إن اختراق البيانات الذي استهدف بلدية هلسنكي يؤكد أن هذه الهجمات تتطلب تفكيراً جديداً في استعداد القطاع العام، وطرق التصدي لها، والتواصل بشأنها

شكّلت الحكومة الفنلندية في يوليو 2024، فريق تحقيق مستقل تابع لمركز التحقيق في الحوادث (OTKES) للتحقيق في اختراق البيانات الذي استهدف بلدية هلسنكي في ربيع 2024. يُقدّر عدد الضحايا بحوالي 300,000 شخص، مما يجعل هذا الاختراق الأكبر في تاريخ فنلندا. وقد أنهى فريق التحقيق تقريره الأمني، وتم تسليمه إلى الحكومة بتاريخ 17.6.2025.[1]

إن جرائم اختراق البيانات هي مجال إجرامي متصاعد، و هي تسبب أضراراً كبيرة، خاصة في ظل التهديدات المتنوعة الحالية. ونظراً لكمية ونوعية البيانات التي يحتفظ بها القطاع العام، فهو يعتبر هدفاً جذاباً للمجرمين. لا تزال هناك حاجة لتطوير قدرات القطاع العام في مواجهة تهديدات جرائم اختراق البيانات، حيث إن أساليب رصد الهجمات والثغرات الأمنية ليست مستخدمة على نطاق واسع بما فيه الكفاية.

تخضع إدارة المعلومات، وأمن المعلومات، وحماية البيانات في القطاع العام لتوجيه عدة جهات حكومية، تعمل كل منها بشكل مستقل وفقاً لمهامها الخاصة. هذا التوجيه مجزأ، و يختلف تطبيق القوانين والتعليمات من جهة إلى أخرى. كما أن الرقابة على الجهات المنفذة محدودة. ومع ذلك، فإن إدارة دورة حياة البيانات تُعد أمراً محورياً لأمن المعلومات وحماية البيانات. يمكن تعزيز قدرات القطاع العام على مواجهة تهديدات اختراق البيانات من خلال تطوير وتوسيع أساليب رصد الهجمات والثغرات.

"إن الاستعداد والتصدي لحوادث مثل اختراق البيانات يضعنا في وضع جديد من نواحٍ عدة: اعتدنا في فنلندا، على التعاون بين السلطات، لكن في حوادث اختراق البيانات، تكون إجراءات التصدي موزعة. وفي الوقت نفسه، فإن التحقيق في حوادث الاختراق وإدارتها يعتمد بشكل كبير على خبرة وتوافر الجهات الفاعلة في القطاع الخاص على سبيل المثال، لم يتم تحديد آلية تعاون مماثلة لعمليات SAR [2] في حالات اختراق البيانات. كما أن الكثير من المسؤولية يقع على عاتق الضحية نفسها" ، تقول رئيسة فريق التحقيق، هانا تيرينكي.

"حتى تعريف الضحية نفسها يحتاج إلى إعادة تفكير. نحن نستخدم قواعد بيانات وخدمات مختلفة يومياً دون أن نلاحظ. تحتفظ السلطات المحلية بمعلومات شخصية متنوعة عنا. في حوادث اختراق البيانات، يمكن للمهاجم تخزين كميات كبيرة من البيانات لاستخدامها لاحقاً. وتُعد البيانات المجمعة من مصادر متعددة نقطة ضعف بالنسبة للضحايا. دائماً ما يكون هناك خطر في اختراق البيانات بأن تُستخدم لاحقاً لأغراض ضارة، مثل سرقة الهوية أو الاحتيال – ولا يدرك الشباب، على سبيل المثال، ما قد يحدث لبياناتهم عندما يبلغون سن الرشد" ، تضيف تيرينكي.

دخل قانون الأمن السيبراني الوطني حيز التنفيذ بتاريخ 8.4.2025 20258. ويُعد تنفيذ التوجيه الأوروبي NIS2 جزءاً من تطبيق هذا القانون. ومع ذلك، فإن البلديات والمدن في فنلندا تتمتع بحكم ذاتي واسع، ولا يشمل توجيه NIS2 هذه الجهات.

"توجيه NIS2 لا يشمل السلطات المحلية في فنلندا. ومن خلال التوصيات التي قدمناها في التحقيق، نحاول سد هذه الفجوة جزئياً". تقول تيرينكي.

يفرض توجيه NIS2 على المؤسسات التزاماً بالإبلاغ خلال 24 ساعة. في حالات اختراق البيانات، تُعدّ الاتصالات جزءاً أساسياً من إجراءات الحماية. فهي تقلل من حالة عدم اليقين، وتمنع انتشار المعلومات المضللة، وتضمن حصول الضحايا على الدعم الذي يحتاجونه. كما أن وضوح الرسائل، وشمولها، وسهولة فهمها تُعدّ عناصر بالغة الأهمية.

---

[1] وفقاً لقانون التحقيقات الأمنية 525/2011، يمكن أن يشمل التحقيق في حدث استثنائي أي واقعة شديدة الخطورة أدت إلى الوفاة، أو هددت الوظائف الأساسية للمجتمع، أو تسببت في أضرار جسيمة لها، على ألا تكون هذه الواقعة حادثاً.

[2] ، البحث والإنقاذ.

