P2024-01 Резюме

Весной 2024 года сфера дошкольного воспитания и образования города Хельсинки (KASKO) подверглась серьезному взлому информационной системы. В результате взлома большое количество данных, касающихся учащихся и персонала, оказалось в распоряжении злоумышленника. Кроме того, документы, хранящиеся на сетевом диске, содержали информацию о других лицах, предприятиях и партнерах, опосредованно или напрямую работающих с городом.

Взлом информационной системы начался во второй половине апреля 2024 года, после чего злоумышленник приступил к сбору объектов внутренней сети и начал расширять свой доступ к различным ресурсам. В конце апреля преступник за четыре раза скопировал с сетевого диска в общей сложности примерно два терабайта информации. Точное количество или содержание файлов установить не удалось. По оценке, полученной в ходе расследования, злоумышленник сумел завладеть примерно 750 000 документами, часть из которых содержала конфиденциальную информацию личного характера.

Взлом продолжался долгое время, так как сетевой мониторинг организации был неоптимальным и на обнаруженные уведомления отреагировали несвоевременно. Когда информация о взломе подтвердилась, администрация города Хельсинки незамедлительно инициировала меры по управлению ситуацией и ее и исправлению, посредством которых взлом удалось остановить.

Копирование значительного объема информации стало возможным из-за наличия двух факторов: информационную систему смогли взломать через плохо обслуживаемый сервер виртуальной частной сети (vpn) и на сетевом диске за многие годы скопилось большое количество информации. Недостатки в содержании и обслуживании были связаны со сменой персонала и изменениями в организации, в результате чего распределение ответственности оказалось нечетким. Информация скапливалась на сетевом диске по причине плохой организации хранения и обработки данных и отсутствия контроля за выполнением инструкций, касающихся использования диска.

Хранение и обработка информации регулируется множеством законов и нормативно-правовых актов, однако осведомленность о них на практике часто оказывается недостаточной. Законодательство и общегосударственные инструкции отчасти сложны для понимания и разрозненны. В особенности на сектор муниципального управления распространяются обязательства, налагаемые несколькими различными официальными органами, что затрудняет контроль в целом.

В результате взлома информационной системы большое количество материалов, содержащих персональные данные, оказалось в распоряжении злоумышленника. Впоследствии информация может быть использована в противоправных целях, например, для кражи цифровой личности или мошенничества. В ходе расследования признаков этого не было обнаружено.

Жертвами взлома информационной системы стали сотни тысяч человек. Расследование показало, что полное выявление всех жертв взлома затруднительно. К персоналу администрации города удалось обратиться, однако связаться с бывшими работниками и учащимися, а также нынешними учащимися в действительности оказалось чрезвычайно трудно, и даже не предпринимались попытки сделать это.

В ходе расследования были даны 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.

1. Министерство финансов совместно с Главным управлением образования Финляндии обеспечит согласование законодательства, касающегося хранения и обработки данных в государственном управлении, и определит его надзорные и управляющие структуры.
2. Министерство финансов совместно с Министерством транспорта и связи выяснит, каким образом можно улучшить в общегосударственном масштабе обнаружение недостатков информационной безопасности в государственном управлении, и убедится, что у государственных органов достаточно возможностей для выявления и устранения недостатков информационной безопасности.
3. Министерство финансов совместно с Главным управлением образования Финляндии позаботится о том, чтобы при информировании о случаях взлома информационных систем муниципалитеты и города разрабатывали понятные и доступные инструкции, которые помогут жертвам защитить себя от последствий взломов и защитить свои персональные данные.
4. Министерство финансов совместно с Союзом муниципалитетов Финляндии окажет муниципалитетам поддержку в выявлении и устранении критических недостатков информационной безопасности, а также разработает систему управления рисками в области хранения и обработки данных и информационной безопасности.