Как управлять рисками утечки критичных данных?

Утечка критичной информации может привести к крайне негативным последствиям для бизнеса – от серьезного ущерба репутации (уменьшение лояльности клиентов к компании и/или бренду) до финансовых потерь (как реальных, так и потенциальных будущих, недополученная прибыль), в том числе к предписаниям и мерам воздействия со стороны регуляторов (от штрафов до отзыва лицензий). Предотвращение утечек является важной задачей, которая может быть решена только путем применения комплекса мер технического и организационного характера

Антон Свинцицкий
Руководитель отдела консалтинга
АО "ДиалогНаука"

Евгения Заяц
Старший консультант отдела консалтинга
АО "ДиалогНаука"

Защита от утечек критичных данных, как и от любых других угроз, должна строиться на результатах анализа рисков и соответствовать определенным в компании целям обеспечения информационной безопасности и, что не менее важно, бизнес-целям и существующим бизнес-процессам.

Определение данных, подлежащих защите

Независимо от того, какой способ контроля каналов утечки будет выбран, на первом этапе необходимо провести обследование информационных потоков и определить состав критичной информации, подлежащей защите. Данная работа должна быть реализована путем анализа внутренних организационно-распорядительных документов, регламентирующих порядок получения доступа, обработки, хранения и защиты информации, а также определения перечня информации и активов, подлежащих защите. При этом устанавливается:

- перечень обрабатываемой информации;
- категории информации и необходимость их защиты;
- порядок обработки и места хранения информации с целью определение легитимных мест хранения;
- легитимные информационные потоки и каналы передачи.

Анализ и сбор данных должен производиться в обязательном порядке в привязке к существующим бизнес-процессам. По результатам анализа этих процессов и информационных потоков должен быть сформирован не только перечень защищаемой информации, но и легитимные каналы ее передачи (в том числе определены лица, ответственные за реализацию этих каналов со стороны структурных подразделений – "владельцы активов") и места хранения (информационные системы, сетевые папки и т.д.).

Выявление каналов утечки информации

На втором этапе необходимо определить потенциальные каналы утечки защищаемой информации, перечень которых напрямую зависит от используемых в компании ИТ-технологий, характеристик корпоративной информационной системы и существующих бизнес-процессов. К таким каналам могут относиться:

- передача данных по электронной почте;
- запись и хранение данных на внешних носителях (в том числе несанкционированное копирование виртуальных машин, на которых обрабатывается защищаемая информация);
- передача данных с применением интернет-сервисов (социальные сети, форумы, облачных хранилища и т.д.);
- использование беспроводных сетей связи и LTE-модемов;
- печать информации;
- передача данных между сегментами корпоративной сети с разным уровнем обеспечения безопасности обрабатываемой информации и др.

Категории нарушителей

Для каждого определенного потенциального канала утечки должна быть определена модель нарушителя, который может реализовать угрозы информационной безопасности. В основном, когда говорят о защите от утечек, рассматривают следующие основные категории нарушителей:

- внешние злоумышленники (используют уязвимости объектов среды обработки защищаемой информации для доступа к критичной информации, используют специально разработанное программное обеспечение для удаленного управления и скрытые каналы связи);
- внутренние нарушители (целенаправленное хищение информации для ее последующей продажи);
- внутренние пользователи (неумышленные утечки защищаемой информации, связанные с некорректными бизнес-процессами и/или организационными уязвимостями).

В деле контроля потенциальных каналов утечки критичной информации современные технологии – это лишь 10%. Остальные 90% – это сложная работа, связанная с построением процессов обеспечения информационной безопасности, настройкой этих систем в соответствии с существующими реалиями и особенностями реализации бизнес-процессов конкретной компании и дальнейшей эксплуатацией

Снижение уровня рисков

Оценка рисков должна проводиться с учетом ценности информации и существующих в компании уязвимостей (организационных, эксплуатационных, технологических), которые могут быть использованы определенным на предыдущем этапе нарушителем для кражи критичной информации. По результатам оценки рисков должны быть определены меры, направленные на снижение уровня риска до приемлемого. Их перечень должен содержать меры, направленные как на выявление и предотвращение потенциальных утечек, так и на снижение вероятности возникновения ситуации, в условиях которой такая утечка возможна. К ним могут относиться:

- управление и контроль доступа к защищаемой информации (например, на основании ролевой модели, в которой все роли определены и четко формализованы в соответствии с потенциально выполняемыми действиями в рамках такой роли);
- превентивные меры, направленные на предотвращение потенциальных каналов

утечки (фильтрация сетевого трафика, контроль используемых протоколов, доступа к внешним ресурсам, запрет/контроль использования периферийных портов);
- обучение по вопросам защиты информации и правилам обработки критичной информации;
- меры правового характера (соглашения о неразглашении с четко описанной ответственностью работника/контрагента);
- авторизация передачи информации за пределы контролируемой зоны со стороны ее владельца.

Системы класса DLP

К мерам, направленным на выявление и предотвращение утечек критичной информации, в первую очередь относятся системы класса DLP (Data Leak Prevention). При недостаточной формализации процессов и знания реальных информационных потоков в компании либо эти системы могут выявлять базовые каналы утечек, связанные с непреднамеренной передачей информации легитимными пользователями, либо количество ошибок (как первого, так и второго рода) будет таким большим, что оператор системы не сможет обнаружить реальные угрозы в потоке событий, связанных со срабатыванием заданных правил выявления потенциальных инцидентов информационной безопасности.

Современные системы класса DLP позволяют определять защищаемую информацию в каналах передачи по следующим критериям:
- цифровые отпечатки;
- ключевые слова (словари) и регулярные выражения;
- машинное обучение (метод опорных векторов, метод ближайших соседей).

