(ترجمانی از زبان فنلندی)

هک یا نفوذ معلوماتی که بر روی شاروالی هلسینکی انجام شده است نشان می دهد که هک های معلوماتی نیاز به اقدامات جدید در آماده بودن و ارتباطات در بخش عمومی و دولتی و همچنین در دفع هک معلوماتی دارد

هیئت دولت در ماه جولای سال 2024 یک گروه تحقیقاتی مستقل در مرکز تحقیقات حوادث (Onnettomuustutkintakeskus، OTKES) تشکیل داد تا هک معلوماتی که در بهار 2024 بر روی شاروالی هلسینکی انجام شده بود را بررسی کند. اشخاصی که قربانی این هک معلوماتی شده اند، تقریباً 000 300 نفر هستند که به این دلیل این هک معلوماتی بزرگترین نوع آن در فنلند بوده است. این گروه تحقیقاتی تحقیقات امنیتی را انجام داده و تمام کرده است و پرونده این تحقیقات در تاریخ 2025/6/17 به هیئت دولت تحویل داده شده است1.

جرایم سایبری یا جرایم اینترنتی رشته ای از جرایم هستند که در حال رشد می باشند و آسیب هایی که وارد می کنند، بویژه در شرایط تهدیدهای ترکیبی امروزی، بسیار مهم می باشند. بخش دولتی و حاکمیت عمومی، به این دلیل که از شیوه های مشاهده حملات و آسیب پذیری به گستردگی کافی استفاده نمی شود، هنوز باید واکنش خود به تهدیدهای جرایم سایبری را توسعه دهد.

مسئولین اداری متعددی مدیریت معلومات، امنیت معلومات و حفاظت از معلومات بخش دولتی و حاکمیت عمومی را مدیریت و هدایت می کنند. مسئولین اداری این مدیریت و هدایت را بطور مستقل و بر اساس وظایف کاری خود انجام می دهند. راهنمایی که به واحدهای مدیریت معلومات داده می شود، پراکنده و غیر متمرکز هستند و بکار بردن قوانین و مقررات و طرزالعمل ها در عمل متفاوت و متغیر است. کاری که مسئولین اداری انجام می دهند، راهنمایی و مدیریت است، ولی نظارت بر کار فعالین کم و ناچیز است. با این حال، از نظر امنیت معلومات و حفاظت از معلومات، دقیقاً مدیریت چرخه عمر معلومات مهمترین عامل است. آمادگی بخش عمومی و دولتی برای واکنش نشان دادن به تهدیدهای اینترنتی را می توان با توسعه و گسترش دادن شیوه های مشاهده حملات و آسیب پذیری، تقویت نمود.

هانا تیرینکی (Hanna Tiirinki) مدیر گروه تحقیقاتی، چنین می گوید: *"آماده بودن برای وقایع مشابه با هک معلوماتی و دفع آنها، ما را به چند لحاظ در شرایط جدید قرار می دهد: مردم در فنلند بطور سنتی به فعالیت مشترک بین مسئولین اداری عادت کرده اند. اقدامات دفع کننده در رویدادهای سایبری پراکنده و غیر متمرکز می باشند. با این حال، همزمان بررسی و روشن نمودن موارد هک معلوماتی به هر حال تا حد زیادی وابسته به کارشناسی و در دست بودن فعالین بخش خصوصی است. به عنوان مثال، مکانیسم های فعالیت مشترک شبیه امور 2SAR برای این موارد هک معلوماتی تعریف نشده اند. بخش زیادی از مسئولیت هم بر دوش خود شخص قربانی باقی می ماند"*.

تیرینکی (Tiirinki) چنین ادامه می دهد: *"تعریف خود شخص قربانی هم نیاز به تفکر مجدد دارد. ما تقریباً بدون این که خودمان متوجه باشیم، تقریباً هر روز از پایگاه معلوماتی و خدمات مختلفی استفاده می کنیم. نهادهای مدیریتی محلی معلومات شخصی مختلفی از ما در اختیار دارند. شخص هکر رویدادهای سایبری می تواند معلومات زیادی از ما را برای استفاده در آینده ذخیره کند. دقیقاً همین معلومات ترکیبی در مورد اشخاص قربانی ، آسیب پذیری محسوب می شود. در هک های معلوماتی باید همیشه این موضوع را تشخیص داد که معلومات را می توان در آینده برای مقاصد مختلفی نظیر سرقت هویتی و فریبکاری مورد استفاده قرار داد و مثلاً نوجوانان لزوماً نمی توانند فکر کنند که وقتی آنها به سن بزرگسالی می رسند، برای معلومات آنها چه اتفاقی می افتد"*.