"يجب أيضاً أخذ الأطفال والشباب بعين الاعتبار كجمهور مستهدف – والتواصل معهم بطريقة تناسب أعمارهم. من الخصائص الأساسية للاتصال في الأزمات وحالات الاضطراب أنه غالباً ما يجب البدء بالمعلومات غير الكاملة – لأن الصورة الكاملة للوضع تتضح طوال الوقت – ولكن هذا النقص الأولي في المعلومات لا يجب أن يكون عائقاً أمام التواصل"، تؤكد تيرينكي.

"ومن الجدير بالذكر أيضاً أن الجهات الفاعلة على المستوى المحلي مختلفة كثيراً، ولا يمكن مقارنتها بشكل مشترك. بعضها مستعد بشكل جيد جداً – بينما لا يزال لدى البعض الآخر الكثير من العمل. إن فنلندا تحقق أداءً جيداً جداً في المقارنات الدولية من حيث الاستعداد. بعد حوادث اختراق البيانات، بدأنا ندرك حجم المشكلة، وبدأنا في معالجتها. أي أن هناك الكثير من الجهود تُبذل بالفعل لمنع ومكافحة حوادث مثل اختراق البيانات"، تؤكد تيرينكي.

يتضمن التحقيق أربع توصيات. وهي موجهة بشكل أساسي إلى وزارة المالية، التي تتحمل مسؤولية تنفيذها بالتعاون مع وزارة العدل، ووزارة النقل والاتصالات، والمجلس الوطني للتعليم، ورابطة البلديات. بالإضافة إلى تطوير إرشادات الاتصال، تتعلق التوصيات بتنسيق إدارة المعلومات، ومراقبتها، وتوجيهها. كما تهدف التوصيات إلى تحسين اكتشاف أوجه القصور في أمن المعلومات في الإدارة العامة، وتعزيز القدرة على اكتشاف هذه الثغرات وتصحيحها.

تعليق الهيئة الوطنية لأمن المعلومات:

مركز الأمن السيبراني (KTK): *"بصفتنا الهيئة الوطنية لأمن المعلومات، فإننا نساعد ونرشد الشركات والسلطات والمواطنين على الاستعداد والتعرف على التهديدات السيبرانية الحالية والمستقبلية. لقد قدم مركز الأمن السيبراني التابع لـ Traficom دعماً شاملاً لبلدية هلسنكي منذ اكتشاف اختراق البيانات، وسنواصل التعاون مع البلدية ومزودي الخدمات"*، يقول المدير سامولي بيرغستروم من مركز الأمن السيبراني في Traficom. *" في الهجمات السيبرانية، تكتسب الاتصالات أهمية خاصة. يتم الشرح في دليل الاتصالات أثناء الأزمات، و الذي أعدته Traficom في ربيع عام 2025 بعنوان كيف تتواصل أثناء الهجمات السيبرانية، الأنواع مختلفة من الهجمات السيبرانية والأساليب والوسائل التي يستخدمها المجرمون. كما يتضمن الدليل نصائح حول الاستعداد الاتصالي، وكيفية التواصل أثناء الهجوم السيبراني وبعده"*، يضيف بيرغستروم.

تحقيقات أخرى تتعلق باختراق البيانات في بلدية هلسنكي:

مكتب التحقيقات الجنائية المركزي (KRP): يتولى مكتب التحقيقات الجنائية المركزي (KRP) مسؤولية التحقيق الأولي في حادثة اختراق بيانات بلدية هلسنكي. ويُصنَّف هذا الاختراق على أنه جريمة اختراق جسيمة. بالإضافة إلى ذلك، يجري المكتب تحقيقاً منفصلاً لتحديد ما إذا كانت البلدية قد قامت بحماية البيانات بشكل مناسب. وفي هذا التحقيق، تُصنَّف الجريمة المشتبه بها، على أنها انتهاك لقوانين حماية البيانات.

مكتب مفوض حماية البيانات (TSV) يقوم بإجراء تحقيق في خرق أمني استهدف البيانات الشخصية، وذلك من منظور الالتزام بتشريعات حماية البيانات. يركّز التحقيق على تقييم مدى كفاية التدابير الأمنية التي اتخذتها بلدية هلسنكي، وما إذا كانت قد قامت بما يلزم لحماية حقوق الأفراد المتضررين من هذا الخرق. التحقيق لا يزال جارياً، ويجري حالياً تحليل التقرير الذي قدمته البلدية حول الحادثة.

من أين تحصل على مساعدة؟

الضحايا - خدمة مساعدة ضحايا الجرائم (RIKU) قد نشرت على صفحتها نصائح للأشخاص الذين وقعوا ضحايا لاختراق أو تسريب بيانات. تؤكد الصفحة على أهمية اتباع تعليمات السلطات المختصة واتخاذ الإجراءات اللازمة لمنع استخدام البيانات الشخصية في عمليات الاحتيال. كما تقدم RIKU أيضاً نقاشات دعم. علماً أن جميع هذه الخدمات هي مجانية.

مزيد من المعلومات:

رئيسة فريق التحقيق هانا تيرينكي، هاتف 50747 02951، om.fi@الكنية.الاسم الأول

بالإضافة إلى الهاتف 50738 02951 أو 1931 050345. إن الاشتراك الهاتفي مفتوح لغاية 1.8.2025. بالإضافة إلى أنه يمكن طرح الأسئلة المحتملة عن طريق عنوان البريد الالكتروني viestintä.otkes@om.fi

بعد تاريخ 1.8 نطلب توجيه الأسئلة المحتملة إلى عنوان البريد الالكتروني viestinta.otkes@om.fi أو مباشرة إلى رئيسة فريق التحقيق.