Deloitte.

Предотвращение утечек информации

Управление рисками организаций

Деятельность современных организаций требует хранения и использования все больших объемов информации, чему способствует снижение стоимости вычислительной мощности, пропускной способности сетей и систем хранения. Вместе с этим растут риски утечки информации, давление со стороны регулирующих органов и ожидания заинтересованных лиц в отношении защищенности информации.

Разглашение конфиденциальной информации может привести к убыткам, повлечь за собой предусмотренную законодательством ответственность, а также повредить репутации за счет публикаций в СМИ и широкой общественной огласки. С учетом растущих рисков промышленного шпионажа и кражи интеллектуальной собственности организациям необходимо предпринять следующие незамедлительные меры:

- определить используемую информацию;
- оценить последствия и вероятность утечки;
- выработать стратегию предотвращения утечек;
- внедрить недостающие средства защиты информации.

Определение используемой информации

Организации стремятся защищать информацию по двум основным причинам:

- секретность – разглашение информации может оказать негативное воздействие на бизнес;
- соответствие – разглашение информации нарушит установленные законодательные требования или договорные обязательства.

Для определения перечня секретной информации организации необходимо проанализировать основные этапы создания продуктов и оказания услуг – исследования, разработку, производство, продажи и поддержку – и выявить информацию, которая в случае опубликования или передачи конкурентам может привести к упущению выгоды, потере конкурентных преимуществ и другим последствиям для бизнеса.

Для определения информации, защита которой обеспечивает соответствие требованиям, необходимо проанализировать содержание информационного обмена между компанией и заинтересованными сторонами, такими как клиенты, поставщики, государственные органы, акционеры, кредиторы, сотрудники и руководство.

Оценка рисков утечки информации

Риск утечки информации складывается из ценности этой информации для организации и вероятности утечки.

Ценность информации определяется на основании таких критериев, как:

- последствия для бизнеса, включая существенный ущерб для репутации и потерю конкурентных преимуществ;
- стоимость необходимых ресурсов и требуемого времени для воссоздания информации;
- юридические последствия, ответственность и иски, штрафы и санкции, отзыв лицензий;
- ликвидность информации – количество лиц, заинтересованных в получении информации, и внешние ограничения для ее распространения и использования;
- актуальность информации, влияние времени на ее ценность.

Для оценки вероятности утечки информации нужно учитывать:

- количество сотрудников, сторонних лиц и организаций, имеющих доступ к информации;
- имеется ли доступ к информации на постоянной или периодической основе;
- какие специальные технические знания и средства необходимы для получения и использования информации;
- требуется ли знание предметной области, чтобы получить доступ к информации и понять ее назначение;
- какие используются организационные и технические меры предотвращения неавторизованного доступа и распространения информации и насколько они эффективны.

Стратегия реагирования и средства предотвращения

Для информации, риск утечки которой превышает допустимый для организации уровень, необходимо сформулировать стратегию реагирования. Эта стратегия должна отвечать на следующие вопросы:

- Для какой информации риски утечки можно принять как данность?
- Для какой информации хранение и обработка не являются необходимыми с точки зрения бизнеса и могут быть прекращены?
- Можно ли снизить последствия утечек информации, разделив ответственность с третьей стороной, например, застраховав риски утечки?
- Для какой информации необходимо внедрить средства предотвращения утечек с целью снижения их вероятности или потенциальных последствий? Какие средства предотвращения являются наиболее подходящими?

Средства предотвращения утечек информации должны быть выбраны исходя из целей защиты и характеристик защищаемой информации. Например, средства предотвращения утечек информации могут включать:

- системы предотвращения утечек данных для обнаружения и предотвращения неавторизованного использования или передачи конфиденциальной информации;
- шифрование файлов, электронной почты и данных в приложениях, полное шифрование диска;
- контроль доступа к периферийным устройствам, например, USB-накопителям.

Наши услуги

«Делойт» предлагает услуги в области предотвращения утечек данных, включая:

- определение информации, используемой организацией;
- оценка вероятности и последствий утечки информации;
- оценка эффективности существующих средств защиты;
- разработка стратегии реагирования на возможные утечки информации;
- содействие в выборе и внедрении средств предотвращения утечек данных.

Компания «Делойт», СНГ имеет обширный опыт оказания консультационных и аудиторских услуг в области информационной безопасности. Квалификация и опыт консультантов «Делойта» в области информационной безопасности подтверждены такими профессиональными квалификациями, как CISA (сертифицированный аудитор информационных систем) и CISSP (сертифицированный профессионал в области информационной безопасности).

Контакты

Сергей Буханов
Директор
Управление рисками организаций
+7 (495) 787 06 00
sbuhanov@deloitte.ru