Витік даних у місті Гельсінкі показує, що витоки даних потребують нового підходу в плані готовності державного сектору, комунікації та запобігання витоку даних

У липні 2024 року уряд призначив незалежну слідчу групу при Центрі з розслідування нещасних випадків (OTKES) для розслідування витоку даних, націленого на місто Гельсінкі навесні 2024 року. За оцінками, витік даних вплинув на близько 300 000 жертв, що зробило його найбільшим витоком даних у Фінляндії. Слідча група завершила розслідування щодо безпеки, і звіт про розслідування було подано до Уряду Фінляндії 17.6.2025.[1]

Кіберзлочинність є зростаючою сферою кримінальних злочинів, шкода, яку вона завдає, є значною, особливо у нинішній ситуації гібридних загроз. Державне управління є метою, яка викликає інтерес, для злочинців через якість та кількість інформації, яку воно містить. Державному сектору ще є простір для вдосконалення у реагуванні на загрози кіберзлочинності, оскільки методи виявлення атак і вразливостей використовуються недостатньо широко.

Управління інформацією державного управління, інформаційна безпека та захист даних регулюються кількома різними органами влади. Органи влади здійснюють керівництво незалежно, виходячи зі своїх власних завдань. Керівництво, яке отримують підрозділи управління інформацією, є децентралізованим, і на практиці застосування нормативних актів і інструкцій різниться. Крім того, робота, яку виконують органи влади, являє собою управління, що спрямовано на досягнення цілей, але нагляд за суб'єктами невеликий. Однак саме управління життєвим циклом інформації має центральне значення для інформаційної безпеки та захисту даних. Можливості державного сектора з реагування на кіберзагрози можна посилити за допомогою розробки та розширення методів виявлення атак та вразливостей.

«Підготовка до таких інцидентів, як витік даних, і боротьба з ними суттєво ставить нас у нову ситуацію: Фінляндія традиційно звикла до співпраці між органами влади. У кіберинцидентах контрзаходи децентралізовані. У той же час розслідування та управління інцидентами витоку даних значною мірою залежить від досвіду і доступності суб'єктів приватного сектору. Наприклад, такий механізм співробітництва, як SAR [2], не було визначено для інцидентів витоку даних. Багато чого також залишається на розсуд самої жертви», - каже Ханна Тіріінкі, керівниця слідчої групи.

«Визначення жертви також потребує переосмислення. Ми користуємося різними базами даних та сервісами майже щодня, навіть не помічаючи цього. Місцеві органи влади мають у своєму розпорядженні широкий спектр персональних даних про нас. У кіберинцидентах зловмисник може зберігати великі обсяги даних для подальшого використання. Саме ці об'єднані дані є вразливими для жертв. При витоках даних завжди існує очевидний ризик того, що дані згодом можуть бути використані в зловмисних цілях, таких як крадіжка особистих даних та шахрайство, а молоді люди, приміром, не обов'язково можуть думати про те, що станеться з їхніми даними, коли вони досягнуть повноліття», - додає Тіірінкі.

Закон про національну кібербезпеку набув чинності 8.4.2025. Національна імплементація Директиви про мережеву та інформаційну безпеку NIS2 є частиною виконання Закону про кібербезпеку. Однак у Фінляндії муніципалітети та міста мають широку автономію, а Директива про кібербезпеку NIS2 не поширюється на муніципалітети та міста.

---

[1] Відповідно до закону, розслідування надзвичайної ситуації (НС) може стосуватися дуже серйозної ситуації, яка призвела до смерті або загрожувала чи завдала серйозної шкоди основним функціям суспільства, але не є нещасним випадком (Закон про розслідування подій у сфері безпеки 525/2011).
[2] Search and Rescue (Пошук і Порятунок).

"Директива NIS2 не поширюється на органи місцевого самоврядування у Фінляндії. За допомогою рекомендацій, зроблених під час розслідування, ми зараз намагаємося частково заповнити цю прогалину", - додає Тіірінкі.

NIS2 накладає на організації обов'язок цілодобового зв'язку. У випадках витоку даних комунікація є важливою частиною заходів із захисту. Комунікація зменшує невизначеність, запобігає поширенню хибної інформації та гарантує, що жертви отримають необхідну підтримку. Доступність, вичерпність і зрозумілість спілкування мають першочергове значення.