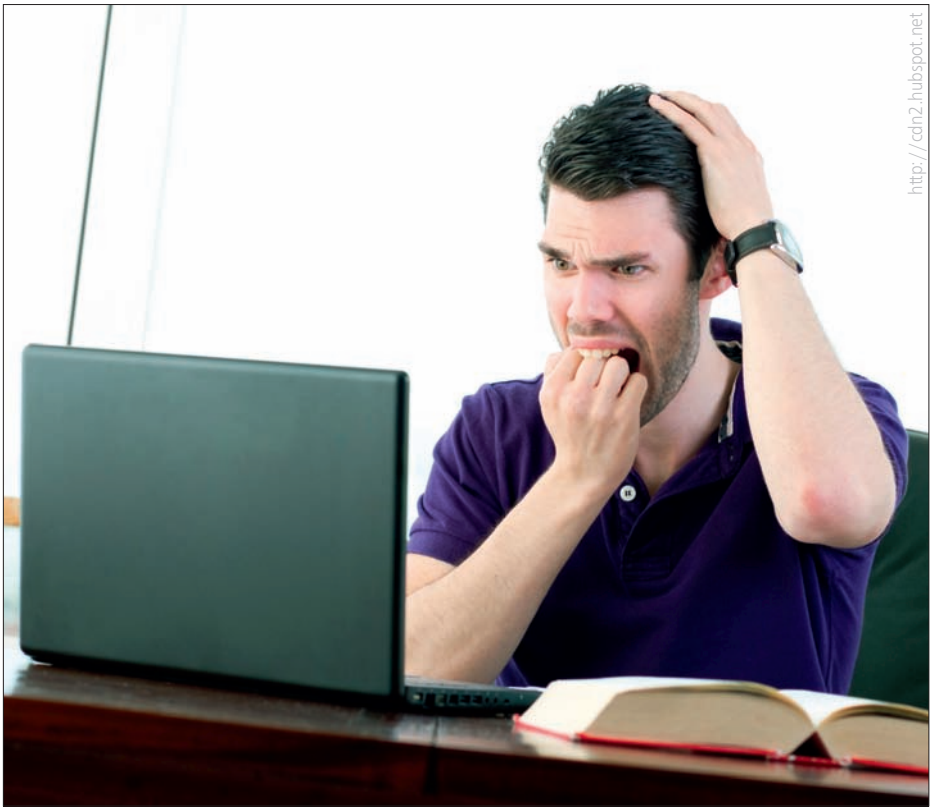
Каждый из методов обладает своими положительными и отрицательными (с точки зрения потенциальных ошибок) особенностями. Применение конкретного метода выявления и отнесения информации к защищаемой должно быть основано на ее особенностях и формах ее представления.

Большим вызовом для обеспечения безопасности критичных данных является использование скрытых каналов передачи информации (например, DNS Covert Channel) для несанкционированной передачи данных за пределы контролируемой зоны. Такие каналы, в некоторых случаях несмотря на небольшую пропускную способность, трудно выявляются и позволяют за "приемлемое с точки зрения злоумышленника" время вывести (украсть) большой объем информации.

Даже при условии применения различных методов защиты информации, которые, как правило, направлены на защиту от внешних угроз, человеческий фактор попрежнему является наиболее критичной уязвимостью.

Рекомендации и требования к защите от утечек

В целях формализации базового подхода к обеспечению защиты от утечек защищаемой информации и накопившегося опыта в апреле 2016 г. Банк России подготовил новый документ – Рекомендации в области стандартизации Банка России РС БР ИББС-2.9–2016 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Предотвращение утечек информации".



Большим вызовом для обеспечения безопасности критичных данных является использование скрытых каналов передачи информации для несанкционированной передачи данных за пределы контролируемой зоны

Рекомендации предназначены для организаций банковской системы РФ, принявших по результатам оценки рисков решение проводить деятельность по предотвращению утечек информации конфиденциального характера, и формализуют основные процессы. Они могут быть использованы как основа для определения требований к защите от утечек в любой компании.

Согласно рекомендациям Банка России процесс защиты утечек включает в себя:
- идентификацию и формирование перечня категорий информации конфиденциального характера;
- идентификацию и учет информационных активов (информационных ресурсов), содержащих информацию конфиденциального характера, и объектов среды информационных активов, используемых для обработки и (или) хранения информации конфиденциального характера;
- определение категорий возможных внутренних нарушителей и актуальных угроз, связанных с их действиями, – потенциальных каналов утечки информации конфиденциального характера;
- выполнение процессов системы обеспечения информационной безопасности, которые организуют непосредственный мониторинг и контроль информационных потоков – потенциальных каналов утечки информации конфиденциального характера.

Рекомендации содержат примеры применения описанной методологии, например Приложение В к РС БР ИББС-2.9–2016 "Пример матриц доступа для различных категорий потенциальных нарушителей" показывает перечень мероприятий по мониторингу и контролю, которые должны быть реализованы в компании по отношению к рассматриваемым каналам утечки и категориям потенциальным нарушителей.

Всесторонняя ответственность за результат

В настоящее время на рынке информационной безопасности представлено большое количество технических решений, позволяющих контролировать потенциальные каналы утечки критичной информации. Однако в решении поставленных задач использование современных технологий – это лишь 10%. Остальные 90% – это сложная работа, связанная с построением процессов обеспечения информационной безопасности, настройкой этих систем в соответствии с существующими реалиями и особенностями реализации бизнес-процессов конкретной компании и дальнейшей эксплуатацией. Реализация мер, направленных на предотвращение утечек защищаемой информации, требует проведения глубокого анализа существующих процессов в компании и вовлечения всех подразделений и владельцев информационных ресурсов. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru