Когда безопасность не приоритет: история одной биотехкомпании.

Нью-йоркская компания Enzo Biochem оказалась в непростой ситуации после кибератаки, произошедшей в 2023 году. Результатом инцидента стала компрометация личных данных более 2,4 миллионов человек.

Генеральный прокурор Нью-Йорка Летиция Джеймс объявила о завершении расследования во вторник. Выводы неутешительны: в компании выявлены многочисленные нарушения правил кибербезопасности, которые не только облегчили доступ хакерам, но и затруднили обнаружение атаки.

Теперь Enzo Biochem придется выплатить штраф в размере 4,5 миллиона долларов. Сумма будет распределена между тремя штатами: Нью-Йорком, Нью-Джерси и Коннектикутом. Нью-Йорк получит наибольшую долю, так как здесь проживает большинство пострадавших — около 1,457 миллиона человек.

Причины столь серьезного нарушения безопасности кроются в ненадлежащем управлении учетными данными. Выяснилось, что две учетные записи использовались сразу пятью сотрудниками. Более того, один из паролей не менялся в течение десяти лет, что вызывает серьезные вопросы о его надежности.

Проблемы на этом не заканчиваются. В Enzo Biochem не использовали двухфакторную аутентификацию. Сотрудники могли получать доступ к электронной почте из любой точки мира без дополнительных проверок. Кроме того, часть серверов и рабочих станций хранили конфиденциальные данные пациентов в незашифрованном виде.

При таком подходе неудивительно, что компания не смогла вовремя обнаружить вторжение. Вместо использования современных автоматизированных систем мониторинга, в Enzo полагались на ручной контроль сетевой активности. В результате злоумышленники несколько дней беспрепятственно действовали в системах компании.

Генеральный прокурор Нью-Джерси Мэтью Дж. Платкин выразил недоумение по поводу того, что медицинская компания не соблюдала даже базовые меры предосторожности для онлайн-аккаунтов, включая инструктаж сотрудников о недопустимости совместного использования паролей.

После инцидента Enzo Biochem разработала комплексный план по улучшению кибербезопасности. Компания внедрила систему обнаружения и реагирования на угрозы, наняла круглосуточную службу мониторинга безопасности, ужесточила

требования к паролям и внедрила двухфакторную аутентификацию. Также был применен подход «нулевого доверия».

Генеральные прокуроры трех штатов наложили на компанию ряд дополнительных требований для обеспечения высокого уровня безопасности и после завершения расследования.

Летиция Джеймс подчеркнула, что медицинские процедуры не должны приводить к риску кражи личных данных пациентов киберпреступниками. Она отметила, что компании, пренебрегающие безопасностью данных, подвергают пациентов серьезной опасности мошенничества и кражи личности.

Случай с Enzo Biochem напоминает о уязвимости медицинских организаций перед киберугрозами. В этом году уже произошли крупные инциденты в Change Healthcare и Synnovis , которые продемонстрировали, насколько серьезными могут быть последствия атак на медицинский сектор.

На перекрестке науки и фантазии — наш канал