DOI: 10.17117/na.2016.01.01.149

<http://ucom.ru/doc/na.2016.01.01.149.pdf>

Поступила (Received): 24.01.2016

Комиссаров И.П., Чернов Д.А., Довголенко А.А. Актуальность ИТ-консалтинга при выборе средств защиты от утечки информации в организациях

Komissarov I.P., Chernov D.A, Dovgolenko A.A.
**The relevance of IT consulting in the choice of means of protection
against information leakage in organizations**

В статье проведен анализ причин, масштабов и стоимости утечки данных в организациях, приведена статистика потери информации по причине отсутствия у компаний стратегии внедрения и развития систем безопасности. Представлен принцип работы и назначение DLP-систем. Рассмотрены несколько ведущих разработчиков решений по предотвращению утечки данных, специфика предлагаемых ими средств и подхода к их разработке. Сделан вывод о необходимости консультирования фирм сторонними экспертами при внедрении средств защиты

Ключевые слова: ИТ-консалтинг, DLP-системы, утечка информации, защита от утечки информации

The article analyzes the causes, extent and cost of data breaches in the organizations, the statistics of the loss of information due to lack of company strategy implementation and development of security systems. The principles of work and the appointment of DLP-systems. Consider a few of the leading developers of solutions to prevent data breaches, the specificity of their proposed tools and approaches to their development. The conclusion about the need for counseling firms outside experts in the implementation of remedies

Key words: IT consulting, DLP systems, information leakage, information leakage protection

Комиссаров Илья Павлович

Магнитогорский государственный технический университет им. Г.И. Носова
г. Магнитогорск, пр. Ленина, 38

Komissarov Ilya Pavlovich

Magnitogorsk state technical university named G.I. Nosov
Magnitogorsk, Lenina st., 38

Чернов Дмитрий Андреевич

Магнитогорский государственный технический университет им. Г.И. Носова
г. Магнитогорск, пр. Ленина, 38

Chernov Dmitriy Andreevich

Magnitogorsk state technical university named G.I. Nosov
Magnitogorsk, Lenina st., 38

Довголенко Арина Андреевна

Магнитогорский государственный технический университет им. Г.И. Носова
г. Магнитогорск, пр. Ленина, 38

Dovgolenko Arina Andreevna

Magnitogorsk state technical university named G.I. Nosov
Magnitogorsk, Lenina st., 38

Потеря данных является одним из основных рисков с точки зрения информационной безопасности, однако он очень часто недооценивается. В результате случайного или намеренного сбоя компания может лишиться части важной для себя информации.

Объемы потерянных данных по всему миру с 2012 г. выросли на 400 %. При этом 82% организаций все еще не уверены в своей способности восстановить данные после нарушений работы. Большинство компаний считают, что не готовы к новой эре мобильных инфраструктур, облачных сред и больших данных. Согласно результатам исследования EMC, за 2014 год потери данных и простои стоили российским организациям \$29 млрд долл.

Хотя количество случаев потери данных в целом снижается, объемы данных, утрачиваемых во время каждого инцидента, растут в геометрической прогрессии. Внедрение передовых технологий защиты данных многократно снижает вероятность нарушений работы. Поэтому для решения задач по защите данных многие компании обращаются сразу к нескольким поставщикам ИТ-услуг. Однако такой разрозненный подход к развертыванию защитных средств может только увеличить риски [9].

Организации обращаются к нескольким поставщикам ИТ-услуг, как правило, из-за отсутствия разработанной стратегии защиты данных. В таких случаях компании выбирают наиболее известных поставщиков, рассчитывая, что совокупность их ИТ-решений обеспечит необходимый уровень информационной безопасности. Однако, это неверный подход, поскольку в данном случае эти ИТ-решения могут обладать схожим функционалом и выполнять одни и те же задачи, при этом не устраняя другие проблемы обеспечения безопасности. Чтобы избежать неэффективных затрат на программное обеспечение, рекомендуется перед внедрением систем защиты информации воспользоваться консалтинговыми услугами в области ИТ [8]. Это позволит исследовать информационную инфраструктуру компании, выявить ее наиболее уязвимые места и разработать стратегию внедрения средств защиты данных, а также получить рекомендации конкретных ИТ-решений, наиболее соответствующих решаемым задачам.

На данный момент существует множество программных средств, предотвращающих утечку данных в организациях [1]. Такие средства носят название DLP-систем и основаны на соответствующих технологиях.

Предотвращение утечек (англ. Data Leak Prevention, DLP) – технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства для такого предотвращения утечек. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы [2]. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения блокируется. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков и анализом контента. Первый способ позволяет избежать ложных срабатываний, но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т.д. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются [4].

В состав DLP-систем входят компоненты (модули) сетевого уровня и компоненты уровня хоста. Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т.п.

Основной задачей DLP-систем, является предотвращение передачи конфиденциальной информации за пределы информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Кроме основной, перед DLP-системой могут стоять и вторичные (побочные) задачи.