قانون امنیت سایبری در تاریخ 2025/4/8 به اعتبار در آمد. اجرای سراسری مقررات امنیت اینترنتی و معلوماتی NIS2 بخشی از اجرای قانون امنیت سایبری است. با این حال، شاروالی ها در فنلند از خودمختاری گسترده ای برخوردار هستند و نفوذ مقررات امنیت اینترنتی NIS2 تا شاروالی ها نمی رسد.

تیرینکی (Tiirinki) اضافه می کند که *"نفوذ مقررات NIS2 در فنلند تا نهادهای مدیریتی محلی نمی رسد. ما تلاش می کنیم که با توصیه هایی که در تحقیقات ارائه می شوند، این حفره را تا حدی پر کنیم"*.

NIS2 سازمان ها را موظف می کند که ارتباطات شبانه روزی برقرارکنند. در موارد هک معلوماتی، ارتباطات بخش مهمی از کار حفاظتی را تشکیل می دهند. ارتباطات عدم اطمینان را کاهش می دهد، از پخش شدن معلومات اشتباه جلوگیری می کند و اطمینان حاصل می کند که اشخاص قربانی کمک مورد نیاز خود را دریافت کنند. قابل دسترس بودن، جامع بودن و قابل فهم بودن ارتباطات از اهمیت ویژه ای برخوردار است.

---

1 تحقیقات در مورد واقعه استثنایی می تواند بر مبنای قانون مربوط به واقعه بسیار جدی منجر به مرگ یا واقعه ای که امور اولیه و پایه جامعه را مورد تهدید قرار می دهد و یا واقعه ای که بطور جدی موجب صدمه و آسیب شده است باشد که اتفاقی نبوده است قانون تحقیقات امنیتی 525/2011.

2 Search and Rescue، جستجو و نجات

تیرینکی (Tiirinki) تأکید می کند که *"علاوه بر این، مثلاً اطفال و نوجوانان منحیث گروه مخاطب و همچنین ارتباط گیری با آنها مطابق با سنشان باید مورد توجه قرار گیرد. ارتباطات زمان بحران و ارتباطات زمان اختلال شامل این می شوند که معمولاً در چنین شرایطی باید با معلومات کمی دست به اقدام زد، چون که تصویر شرایط مدام تکمیل می شود، این معلوماتی که در ابتدا ناقص بوده است نباید مانع اطلاع رسانی شود"*.

تیرینکی (Tiirinki) تأکید می کند که *"باید اضافه کرد که فعالین بخش محلی بسیار متفاوت هستند و با یکدیگر قابل مقایسه نیستند. بعضی از آنها خود را بسیار خوب آماده کرده اند، بعضی دیگر باید هنوز تلاش کنند تا به دیگران برسند. فنلند در عرصه بین المللی در آماده بودن در مقام بسیار خوبی قرار دارد. بعد از هک های معلوماتی هم ما شروع به توجه کردن به مشکل نموده ایم و حل کردن مشکلات را آغاز نموده ایم. یعنی این که همین حالا برای جلوگیری و دفع رویدادهای هک معلوماتی کارهای زیادی در حال انجام شدن است"*.

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. علاوه بر توسعه راهنمایی ارتباطالت، این توصیه ها در ارتباط با هماهنگ کردن مدیریت معلومات، نظارت بر آن و راهنمایی کردن آن است. علاوه بر این، با این توصیه ها در بهبود مشاهده کمبودها و نقص های امنیت معلومات بخش دولتی و حاکمیت عمومی و بهبود این توانایی که کمبودها و نقص های امنیت معلومات را بتوان مشاهده نمود و آنها را اصلاح کرد، مداخله شده است.

