی که در این تحقیق ارائه کرده‌ایم، تلاش داریم تا حدی این خلأ را جبران کنیم" .*

---

[1]تحقیق درباره رویدادهای استثنایی طبق قانون، تحقیق درباره رویدادهای استثنایی می‌تواند شامل حوادثی بسیار جدی باشد که منجر به مرگ شده یا به طور جدی تهدیدکننده یا آسیب‌زننده به عملکردهای اساسی جامعه بوده و در عین حال به عنوان حادثه شناخته نشود. قانون تحقیق امنیتی شماره 2011/525.

[2]جستجو و نجات، عملیات جستجو و نجات

دستورالعمل NIS2 سازمان‌ها را موظف می‌کند که ظرف 24 ساعت اطلاع رسانی انجام دهند. در موارد نفوذ اطلاعاتی، ارتباطات بخش حیاتی اقدامات حفاظتی است. ارتباط مؤثر باعث کاهش ابهام، جلوگیری از انتشار اطلاعات نادرست و تضمین دریافت حمایت‌های لازم توسط قربانیان می‌شود. دسترسی پذیری، گستردگی و قابل فهم بودن پیام‌های ارتباطی از اهمیت بالایی برخوردار است.

تییرینکی Tiirinki تأکید می‌کند: *"همچنین، باید به گروه‌های هدفی مانند کودکان و نوجوانان توجه ویژه داشت – و با آنها باید متناسب با سن‌شان ارتباط برقرار شود. یکی از ویژگی‌های اساسی ارتباطات در بحران‌ها و شرایط اضطراری این است که اغلب باید با اطلاعات ناقص آغاز کرد – چرا که تصویر کلی از وضعیت به تدریج کامل می‌شود. این نقص اولیه در اطلاعات نباید مانعی برای اطلاع رسانی باشد".*

تییرینکی Tiirinki تأکید می‌کند: *"لازم به ذکر است که فعالان بخش محلی بسیار متنوع هستند و نمی‌توان آنها را با یک معیار واحد سنجید. برخی از آن‌ها آمادگی بسیار خوبی دارند – در حالی که برخی دیگر هنوز نیاز به پیشرفت دارند. فنلاند در مقایسه های بین‌المللی از نظر آمادگی عملکرد بسیار خوبی دارد. پس از رخدادهای نفوذ اطلاعاتی، ما نیز نسبت به این مسئله آگاه‌تر شده‌ایم و اقدامات اصلاحی آغاز شده است. بنابراین، تلاش‌های زیادی برای پیشگیری و مقابله با رویدادهایی مشابه نفوذهای اطلاعاتی در حال انجام است".*

در این تحقیق، چهار توصیه ارائه شده است. این توصیه‌ها عمدتاً متوجه وزارت دارایی فنلاند هستند که مسئول اجرای آنها در همکاری با وزارت دادگستری، وزارت حمل‌و نقل و ارتباطات، اداره آموزش ملی و انجمن شهرداری‌ها می باشد. علاوه بر توسعه دستورالعمل های ارتباطی، این توصیه‌ها شامل هماهنگ سازی مدیریت داده‌ها، نظارت بر آن و ارائه دستورالعمل های مربوطه نیز می‌شوند. همچنین، این توصیه‌ها به بهبود شناسایی نواقص امنیت اطلاعات در بخش دولتی و تقویت توانایی آن برای شناسایی و اصلاح این نواقص می‌پردازند.

