

Семь способов предотвратить утечку данных и нарушение безопасности данных в 2022 году

Репенко Дмитрий Сергеевич

Бурлаков Евгений Александрович

Аннотация: в данной статье рассмотрены тенденции роста киберпреступности, возможности злоумышленников и последствия утечки данных коммерческих компаний.

Ключевые слова: киберпреступление, утечка данных, коммерческая тайна.

Новостная лента не будет полной, если она не приправлена новостями об утечке данных. Каждый день престижные предприятия становятся жертвами разрушительной угрозы, которая, как ожидается, будет стоить миру 10,5 триллиона долларов в год к 2025 году.

Ключом к преодолению значительной тенденции роста утечек данных является предотвращение событий, которые потенциально могут перерасти в утечку данных. Все утечки данных должны быть выявлены и устранены до того, как их обнаружат киберпреступники.

Что такое утечка данных?

Утечка данных — это незамеченное раскрытие конфиденциальных данных в электронном или физическом виде. Утечки данных могут происходить на внутренних или физических устройствах, таких как внешние жесткие диски или ноутбуки.

Если киберпреступник обнаруживает утечку данных, он может использовать эту информацию, чтобы подготовиться к нарушению безопасности.

Примеры утечек данных

Святым Граалем раскрытия конфиденциальной информации является личная информация (PII - Personally Identifiable Information), такая как имена, контактная информация и финансовые данные. Другие, менее 'полезные' формы данных могут использоваться для разведывательных миссий для раскрытия внутренних секретов.

Существует четыре основных категории утечек данных: информация о клиентах, информация о компании, коммерческая тайна и аналитика.

1. Информация о клиенте

Некоторые из самых крупных утечек данных включали утечку данных о клиентах, связанную с личной идентифицируемой информацией. Данные о клиентах уникальны для каждой компании. Конфиденциальная информация клиента может включать любое из следующего:

- Имена клиентов
- Адреса
- Телефонный номер
- Адрес электронной почты
- Имена пользователей
- Пароли
- Истории платежей
- Привычки просмотра продуктов
- Номера карт

2. Информация о компании

Утечка информации о компании раскрывает конфиденциальную внутреннюю деятельность. Такие утечки данных, как правило, попадают в поле зрения недобросовестных компаний, преследующих маркетинговые планы своих конкурентов.

- Утечки данных компании могут включать следующее:
- Внутренние коммуникации
- Показатели эффективности
- Рыночные стратегии

3. Коммерческая тайна

Это самая опасная форма утечки данных для бизнеса. Кража интеллектуальной собственности уничтожает потенциал бизнеса, сводя его к нулю.

Утечка данных, составляющих коммерческую тайну, может включать следующее:

- Предстоящие планы продуктов
- Программное кодирование
- Собственная информация о технологиях

4. Аналитика

Аналитические информационные панели содержат большие наборы данных, и киберпреступники обращаются к любому значительному пулу данных. Таким образом, программное обеспечение для аналитики является вектором атаки, который необходимо отслеживать.

- Утечки данных аналитики могут включать следующее:
- Данные о поведении клиентов
- Психологические данные
- Смоделированные данные

Разница между утечкой данных и нарушением безопасности данных

Нарушение безопасности данных — это результат запланированной кибератаки, а утечка данных — это случайное раскрытие конфиденциальных данных бизнесом. Киберпреступники не создают утечки, они обнаруживают их, а затем используют для нарушений безопасности данных.

Утечки данных, как правило, происходят из-за плохой практики безопасности. На бизнес также может повлиять утечка данных у любого из его поставщиков. Поскольку эти уязвимости встречаются в обширной среде атак, их трудно обнаружить и устранить, пока не стало слишком поздно.

Без сложного решения для защиты данных предприятия останутся уязвимыми для утечки данных через стороннюю сеть.

7 советов, как защитить свой бизнес от утечек данных

Следующие методы обеспечения безопасности данных могут предотвратить утечку данных и свести к минимуму вероятность утечки данных.

1. Оценить риск третьих лиц

К сожалению, ваши поставщики могут не относиться к кибербезопасности так серьезно, как вы. Важно постоянно оценивать состояние безопасности всех поставщиков, чтобы убедиться, что они не подвергаются риску утечки данных.

Оценка рисков поставщика — это распространенный метод обеспечения соответствия третьих сторон нормативным стандартам, таким как HIPAA, PCI-DSS или GDPR. Анкеты рисков могут быть составлены путем добавления соответствующих вопросов из существующих фреймворков или, в идеале, отправлены из стороннего решения для мониторинга поверхности атаки.

