Затронувший Хельсинки взлом информационной системы показывает, что кибератаки требуют нового подхода к обеспечению готовности, организации коммуникации и противодействия таким атакам в государственном секторе

В июле 2024 года Правительство Финляндии учредило независимую следственную группу в составе Службы расследования причин аварий и инцидентов (OTKES) для расследования затронувшего весной 2024 года Хельсинки взлома информационной системы. По оценкам, жертвами кибератаки стали примерно 300 000 человек, что делает ее крупнейшей в Финляндии. Следственная группа завершила расследование по вопросам обеспечения безопасности, и отчет о расследовании был передан Правительству 17.06.2025.[1]

Киберпреступность является развивающимся криминальным направлением, и причиняемый ею вред значителен, особенно в нынешних условиях воздействия гибридных угроз. Государственное управление в силу характера и количества обладаемой им информации является привлекательной целью для преступников. Государственному сектору все еще есть, над чем работать в вопросах реагирования на угрозы кибербезопасности, поскольку методы обнаружения атак и уязвимостей используются недостаточно широко.

Хранение и обработка информации, информационная безопасность и защита данных в сфере государственного управления координируется несколькими различными органами. Официальные органы осуществляют руководство самостоятельно, исходя из собственных задач. Инструкции, получаемые отделами, занимающимися хранением и обработкой информации, разрозненны, и применение правовых положений и инструкций на практике различается. Кроме того, выполняемая официальными органами работа сводится к руководству, но контроль за деятельностью исполнителей незначителен. Однако, именно контроль над всеми этапами существования информации является центральным для информационной безопасности и защиты данных. Готовность государственного сектора реагировать на киберугрозы может быть усилена посредством разработки и расширения методов обнаружения атак и уязвимостей.

«Готовность к происшествиям, подобным взлому информационных систем, и борьба с ними ставит нас во многих отношениях в новое положение: для Финляндии характерно взаимодействие официальных органов. Однако, в отношении кибератак меры реагирования оказываются разрозненным. В то же время расследование случаев взлома информационных систем и контроль над ситуацией во многом зависят от профессионализма и доступности исполнителей частного сектора. Например, для борьбы с утечками данных не существует механизма сотрудничества, подобного SAR[2]. Многое также остается на совести самих потерпевших», — отмечает руководитель следственной группы Ханна Тийринки.

«Определение жертвы также требует переосмысления. Мы почти ежедневно, даже не замечая этого, используем различные базы данных и сервисы. Местные официальные органы располагают персональных данными, касающимися различных аспектов нашей жизни. Посредством кибератаки злоумышленники могут завладеть большим объемом данных для последующего использования. Именно эта совокупная информация является уязвимостью в отношении жертв. Взлом информационных систем всегда сопряжен с риском того, что данные впоследствии могут быть использованы в преступных целях,

[1] В соответствии с законом, расследование чрезвычайного происшествия может проводиться в отношении очень серьезного инцидента, приведшего к гибели людей, или поставившего под угрозу или причинившего значительный ущерб реализации основных функций общества, но не являющегося несчастным случаем. Закон «О проведении расследования в целях обеспечения безопасности» 525/2011.

[2] Search and Rescue, поиск и спасение

таких как кража цифровой личности и мошенничество, при этом, например, подростки, могут не задумываться о том, что происходит с их данными, когда они достигают совершеннолетия», — добавляет Тийринки.

Национальный Закон «О кибербезопасности» вступил в силу 08.04.2025. Национальная реализация Директивы Европейского Союза о сетевой и информационной безопасности NIS2 является составной частью процесса исполнения этого Закона на практике. Однако в Финляндии муниципалитеты и города обладают широкой автономией, а Директива о кибербезопасности NIS2 не распространяется на муниципалитеты и города.

«Директива NIS2 не распространяется на местные официальные органы в Финляндии. С учетом рекомендаций, данных в ходе расследования, мы пытаемся сейчас частично заполнить этот пробел», — комментирует Тийринки.

Директива NIS2 налагает на организации обязательство по обеспечению круглосуточной связи. В случаях взлома информационных систем коммуникация является существенной составляющей мер защиты. Коммуникация снижает неопределенность, предотвращает распространение ложной информации и гарантирует, что жертвы получат необходимую поддержку. Доступность, полнота и понятность коммуникации имеют первостепенное значение.

