

КРУПНЫЕ КЕЙСЫ
ВЗЛОМОВ И УТЕЧЕЧЕК
ДАННЫХ

JP MORGAN CHASE



В 2014 году крупнейший американский банк JP Morgan Chase столкнулся с одним из самых масштабных банковских взломов в истории. Хакеры получили доступ к данным около 83 миллионов клиентов и 7 миллионов компаний. Атака использовала уязвимости в сети банка и слабую сегментацию серверов, благодаря чему преступники оставались незамеченными несколько месяцев. Последствия были серьёзными: банк значительно увеличил бюджет на кибербезопасность и пересмотрел архитектуру сети. Этот кейс показывает, что даже крупные финансовые организации уязвимы, если их внутренняя защита слабая.

FACEBOOK

В 2018–2019 годах платформа Facebook стала жертвой утечки данных 533 миллионов пользователей, о которой стало известно только в 2021 году. Злоумышленники воспользовались уязвимостью в функции импорта контактов, получив доступ к именам, телефонам, e-mail и датам рождения. Данные использовались для фишинговых атак, что нанесло ущерб репутации компании и привело к штрафам по GDPR. Этот кейс демонстрирует, что даже «обычные» функции соцсетей могут представлять серьёзную угрозу безопасности.



YAHOO



Yahoo пережила крупнейшую в истории интернет-компанию утечку данных — были скомпрометированы 3 миллиарда аккаунтов. Хакеры получили логины, e-mail, хешированные пароли и секретные вопросы пользователей. Компания скрывала факт взлома несколько лет, что привело к падению доверия и уменьшению стоимости при продаже Verizon. Этот кейс наглядно показывает, что сокрытие инцидентов может лишь усугубить ущерб и ударить по репутации.



www.yahoo.com





TARGET

Сеть магазинов Target в 2013 году пострадала от утечки данных 40 миллионов банковских карт через компанию-подрядчика, обслуживавшую системы кондиционирования. Хакеры сначала взломали подрядчика, а затем проникли в основную сеть Target. Инцидент привёл к крупным финансовым потерям, судебным искам и массовой замене карт. Этот кейс подчёркивает важность защиты не только собственной инфраструктуры, но и всех партнёров.



www.target.com



ROCKYOU



В 2009 году компания RockYou допустила утечку 32 миллионов паролей в открытом виде, без шифрования или хеширования. Эти пароли стали основой для словарей атак, которые используются до сих пор. Кейс RockYou показывает, что правильное хранение паролей – ключевой элемент безопасности, и халатность в этом вопросе может иметь долгосрочные последствия.

ЧТО ДЕЛАТЬ В ТАКИХ СИТУАЦИЯХ?

Для компаний:

- Регулярно обновлять ПО и патчи – предотвращает атаки через уязвимости (Equifax, Yahoo).
- Сегментация сети и контроль доступа – ограничивает последствия взлома (JP Morgan).
- Обучение сотрудников – фишинг и MFA-атаки срабатывают только при человеческой ошибке (Facebook, Uber).
- Безопасность подрядчиков – проверка и контроль поставщиков и партнёров (Target, Capita).
- Шифрование и защита данных – пароли и личная информация должны быть надежно защищены (RockYou).

для пользователей:

- Сильные уникальные пароли и менеджер паролей – чтобы утечка одного сервиса не ударила по всем аккаунтам.
- Двухфакторная аутентификация (2FA) – снижает риск взлома, даже если пароль скомпрометирован.
- Регулярная проверка и обновление аккаунтов – контролируйте, где вы авторизованы.
- Осторожность с ссылками и приложениями – даже мессенджеры могут использовать уязвимости.

ОБЩИЕ ВЫВОДЫ

Все рассмотренные кейсы демонстрируют, что угрозы существуют в разных сферах – от банковских систем и соцсетей до ритейла и онлайн-сервисов. Основные причины инцидентов – технические уязвимости, ошибки людей и недостаточная защита подрядчиков. Урок простой: кибербезопасность – это не только ИТ, но и бизнес, где доверие, контроль и внимание к деталям имеют решающее значение.

**СПАСИБО ЗА
ВНИМАНИЕ!!!**