توضیح مسئول امنیت اطلاعات ملی:

مرکز امنیت سایبری (KTK): به گفته مدیر مرکز امنیت سایبری ترافی کوم (Traficom)، ساموﻟی برگستروم (Samuli Bergström) "ما در جایگاه مسئولین اداری امنیت معلومات ملی، به کمپانی ها، مسئولین و شهروندان کمک می کنیم تا برای تهدیدات سایبری کنونی و آینده، آماده باشند و آنها را تشخیص دهند. مرکز امنیت سایبری ترافی کوم از همان لحظه مشاهده هک معلوماتی بطور گسترده به شاروالی هلسینکی کمک کرده است و ما به همکاری با شاروالی و ارائه کنندگان خدمات ادامه می دهیم. در حمله سایبری، اهمیت ارتباطات برجسته می شود. در طرزالعمل ارتباطات موارد بحرانی "چگونه در مورد حملات سایبری باید اطلاع رسانی نمود" که ترافی کوم در بهار سال 2025 تولید کرده است، در مورد حملات مختلف سایبری و شیوه ها و راه هایی که مجرمین از آنها استفاده می کنند، توضیح داده شده است. علاوه بر این، در این طرزالعمل راهنمائی هایی در مورد آماده شدن برای ارتباط گیری و همچنین آماده شدن برای اطلاع رسانی در زمان حمله سایبری و بعد از آن ارائه شده است".

تحقیقات دیگر در ارتباط با هک معلوماتی شاروالی هلسینکی:

پلیس مرکزی جنایی (KRP): KRP مسئولیت تحقیقات در مورد هک معلوماتی که بر روی شاروالی هلسینکی انجام شده است، بر عهده پلیس مرکزی جنایی است. این هک معلوماتی منحیث هک معلوماتی شدید و سنگین مورد بررسی و تحقیق قرار گرفته است. علاوه بر این، KRP در یک تحقیقات مقدماتی دیگر این موضوع را مورد بررسی قرار می دهد که آیا شاروالی بطور مناسب از معلومات حفاظت کرده است یا خیر. نام جرم در این بخش از تحقیقات، ظن به جرم حفاظت از معلومات است.

اداره نماینده حفاظت از معلومات (TSV) نقض های امنیت معلوماتی که بر روی اشخاص انجام شده است را از نقطه نظر مقررات و قوانین رعایت حفاظت از معلومات مورد بررسی قرار می دهد. در این بررسی بویژه این موضوع مورد ارزیابی قرار می گیرد که آیا شاروالی هلسینکی از اقدامات محافظتی کافی استفاده کرده است و آیا حقوق اشخاصی که قربانی این نقض شده اند را در نظر گرفته است. این تحقیقات در حال انجام است و اکنون توضیحات دریافت شده از شاروالی هلسینکی در مورد واقعه، در این تحقیقات در دست بررسی هستند.

از کجا می توان کمک دریافت نمود؟

مرکز کشیک قربانیان جرم (RIKU) در صفحات اینترنتی خود راهنمائی هایی برای اشخاصی که قربانی هک معلوماتی و درز معلومات شده اند، منتشر کرده است. در این صفحات تأکید می شود که مهم است که طرزالعمل های مسئولین اداری انجام شوند و اقدامات مربوط به بستن حساب ها را انجام داد تا از معلومات شخصی برای انجام جرم استفاده نشود. RIKU از طریق گفتگو و صحبت، کمک هم ارائه می کند. این خدمات رایگان هستند.

معلومات بیشتر:

هانا تیرینکی (Hanna Tiirinki) مدیر گروه تحقیقاتی، نمبر تلیفون: 02951 50747، etunimi.sukunimi@om.fi

علاوه بر این، نمبر تلیفون 02951 50738 یا 050345 1931. این خط تلیفون که برای تحقیقات باز شده است، تا تاریخ 2025/8/1 باز است.

تقاضا می شود که بعد از تاریخ 8/1/ ، سؤالات احتمالی خود را به آدرس ایمیل viestinta.otkes@om.fi و یا مستقیماً به مدیر گروه تحقیقاتی روان کنید.

(ترجمانی از زبان فنلندی)

این متن از زبان فنلندی ترجمانی گردیده است. نوشته های داخل پرانتز که زیرشان خط کشیده شده توضیحات ترجمان می باشند.