«В частости, дети и подростки, как целевая группа, а также соответствующие их возрасту методы информирования должны быть приняты во внимание. Для оповещения в кризисных ситуациях различного происхождения характерно то, что зачастую поначалу приходится ограничиваться неполной информацией, поскольку картина происходящего постоянно дополняется. Этот изначально неполный объем информации не должен быть препятствием для коммуникации», — подчеркивает Тийринки.

«Также следует отметить, что непосредственные исполнители на местном уровне сильно отличаются друг от друга. Некоторые из них уже хорошо подготовились к возможным ситуациям, другим еще есть, над чем поработать. Уровень подготовки Финляндии по сравнению с другими странами достаточно высокий. После случаев взломов информационных систем мы также осознали проблему и предприняли действия для ее исправления. Другими словами, уже многое делается для предотвращения и борьбы с такими происшествиями, как взломы и утечки данных», — отмечает Тийринки.

В ходе расследования было дано четыре рекомендации. Они ориентированы главным образом на Министерство финансов, которое ответственно за их реализацию при содействии Министерства юстиции, Министерства транспорта и связи, Главного управления образования Финляндии и Союза муниципалитетов Финляндии. Помимо разработки инструкций по организации коммуникации, рекомендации касаются координации в области хранения и обработки информации, контроля за этим процессом и руководства. Кроме того, рекомендации затрагивают вопросы повышения эффективности выявления уязвимостей информационной безопасности в государственном управлении и совершенствования его способности обнаруживать и устранять такие уязвимости.

Комментарий национального органа по информационной безопасности:

Центр кибербезопасности (КТК): *«Как национальный орган по обеспечению информационной безопасности, мы оказываем помощь и консультируем предприятия, официальные органы и граждан в вопросах подготовки к текущим и будущим киберугрозам и их выявлении. Центр кибербезопасности Агентства транспорта и связи (Traficom)*

оказывал администрации Хельсинки всестороннюю поддержку с момента обнаружения взлома, и мы продолжаем взаимодействовать с городом и поставщиками услуг», – говорит руководитель Центра кибербезопасности Агентства транспорта и связи Самули Бергстрём. *«Организация коммуникации в случае кибератаки приобретает большое значение. Выпущенное Агентством транспорта и связи весной 2025 года руководство по кризисной коммуникации «Как информировать о кибератаках», содержит информацию о различных кибератаках, а также методах и средствах, используемых преступниками. Руководство также содержит советы по подготовке к информированию и организации коммуникации во время и после кибератаки»,* – продолжает Бергстрём.

Другие расследования, проводимые в связи со взломом информационной системы Хельсинки:

Центральная криминальная полиция (KRP): за проведение предварительного расследования обстоятельств совершения взлома информационной системы Хельсинки отвечает Центральная криминальная полиция. Взлом квалифицируется при расследовании как тяжкое деяние. В рамках отдельного предварительного расследования Центральная криминальная полиция также выясняет, обеспечила ли администрация города надлежащую защиту данных, при этом преступление квалифицируется как подозрение в нарушении защиты данных.

Офис уполномоченного по защите данных (TSV) проводит расследование нарушения информационной безопасности, затронувшей персональные данные, с позиции соблюдения законодательства о защите данных. Особое внимание при проведении расследования будет уделено тому, были ли предприняты администрацией Хельсинки необходимые меры по обеспечению защиты и позаботилась ли она о соблюдении прав людей, пострадавших в результате нарушения. Расследование продолжается, и в ходе него изучается только что полученный от администрации отчет о произошедшем.

Куда обратиться за помощью?

Служба поддержки жертв преступлений (RIKU) опубликовала на своем сайте советы для жертв взлома информационных систем или утечки данных. На сайте подчеркивается важность выполнения данных официальными органами инструкций и принятия необходимых мер по блокировке данных, чтобы не допустить использование персональных данных в целях мошенничества. Служба поддержки жертв преступлений также предлагает бесплатную услугу терапевтических бесед.

Дополнительная информация:

Руководитель следственной группы Ханна Тийринки, тел. 02951 50747, etunimi.sukunimi@om.fi

Дополнительные телефоны 02951 50738 или 050345 1931. Линия, открытая в целях проведения расследования, будет работать до 01.08.2025.

После 01.08. просим адресовать возможные вопросы на адрес электронной почты viestinta.otkes@om.fi или напрямую руководителю следственной группы.