Рассмотрим несколько фирм, чьи DLP-решения являются самыми популярными в различных формах бизнеса, и специфику предлагаемых ими программных средств.

Одна из рассматриваемых фирм, Code Green Networks, предлагает DLP-средства, спроектированные для защиты интеллектуальной собственности и информации о клиентах [3]. Отличительной особенностью является то, что компания недавно разработала доступное по цене приложение, предназначенное для малого и среднего бизнеса и филиалов [5].

Ключевые особенности DLP-пространства – мониторинг перемещающихся данных (или сети) и исследование данных, хранящихся в ИТ-инфраструктуре организации. Code Green не предлагает на данный момент исследование хранящихся данных, но планирует добавить данную функцию в будущем [6].

Фирма McAfee предлагает DLP-приложения, совмещающие в одной платформе мониторинг данных в сети и сканирование хранящейся на предприятии информации, а также средства контроля портативных устройств.

Большинство DLP-решений качественно защищают данные фиксированного формата, такие, как номера кредитных карт [7].

Еще одной компанией, чьи ИТ-решения стали одними из самых востребованных, является Vericept, один из первых разработчиков DLP-средств. Их программное обеспечение, сочетающее возможности сканирования данных и анализа контента, лучшим образом подходит для крупных предприятий.

Vericept имеет программируемые средства обнаружения и анализа контента, адаптирующиеся под требования к контенту конкретной организации, которые критичны при обнаружении неструктурированных данных, таких как IP.

Таким образом, существует множество решений проблемы утечки данных в организациях, а каждый из разработчиков соответствующих программных средств имеет собственный подход к их созданию. Вследствие этого, не существует универсального ИТ-решения, подходящего любой компании. Поэтому перед внедрением системы защиты информации необходимо провести исследование предметной области и разработать стратегию, что выгоднее всего осуществить, воспользовавшись услугами ИТ-консалтинга.

Список используемых источников:

1. Хамутских Е.Ю., Сторожева Е.В. Актуальность профилактики и противодействия радикализации Интернет-экстремизма в молодежной среде // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. Магнитогорск: Дом Печати, 2014. С. 183-187.

2. Каширин Б.А., Хамутских Е.Ю. Методика преподавания темы «Правовые основы противодействия киберэкстремизму и киберэкстремизму в среде молодежи» для студентов педагогических специальностей вузов // Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи. Магнитогорск: Дом Печати, 2014. С. 107-114.
3. Попова Е.В., Сторожева Е.В. Безопасность платёжных систем в Интернет // Теоретические и прикладные вопросы науки и образования. Ч. 1. Тамбов: Консалтинговая компания Юком, 2015. С. 120-122. URL: <http://www.ucom.ru/doc/conf/2015.01.31.01.pdf>
4. Сторожева Е.В., Давлеткиреева Л.З., Ошурков В.А., Старков А.Н., Макашова В.Н., Хамутских Е.Ю. Интегрирование сервисов облачных технологий в контексте информационной безопасности электронных платежных систем. Магнитогорск: изд-во Магнитогорск гос. техн. ун-та. им. Г.И. Носова, 2015. 149 с.
5. Бикчурина А.И., Сторожева Е.В. Применение количественных статистических инвестиционных методов оценки экономической эффективности в информационных технологиях // Теплотехника и информатика в образовании, науке и производстве (ТИМ-2015). 2015. С. 204-207.
6. Иванова А.А., Бобина Е.С., Сторожева Е.В. Применение технических программно-аппаратных средств для защиты информации в информационных системах // Антикризисные Технологии в экономике как фактор развития современного общества. Саратов. 2015. С. 25-30.
7. Измайлов Д.Г., Сторожева Е.В. Применение метода информационная экономика для оценки экономической эффективности WEB-приложения // Информационные технологии в науке, управлении, социальной сфере и медицине. Томск, 2015. С. 304-304.
8. Сторожева Е.В., Хамутских Е.Ю. К вопросу об актуальности оценки эффективности внедрения информационных систем в предприятия малого и среднего бизнеса // Информационные технологии в науке, управлении, социальной сфере и медицине. Томск, 2015. С. 299-301.
9. Скокова И.К., Сторожева Е.В. Применение IT-технологии для модернизации бизнес-процесса информационного обеспечения предприятия // Современная техника и технологии. 2015. № 3 (43). С. 29-32.
10. Аналитический центр компании InfoWatch. Компания InfoWatch. URL: <http://www.infowatch.ru/analytics>

© 2016, Комиссаров И.П., Чернов Д.А.,
Довголенко А.А.
Актуальность ИТ-консалтинга при выборе
средств защиты от утечки информации в
организациях

© 2016, Komissarov I.P., Chernov D.A.,
Dovgolenko A.A.
The relevance of IT consulting in the choice of
means of protection against information leakage
in organizations