ДВ Капитал

30 Апреля 2013, 00:47 | Рынки

Как защитить бизнес Дальнего Востока от утечки конфиденциальной информации

Утечки конфиденциальной информации - одна из наиболее острых проблем, с которой сталкиваются все современные предприятия. Согласно Глобальному исследованию InfoWatch по утечкам информации за 2012 год, в СМИ было обнародовано 934 случая утечки конфиденциальных данных, скомпрометировано более 1,8 млрд записей, в том числе финансовые и персональные данные. Только прямые потери компаний составили более $37,8 млн.

Безусловно, компании осознают проблему, но не всегда адекватно оценивают реальный масштаб последствий от утечки информации и часто откладывают решение вопроса на потом. Что же происходит, когда утекают данные, и как бизнесу реабилитироваться после инцидента.

Клиентская база дороже золота

Самым ценным активом любой компании являются ее клиенты. Утечка клиентских данных напрямую или косвенно всегда приводит к финансовым потерям. Вероятность случайной утечки такой информации чрезвычайно мала. В подавляющем большинстве случаев персональные данные клиентов «выносятся» из компании злонамеренно ее же сотрудниками.

Все намеренные утечки можно разделить на те, которые происходят в период работы сотрудника в компании, и те, что происходят непосредственно перед увольнением. Что касается действующих сотрудников, копирующих информацию с целью ее дальнейшей перепродажи, то предотвратить инцидент можно еще в процессе их работы путем установки DLP-системы (защита данных от утечки). Если же сотрудник увольняется и уносит с собой базу данных, вероятны три сценария развития событий: 20% данных использовано не будет, 10% данных будет использовано для кросс-продаж (схожее, но не аналогичное направление), 70% данных будет использовано конкурентом для продажи аналогичных услуг. Наиболее ценной является информация по VIP-клиентам.

В зависимости от привлекательности условий по конкретной услуге клиент с определенной долей вероятности перейдет к конкуренту. Например, утечка 1000 записей кредитных карт оценивается аналитиками в среднем в 20 млн руб., и это только прямые финансовые потери от ухода клиентов! Еще порядка 130 млн рублей понадобятся на покрытие репутационных потерь.

Компенсация и устранение последствий

Одним из самых популярных информационных объектов кражи у мошенников является номер кредитной карты. Даже для небольшой утечки в размере 1000 записей затраты на устранение

последствий составят почти миллион рублей. Эти средства пойдут на обнаружение инцидента, рассылку уведомительных писем и обзвон клиентов, а также на перевыпуск кредитных карт.

Упущенная выгода

Запуск новой услуги или продукта всегда тщательно просчитывается. Компания ожидает получить отклик от нового предложения в течение определенного периода. Если об этих планах узнает конкурент и в кратчайшие сроки выйдет с более выгодным предложением, то результатом станет: упущенная прибыль, потеря клиентов и затраты в виде рекламных бюджетов, ресурсов на разработку новой услуги, планов по ее запуску и продвижению.

Защищаем информацию от утечки

Защита информации от утечек условно сводится к двум методам: ограничение доступа к корпоративным данным и отслеживание трафика. Наибольшая эффективность достигается при их совокупном использовании, для чего и применяются возможности DLP-систем.

DLP-системы отслеживают и анализируют данные, отправляемые за пределы организации через корпоративную и веб-почту, Интернет, а также системы мгновенного обмена сообщениями типа ICQ и Skype. Они позволяют офицеру безопасности контролировать отправку файлов на принтеры и копирование информации на съемные носители. При нарушении политики безопасности процесс передачи документа и данных может быть заблокирован.

DLP-технологии могут с высокой точностью детектировать конфиденциальные данные и определять тематику документов и сообщений, передаваемых за пределы организации. Правда, на это способны лишь немногие системы, в основе которых лежит комплексный анализ, например InfoWatch Traffic Monitor Enterprise.

Это решение позволяет не только предотвратить утечку конфиденциальной информации, но и расследовать ИБ-инциденты, связанные с неправомерными действиями сотрудников, выявить злоумышленников, лиц, занимающихся промышленным шпионажем. Архив всей перехваченной информации позволяет отследить маршруты ее движения, случаи нецелевого использования ресурсов организации, определить отправителя и получателя данных и является надежной доказательной базой для анализа и расследования инцидента.

Выводы

Ущерб от единичного случая утраты даже небольшого объема конфиденциальной информации может составлять сотни миллионов рублей. Стоимость же внедрения и обслуживания DLP-системы соизмерима с размером только прямых потерь от одного среднего инцидента. Следовательно, использование таких систем имеет ощутимый экономический эффект и помогает компаниям серьезно сэкономить на ликвидации последствий инцидента.

Хотите узнать подробнее, как экономить на утечках информации?

Пишите на Andrey.Dankevich@infowatch.com или обращайтесь к нашим партнерам в Дальневосточном федеральном округе:

ООО «Системы информационной безопасности»

Адрес: 630009 г. Новосибирск, ул. Добролюбова, 16, корп. 2, оф. 206, тел.: 8 (383) 354-22-54, 206-12-09, e-mail: info@sib-nsk.net

Адрес в г. Владивостоке: 690950 г. Владивосток, ул. Тигровая, 29, оф. 11,тел. 8 (914) 696-80-82, e-mail: prim@sib-nsk.net