Может быть трудно идти в ногу с требованиями управления рисками обширной сети сторонних облачных сервисов. Чтобы предотвратить упущенные из виду риски поставщиков, которые делают предприятия уязвимыми к утечке данных, управление сторонними рисками лучше всего доверить команде аналитиков CyberResearch.

2. Контролируйте весь доступ к сети

Чем больше отслеживается корпоративный сетевой трафик, тем выше вероятность выявления подозрительной активности. Атакам утечки данных обычно предшествуют разведывательные кампании — киберпреступникам

необходимо определить конкретные средства защиты, которые необходимо обойти во время атаки.

Решения по предотвращению утечек данных позволяют организациям выявлять и усиливать уязвимости в системе безопасности, чтобы предотвратить возможность проведения разведывательных кампаний.

Возможно, потребуется пересмотреть политики безопасности, чтобы обеспечить привилегированный доступ к особо конфиденциальным данным.

3. Определите все конфиденциальные данные

Прежде чем можно будет приступить к практике предотвращения потери данных (DLP), компаниям необходимо определить все конфиденциальные данные, которые необходимо защитить. Затем эти данные необходимо правильно классифицировать в соответствии со строгими политиками безопасности.

Категории могут включать защитную медицинскую информацию наряду с другими формами конфиденциальных данных.

Когда все конфиденциальные данные идентифицированы и правильно классифицированы, компания может адаптировать наиболее эффективные средства защиты от утечки данных для каждой категории данных.

4. Защитите все конечные точки

Конечная точка — это любая удаленная точка доступа, которая взаимодействует с бизнес-сетью либо через конечных пользователей, либо автономно. Сюда входят устройства Интернета вещей, компьютеры и мобильные устройства.

Сейчас, когда большинство предприятий переходят на ту или иную модель удаленной работы, конечные точки стали рассредоточены (иногда даже по всему миру), что усложняет их защиту.

Брандмауэры и VPN предлагают базовый уровень безопасности конечных точек, но этого недостаточно. Сотрудники часто обманом заставляют внедрять вредоносное ПО в экосистему, чтобы обойти эти средства защиты.

Организации должны обучать своих сотрудников распознавать уловки кибератак, особенно фишинговые атаки по электронной почте и атаки с использованием социальной инженерии. Образование — очень мощное решение для предотвращения утечки данных.

5. Зашифруйте все данные

Киберпреступникам может быть сложно использовать утечку данных, если данные зашифрованы. Существует две основные категории шифрования данных — шифрование с симметричным ключом и шифрование с открытым ключом.

В то время как зашифрованные данные могут поставить в тупик второкурсника-хакера, едкие кибер-злоумышленники могут расшифровать данные без ключа дешифрования. По этой причине шифрование данных не должно быть единственной тактикой предотвращения утечки данных, а должно использоваться вместе со всеми методами в этом списке.

6. Оцените все разрешения

В настоящее время к вашим конфиденциальным данным могут получить доступ пользователи, которым они не нужны. В качестве первоначального ответа следует оценить все разрешения, чтобы убедиться, что доступ не предоставляется авторизованным сторонам.

Как только это будет проверено, все важные данные должны быть классифицированы по разным уровням чувствительности для контроля доступа к различным пулам данных. Только заслуживающий доверия персонал с основными требованиями должен иметь доступ к особо конфиденциальным данным.

Этот процесс назначения привилегированного доступа может также выявить любых злонамеренных инсайдеров, которые способствуют краже конфиденциальных данных.

7. Следите за состоянием безопасности всех поставщиков

Отправка оценок рисков побудит поставщиков усилить свои усилия по обеспечению кибербезопасности, но без решения для мониторинга усилия по исправлению не могут быть подтверждены.

Оценка безопасности — это высокоэффективный способ оценки восприимчивости поставщика к утечке данных. Эти решения для мониторинга отображают всех поставщиков в сторонней сети вместе с их рейтингом безопасности, предоставляя организациям мгновенную прозрачность состояния всей сети поставщиков.

Литература

- Амелин Р. В. Информационная безопасность / Р.В. Амелин ; М.: Юрист, 2010, - С. 121.
- 2. Кнопкин Н. Защита персональных данных: антикризисный подход / Н. Кнопкин // IT-manager. 2011. - № 6. - С. 23.
- 3. Садердинов А.А. Информационная безопасность / А.А Садердинов, В.А. Трайнев; М.: Дашков и К', 2004. - 335 с.
- 4. Документооборот и документоуправление на предприятии - [Электронный ресурс] - <http://docrev.ru/zashhishhyonnye-dokumentopotoki/>
- 5. Технологии будущего - Информационная безопасность - [Электронный ресурс] - http://www.future-techno.biz/page/news-kanali_utechki.