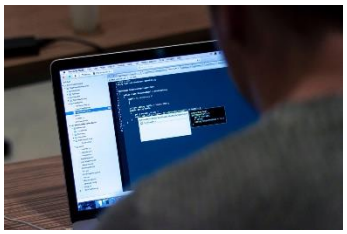
Лекция. Как эффективно ликвидировать последствия информационной утечки



Нередко при увольнении или просто ради дополнительного заработка сотрудники копируют и в дальнейшем используют в собственных интересах базы данных по контрагентам или ценные рабочие документы. Если подобное произошло в вашей компании, и вы ответственны за защиту информационных каналов утечки информации, эта для вас.

Что такое утечка информации?

Утечка данных представляет собой распространение информации, доступ к которой изначально ограничен, за пределы организации. Информационные утечки разнообразны:

- Данные о клиентской базе стали достоянием конкурентов.
- Пропали внутренние документы с грифом «секретно».
- В руки конкурентов попал финансовый план организации на будущее.
- В открытый доступ попала важная информация об особенностях производства той или иной продукции.

Информационные каналы утечки

Поиск каналов утечки информации имеет первостепенное значение для обеспечения информационной безопасности в дальнейшем. Канал утечки представляет собой путь, по которому информация прошла от первоначального источника до получателя в результате случайных или злонамеренных действий.

С технической точки зрения, каналы утраты конфиденциальных данных делятся на следующие типы:

- визуально-оптические каналы — все, что можно «подглядеть», зафиксировать с помощью фото и видео оборудования;
- акустические каналы — создание аудиозаписи с важными данными для дальнейшего несанкционированного использования;

- электромагнитные каналы, возникающие за счет различных ПЭМИН (побочное электромагнитное излучение и наводки);
- материально-вещественные каналы утечки — передача данных через дисковые и флеш-накопители, бумажные и прочие носители.

Мероприятия по ликвидации последствий утечки включают детальную проработку канала, по которому информация дошла до третьих лиц. Если утечка произошла через электромагнитный канал, необходимо произвести экранирование соответствующих технических средств. В тех случаях, когда файлы становятся добычей мошенников через рабочий компьютер, на который неизвестным образом попало вирусное программное обеспечение, вопрос о защите этого канала решают IT-специалисты организации.

Алгоритм действий по ликвидации

Когда факт утечки информации налицо, наступает время произвести внутреннюю реформу информационной безопасности. Основные характеристики происшествия, которые помогут исправить последствия утечки данных, и исключить повторное возникновение инцидента:

- какая информация и в каком количестве перестала быть конфиденциальной;
- когда была обнаружена утечка, и какое время прошло с момента события до момента обнаружения. Если об утечке данных вы узнаете со стороны, это говорит о серьезных брешах в информационной безопасности;
- кто допустил или организовал утечку информации, и с какими целями;
- как именно и кто использовал конфиденциальную информацию.

Когда картина происшедшего начинает проясняться, необходимо в срочном порядке принимать меры по исправлению ситуации. Нужно не только ликвидировать последствия слива данных, но и принять меры для исключения подобных ситуаций в будущем.

Определение масштабов утечки

О краже можно узнать двумя путями: от сотрудника, который заметил факт «слива» и с помощью специального ПО.

В первом случае ликвидировать последствия будет нетрудно: потребуется найти виновника слива и разъяснить ему какую ответственность он понесет за создание киберугрозы, а затем обезопасить канал, по которому произошла утечка.

Во втором случае утечку данных обнаружит DLP-система, которая занимается контролем информационных каналов. Встроенные инструменты аналитики DLP-системы фиксируют любое движение данных, обойти такой контроль невозможно. Даже если сотрудник будет сливать информацию скриншотами через личную переписку с телефона, система вычислит его, и виновнику придется отвечать за свои действия.

Отметим, что кража информации противозаконна, и за подобные действия можно получить вполне реальный тюремный срок. Так уже случалось и случается с предприимчивыми, но юридически неграмотными людьми во всем мире.

Поиск виновных

Утечка информации может быть случайной или преднамеренной. Когда в дело вмешивается человеческий фактор, возможны оба варианта. Вероятные пути возникновения случайных утечек:

- сотрудник открыл спам-письмо, перешел по ссылке, в результате на рабочий компьютер попал вирус, и в сеть утекла база данных;
- из-за редкой смены паролей или использования одного пароля для нескольких сервисов мошенники получили доступ к конфиденциальным данным;
- сотрудник передавал важные файлы через незащищенную сеть вайфай в кафе, информация утекла в открытый доступ.

Осознанные утечки всегда более продуманы. Это не значит, что их нельзя отследить и пресечь. Варианты развития событий:

- Осознанные утечки всегда более продуманы. Это не значит, что их нельзя отследить и пресечь. Варианты развития событий:
- сотрудник использовал дисковый или флеш-накопитель для сохранения важной информации и дальнейшего выноса данных с объекта;
- пользователь передавал конфиденциальные данные третьим лицам через свой ноутбук или смартфон, ссылаясь на то, что его гаджеты и прочие технические устройства не подпадают под действие политики безопасности компании.

Во всех перечисленных случаях обнаружить виновных поможет корректно настроенная система информационной безопасности.

Ликвидация последствий

Когда вы обнаружили утечку информации, необходимо провести комплекс мероприятий:

- определить каналы и обезопасить их для сохранности конфиденциальных данных в будущем;
- найти и наказать виновных;
- принять меры по стабилизации ситуации с учетом последствий утечки: оповестить клиентов и компаньонов о случившемся, при необходимости дать комментарии в СМИ.

Примите меры по усилению информационной безопасности для исключения утечек в будущем. Не забудьте оповестить сотрудников организации под подпись об ответственности за распространение конфиденциальных данных, чтобы в будущем не стать жертвой недобросовестности работников. Обучите сотрудников азам кибербезопасности, чтобы исключить опасность фишинга и случайного слива данных через спам и другие подобные каналы.