نظر مقام مسئول امنیت سایبری ملی:

مرکز امنیت سایبری(KTK) : **"** به عنوان مقام ملی مسئول امنیت سایبری، ما به شرکت‌ها، سازمان‌ها و شهروندان کمک و راهنمایی می‌کنیم تا بتوانند تهدیدهای سایبری کنونی و آینده را شناسایی و برای آن‌ها آماده شوند. مرکز امنیت سایبری ترافیکوم از همان ابتدا که حمله سایبری به شهرداری هلسینکی مشخص و گزارش شد، به طور گسترده‌ای از شهرداری حمایت کرده و همچنان همکاری خود را با شهرداری و ارائه دهندگان خدمات ادامه می‌دهد**"**، ساموئلی برگستروم Bergström، مدیر مرکز امنیت سایبری ترافیکوم می‌گوید. **"**در حملات سایبری، اهمیت اطلاع رسانی و ارتباطات بیش از پیش مشهود است. در دستورالعمل مدیریت بحران با عنوان **"**چگونه درباره حملات سایبری اطلاع رسانی کنیم**"** که توسط ترافیکوم در بهار 2025 منتشر شده است، انواع مختلف حملات سایبری و روش‌ها و تکنیک های مجرمان توضیح داده شده است. همچنین در این دستورالعمل نکاتی برای آمادگی در زمینه ارتباطات و نحوه اطلاع رسانی در طول حمله سایبری و پس از آن ارائه شده است**"**، برگستروم Bergström اضافه می‌کند.

سایر تحقیقات مرتبط با حمله سایبری به شهرداری هلسینکی Helsinki:

پلیس جنایی مرکزی (KRP)

پلیس جنایی مرکزی (KRP) مسئول تحقیقات مقدماتی درباره نقض امنیت داده‌های شهرداری هلسینکی Helsinki است. این نقض به عنوان جرم سنگین نفوذ غیرمجاز به داده‌ها در حال بررسی است. همچنین، KRP در تحقیقی جداگانه بررسی می‌کند که آیا شهرداری اقدامات حفاظتی لازم را به‌طور مناسب انجام داده است یا خیر. در این تحقیق، عنوان اتهامی نقض احتمالی قوانین حفاظت از داده‌ها مطرح است.

دفتر نظارت بر حفاظت از داده‌ها(TSV)

دفتر نظارت بر حفاظت از داده‌ها (TSV) در حال بررسی نقض اطلاعات شخصی است که احتمال دارد ناشی از یک حمله سایبری بوده باشد. این بررسی با هدف بررسی رعایت قوانین مربوط به حفاظت از داده‌ها انجام می‌شود. در این بررسی مشخص می‌شود که آیا شهرداری هلسینکی Helsinki اقدامات امنیتی کافی برای محافظت از داده‌های افراد انجام داده و آیا به درستی از حقوق کسانی که اطلاعات‌شان فاش شده حمایت کرده است یا نه. تحقیقات همچنان ادامه دارد و اطلاعات و توضیحاتی که شهرداری هلسینکی Helsinki درباره این اتفاق ارائه داده، در حال بررسی است.

از کجا کمک بگیریم؟

سازمان خدمات قربانیان جرم (RIKU) در وب سایت خود راهنمایی‌هایی برای افرادی که قربانی حمله سایبری یا نشت اطلاعات شخصی شده‌اند منتشر کرده است. در این وب سایت تأکید شده که بسیار مهم است افراد از دستورالعمل‌های مقامات رسمی پیروی کرده و اقدامات لازم را برای محافظت از اطلاعات شخصی خود انجام دهند، تا از سوءاستفاده یا کلاهبرداری با استفاده از این اطلاعات جلوگیری شود. ریکو RIKU همچنین امکان گفت وگو و دریافت حمایت عاطفی و روانی را فراهم می‌کند. این خدمات برای همه رایگان هستند.

اطلاعات بیشتر:

رئیس تیم تحقیقات، هانا تیرینکی، تلفن: 02951 50747، etunimi.sukunimi@om.fi

همچنین، تلفن: 02951 50738 یا 050345 1931. ارتباط تلفنی تا 1.8.2025 برقرار است. علاوه بر این، هرگونه سؤالی را می‌توان از طریق ایمیل به viestintä.otkes@om.fi ارسال کرد.

پس از 1.8.، از شما می‌خواهیم که هرگونه سؤالی را به آدرس ایمیلviestinta.otkes@om.fi یا مستقیماً به رئیس تیم تحقیقات ارسال کنید.