Deloitte.

Предотвращение утечек информации

Как измерить риск?

Управление рисками организаций

Оценка рисков утечки информации

Большинство организаций владеют конфиденциальными данными и, следуя ожиданиям своих клиентов, акционеров, партнеров по бизнесу и надзорных органов, стараются обеспечить их защиту. Несмотря на это, количество громких случаев утечки персональных данных и конфиденциальной информации не снижается.

Разглашение конфиденциальной информации может привести к убыткам, повлечь предусмотренную законодательством ответственность, а также повредить репутации компании через публикации в СМИ и широкую общественную огласку. С учетом возрастающих рисков промышленного шпионажа и кражи интеллектуальной собственности организациям необходимо предпринять незамедлительные меры: определить, какая именно информация из сведений, которыми они владеют, является конфиденциальной, оценить эффективность существующих средств контроля, выбрать механизмы предотвращения возможной утечки данных.

Ключевые вопросы, над которыми организациям стоит задуматься:

- Конфиденциальность какой информации необходимо обеспечивать?
- Где хранится и как обрабатывается эта информация?
- Каким образом и кто ее использует?
- Каким образом снижается риск ее утечки?

Мы поможем ответить на эти вопросы

Мы используем передовые программные решения, которые помогают найти ответы на эти вопросы и посредством экспресс оценки позволяют выразить в количественной форме риски утечки информации, с которыми сталкивается организация.

Мы осуществим настройку программного решения и проведем мониторинг сети вашей организации для выявления различных типов данных, которые хранятся или передаются в нарушение существующих требований. Оценка может включать следующие действия:

1. **Используемые данные**
   Мониторинг действий пользователей для выявления инцидентов сохранения и перемещения важной информации, например, сохранение информации на USB-носителях.
2. **Передаваемые данные**
   Мониторинг сети для выявления важной информации, пересылаемой по электронной почте, через Интернет, посредством мгновенных сообщений и т. д.
3. **Хранящиеся данные**
   Сканирование и анализ хранилищ данных для определения мест хранения важной информации.

Оценка рисков состоит из четырех этапов

Этап 1. Определение требований

Совместно с клиентом мы определим основные приоритеты в области предотвращения утечки данных:

- определим информацию, утечка которой представляет собой значительный риск, а также ее отправителей и получателей;
- рассмотрим сценарии возможной утечки данных;
- определим типы данных и файловые сервера для мониторинга;
- определим основные законодательные и нормативные требования, а также внутренние регламенты, которым необходимо соответствовать.

На данном этапе помимо менеджера проекта со стороны организации, как правило, требуется участие ключевых сотрудников/владельцев данных, заинтересованных руководителей, специалистов по информационной безопасности и системных администраторов.

Этап 2. Установка и конфигурация политики мониторинга

Мы осуществим установку программного обеспечения и, используя выработанные

Данные	Ущерб от утечки	Хранящиеся данные		Используемые данные	
		Частота	Риск	Частота	Риск
Информация о клиентах	**Значительный**	Высокая 721 инцидент		Высокая 256 инцидентов	
Цены и условия продаж	**Значительный**	Очень высокая 2178 инцидентов		Высокая 1 164 инцидента	
Договоры с поставщиками	**Значительный**	Средняя 25 инцидентов		Низкая 5 инцидентов	
Информация о сотруд- никах и зарплатах	**Значительный**	Низкая 2 инцидента		Низкая 3 инцидента	

 Низкий риск

 Средний риск

 Высокий риск

 Очень высокий риск

на предыдущем этапе требования, настроим его для мониторинга заданных участков, включая рабочие станции, сеть и системы хранения данных.

Этап 3. Мониторинг
Далее мы проведем мониторинг для выявления случаев утечки данных на заданных участках. Целью данного этапа мониторинга является количественная оценка уровня риска в отношении типов данных, мест хранения, отправителей, получателей и сетевых протоколов.

Как правило, установка и настройка программного обеспечения занимает не более одного рабочего дня, а мониторинг необходимо проводить в течение двух-четырех недель.

Этап 4. Презентация результатов
По результатам предыдущих этапов мы проведем встречу с ключевыми сотрудниками/ владельцами информации и заинтересованными руководителями для обсуждения отчетов по оценке рисков утечки данных и выработки дальнейших шагов.

Мы подготовим следующие отчеты по результатам оценки рисков:

- сводная оценка рисков утечки данных на основании определенной организацией критичности данных и фактической частоты утечки;
- сравнительный анализ уровня риска в организации и в среднем по отрасли;
- оценка соответствия применимым нормативным и законодательным требованиям, включая Федеральный закон № 152-ФЗ «О персональных данных».

С учетом полученной в ходе проекта информации мы поможем подготовить обоснование необходимости совершенствования системы информационной безопасности в организации, включая внедрение специализированных программных решений.

Преимущества «Делойта»?
«Делойт» имеет обширный опыт оказания консультационных и аудиторских услуг в области управления рисками информационных технологий. Квалификация и опыт наших консультантов подтверждены такими профессиональными сертификатами, как CISA (сертифицированный аудитор информационных систем) и CISSP (сертифицированный профессионал в области информационной безопасности).

Помимо обширных знаний в области информационных систем и инфраструктуры мы также обладаем пониманием специфики бизнес-процессов, присущей различным отраслям. Это позволяет нам формулировать четкие выводы и предоставлять клиентам рекомендации, учитывающие все их потребности.

Контакты

Пол Огден
Партнер
Управление рисками организаций
+7 (495) 787 06 00 доб. 2031
paogden@deloitte.ru

Владислав Дутов
Старший менеджер
Управление рисками организаций
+7 (495) 787 06 00 доб. 5423
vdutov@deloitte.ru