ملخص P2024-01

في ربيع عام 2024، تعرضت مديرية التربية والتعليم (KASKO) التابعة لبلدية هلسنكي لاختراق معلوماتي خطير. نتيجة لهذا الاختراق، حصل المهاجم على كمية كبيرة من بيانات المتعلمين والموظفين. كما احتوت مستندات القرص الشبكي على معلومات لأشخاص وشركات وجهات تعاون أخرى كانت على اتصال مباشر أو غير مباشر مع البلدية.

بدأ الاختراق في منتصف أبريل 2024، حيث بدأ المهاجم في استكشاف الشبكة الداخلية وتوسيع نطاق وصوله إلى خوادم مختلفة. وفي نهاية أبريل، قام المهاجم بنسخ حوالي 2 تيرابايت من البيانات من الالقرص الشبكي على أربع دفعات. لم يكن من الممكن تحديد عدد الملفات أو محتواها بدقة. وقدرت التحقيقات أن المهاجم حصل على حوالي 750 000 مستند، بعضها يحتوي على بيانات شخصية حساسة.

استمر الاختراق لفترة طويلة بسبب ضعف مراقبة الشبكة في المؤسسة وعدم الاستجابة في الوقت المناسب للتنبيهات. وعندما تأكدت البلدية من حدوث الاختراق، بدأت فوراً باتخاذ إجراءات إدارية وتصحيحية لوقف الهجوم.

كان هناك عاملان رئيسيان مكّنا من نسخ هذه الكمية الكبيرة من البيانات: تمكّن المهاجم من الدخول إلى النظام عبر خادم VPN والذي لم تتم صيانته بشكل كافٍ. كما تراكمت كمية كبيرة من البيانات على القرص الشبكي على مدى سنوات، نتيجة ضعف إدارة المعلومات وعدم مراقبة الالتزام بالتعليمات المتعلقة باستخدام القرص.

ترتبط إدارة المعلومات بعدة قوانين وتشريعات، لكن المعرفة بها بين العاملين في الميدان غالباً ما تكون غير كافية. كما أن التشريعات والإرشادات الوطنية معقدة ومجزأة. وتواجه البلديات بشكل خاص التزامات من عدة جهات رسمية، مما يصعّب إدارة الصورة بشكل كامل.

و نتيجةً للاختراق، فقد حصل المهاجم على كمية كبيرة من المواد التي تحتوي على بيانات شخصية، والتي قد تُستخدم لاحقاً لأغراض ضارة مثل سرقة الهوية والاحتيال. لم يتم ملاحظة مؤشرات على ذلك أثناء التحقيق.

بلغ عدد ضحايا الاختراق مئات الآلاف. وأظهر التحقيق أن تحديد جميع الضحايا بدقة كان أمراً صعباً. تم الوصول إلى الموظفين الحاليين بسهولة، لكن الوصول إلى الموظفين السابقين والمتعلمين السابقين والحاليين كان صعباً للغاية، ولم يتم حتى محاولة ذلك.

يتم إعطاء أربع توصيات صادرة عن التحقيق. تُوجَّه هذه التوصيات بشكل رئيسي إلى وزارة المالية، التي تتولى مسؤولية تنفيذها بالتعاون مع وزارة العدل، ووزارة النقل والاتصالات، والهيئة الوطنية للتعليم، و أيضاً اتحاد البلديات.

1 . وزارة المالية، بالتعاون مع وزارة العدل، تتولى تنسيق تشريعات إدارة المعلومات في الإدارة العامة وتوضيح هياكل الرقابة والتوجيه الخاصة بها.

2 . وزارة المالية، بالتعاون مع وزارة النقل والاتصالات، تدرس كيفية تحسين اكتشاف نقاط الضعف في أمن المعلومات على المستوى الوطني، وضمان امتلاك الجهات العامة للقدرات الكافية لاكتشاف هذه الثغرات ومعالجتها.

3 . وزارة المالية، بالتعاون مع الهيئة الوطنية للتعليم، تضمن أن تقوم البلديات والمدن بتطوير إرشادات واضحة وسهلة الوصول للتواصل في حالات اختراق البيانات، بحيث يتمكن الضحايا من حماية أنفسهم وبياناتهم الشخصية.

4 . وزارة المالية، بالتعاون مع اتحاد البلديات، تدعم البلديات في تحديد ومعالجة الثغرات الأمنية الحرجة، وتعمل على تطوير إدارة المخاطر المتعلقة بإدارة المعلومات وأمنها.