«Наприклад, діти і молодь є цільовою групою і комунікації з ними відповідно до їх вікового рівня також мають бути взяті до уваги. Базовий характер кризової комунікації та комунікації при інцидентах полягає в тому, що в ситуації вам часто доводиться починати з неповної інформації оскільки ситуаційна картина постійно доповнюється і цей недостатній обсяг інформації не повинен бути перешкодою для комунікації», - наголошує Тіірінкі.

«Також слід зазначити, що суб'єкти в місцевому секторі дуже різні та неоднакові. Деякі з них вже дуже добре підготувалися, інші ще потребують посилення. Фінляндія має дуже якісні результати з погляду підготовки у міжнародному порівнянні. Після витоку даних ми також помітили проблему, і почали її виправляти. Тому чимало вже зроблено для запобігання та боротьби з такими інцидентами, як витоки даних», - підкреслює Тіірінкі.

Розслідування дає чотири рекомендації. Ці рекомендації переважно 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. Окрім розробки керівних принципів комунікації, рекомендації стосуються координації управління інформацією, її нагляду та керівних принципів. Крім того, рекомендації стосуються покращення виявлення недоліків інформаційної безпеки в державному управлінні та покращення здатності виявляти та усувати недоліки інформаційної безпеки.

Коментар Державного органу з інформаційної безпеки:

Центр кібербезпеки (KTK): *«Як державний орган з інформаційної безпеки, ми допомагаємо та консультуємо компанії, органи влади і громадян з підготовки до нинішніх та майбутніх кіберзагроз та їх виявлення. Центр кібербезпеки Агентства транспорту і зв'язку Фінляндії Traficom всебічно підтримував місто Гельсінкі з моменту виявлення витоку даних, і ми продовжимо співпрацювати і надалі з містом та постачальниками послуг»,* - каже директор Самулі Берґстрьом із Центру кібербезпеки Агентства Traficom. *«Важливість комунікації наголошується під час кібератаки. Інструкція з комунікації в кризових ситуаціях «Як повідомляти про кібератаки», опублікована Агентством Traficom навесні 2025 року, містить інформацію про різноманітні кібератаки, а також методи та засоби, що використовуються кіберзлочинцями. В інструкції також даються поради щодо готовності до комунікації та спілкування під час та після кібератаки»,* - розповідає далі Берґстрьом.

Інші розслідування, пов'язані з витоком даних міста Гельсінкі:

Центральна кримінальна поліція (KRP): Центральна кримінальна поліція Фінляндії відповідає за попереднє розслідування витоку даних міста Гельсінкі. Витік даних розслідується як порушення даних при обтяжуючих обставинах. Крім того, Центральна кримінальна поліція розслідує в рамках окремого попереднього розслідування, чи захистило місто належним чином дані. У цьому розслідуванні назва злочину є підозрюваним злочином, що пов'язаний з захистом даних.

Офіс омбудсмена із захисту даних (TSV) розслідує витік персональних даних з огляду дотримання законодавства про захист даних. Під час розслідування буде спеціально визначено, чи забезпечило місто Гельсінкі достатні заходи безпеки і чи подбало про права людей, які постраждали від порушення. Розслідування триває, і зараз надається оцінка звіту, який був отриманий від міста Гельсінкі з приводу інциденту.

Звідки можна отримати допомогу?

Служба підтримки жертв злочинів (RIKU) опублікувала на своєму сайті рекомендації для жертв викрадення даних або витоку даних. На сайті наголошується, що важливо дотримуватись інструкцій органів влади та вживати необхідних заходів блокування, щоб запобігти використанню персональних даних у шахрайських цілях. Служба RIKU також пропонує підтримку через обговорення. Послуги служби надаються безкоштовно.

Додаткова інформація:

Керівниця слідчої групи Ханна Тіірінкі (Hanna Tiirinki), тел. 02951 50747, etunimi.sukunimi@om.fi

Додаткові тел. 02951 50738 або 050345 1931. Для цілей розслідування відкрита телефонна лінія працює до 1.8.2025.

Після 1 серпня будь-які запитання надсилайте на електронну адресу viestinta.otkes@om.fi або безпосередньо до керівниці слідчої групи.