P2024-01 Короткий зміст

Навесні 2024 року департамент дошкільного виховання і освіти міста Гельсінкі (KASKO) став жертвою серйозного витоку даних. Внаслідок витоку даних великий обсяг інформації про учнів та співробітників департаменту . Крім того, документи на мережевому диску містили інформацію про інших людей, компанії та інших партнерів, які мали прямі чи опосередковані стосунки з містом.

Злом даних почався в середині квітня 2024 року, після чого зловмисник почав відображати карту цілей внутрішньої мережі та розширювати свій доступ до різних серверів. Наприкінці квітня зловмисник чотирма частинами скопіював із мережевого диска близько двох терабайт інформації. Точну кількість або вміст файлів визначити не вдалося. Слідство дійшло висновку, що зловмисник отримав приблизно 750 000 документів, деякі з яких містили конфіденційні особисті дані.

Витік даних продовжувався протягом тривалого часу, оскільки мережевий моніторинг організації був недостатнім, а на виявлені сповіщення не відбулося своєчасної реакції. Коли інформація про злом підтвердилася, місто Гельсінкі негайно розпочало заходи з управління та відновлення, за допомогою яких вдалося припинити атаку.

Два фактори дозволили скопіювати великий обсяг даних: інформаційна система була зламана через сервер віддаленого доступу VPN, який незадовільно обслуговувався, і за кілька років на мережевому диску накопичилася велика кількість даних. Неналежне технічне обслуговування було спричинене кадровими та організаційними змінами, що призвело до нечіткої відповідальності. Файли накопичувалися на мережному диску, оскільки керування даними не відповідало вимогам, а дотримання інструкцій щодо використання диска не контролювалося.

Існує кілька законів і нормативних актів, пов’язаних з управлінням даними, але їх обізнаність серед практикуючих спеціалістів часто є недостатньою. Законодавство та принципи з управління на державному рівні частково складні для розуміння та фрагментарні. Муніципальний сектор, зокрема, підпадає під зобов’язання, встановлені кількома різними органами влади, що ускладнює управління у цілому.

Внаслідок витоку даних великий обсяг матеріалу, що містить персональні дані, опинився в руках зловмисника. Згодом ця інформація може бути використана в зловмисних цілях, наприклад, для крадіжки особистих даних та шахрайства. Жодних ознак цього під час розслідування не було виявлено.

Жертвами витоку даних стали сотні тисяч людей. Розслідування показало, що провести всебічне картування всіх жертв було складно. Зв’язатися з персоналом міста було нескладно, але зв’язатися з колишніми працівниками та учнями, а також з учнями, хто зараз навчається, було б дуже складним на практиці і цього навіть не було зроблено.

Розслідування дає чотири рекомендації. Ці рекомендації в основному адресовані Міністерству фінансів, яке відповідає за їх впровадження у співпраці з Міністерством юстиції, Міністерством транспорту та зв'язку, Національним управлінням освіти та Асоціацією муніципалітетів Фінляндії.

1. Міністерство фінансів у співпраці з Міністерством юстиції забезпечують координацію законодавства щодо управління інформацією в державному адмініструванні, а також уточнення його наглядових та контрольних структур.
2. Міністерство фінансів у співпраці з Міністерством транспорту та зв'язку з'ясовує, як можна покращити виявлення вразливостей інформаційної безпеки в державному управлінні в масштабах країни та забезпечити, щоб державні суб'єкти мали достатні можливості для виявлення та виправлення недоліків інформаційної безпеки.
3. Міністерство фінансів у співпраці з Національним управлінням освіти забезпечує розробку муніципалітетами та містами чітких й доступних інструкцій щодо інформування про витік даних, що допоможе жертвам захистити себе від наслідків витоку даних та захистити свої персональні дані.
4. Міністерство фінансів у співпраці з Асоціацією муніципалітетів Фінляндії надає підтримку муніципалітетам у виявленні та усуненні критичних недоліків щодо інформаційної безпеки, а також у розвитку управління інформацією та управління ризиками інформаційної безпеки.