Александр Павлович Анчишкин,
студент 2 курса Института прикладной математики и компьютерных наук,
Тульский государственный университет

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Аннотация. В работе рассматривается актуальная проблема утечки информации предприятия и экономический ущерб, который могут нанести организациям утрата конфиденциальной информации. Автором проанализированы статистические данные об утечках информации и убытках предприятий, а также рассмотрены комплексные решения защиты информационной системы предприятия от внутренних потерь информации (инсайдеров).

Ключевые слова: корпоративная сеть, экономическая безопасность, информационная безопасность, защита.**Abstract.** The article deals with topical problem of information leakage of an enterprise and the economic damage that can cause organizations to lose confidential information. The author analyzed statistical data on information leakages and enterprise losses as a result of this, and also considered complex solutions for protecting the enterprise information system from internal information losses (insiders).

Key words: corporate network, economical security, information security, protection.

В современных реалиях развития информационных систем задача защиты информации становится крайне острой для организаций в совершенно любых сферах деятельности. Это связано с тем, что на сегодняшний день информация оказывает существенное влияние на экономические выгоды организаций, при этом ее утечка может привести к существенным убыткам. Поэтому задача защиты конфиденциальных данных становится одной из актуальных на сегодняшний день.

Под утечкой информации нами понимается масштабное разглашение конфиденциальных данных работников и клиентов предприятия или информации, составляющей коммерческую тайну организации.

По данным InfoWatch за первое полугодие 2016 года обнаружено 840 случаев утечки информации, что на 16% больше прошлогоднего показателя (743 утечки). В результате скомпрометировано 1,06 млрд. персональных данных [1].

Из последствий, которые ожидают организацию в случае утечки информации, можно назвать следующие:

- Расходы на реагирование, устранение и расследование случаев утечки;
- Оплата штрафа и другие санкции регуляторов;
- Потеря репутации и упущение выгоды;
- Расходы на внедрение новых средств защиты информации;
- Затраты на возмещение ущерба клиентам из-за нарушения договора о конфиденциальности данных;
- Дальнейший ущерб от мошеннических лиц, в чьи руки попали скомпрометированные данные;

• Расходы на юридическое преследование со стороны третьих лиц, возмещение ущерба по решению суда, стоимость договоренностей во вне судебного порядка.

Отсюда следует, что масштаб убытков может быть крайне высоким, поэтому задача защиты информации должна стоять на предприятии в числе основных.

Устоявшиеся программные продукты обеспечения информационной безопасности такие как: системы обнаружения атак, межсетевые экраны, антивирусное ПО — защищают информации от внешних угроз, но не обеспечивают защиту секретных данных от внутренних злоумышленников (инсайдеров).

Разумеется, для обеспечения защиты информации в нынешних условиях требуются концептуально новые решения, учитывающие специфику современности. Первое требование — обеспечение защиты данных при мобильной работе сотрудника путем внедрения на каждое рабочее место локального агента программного обеспечения защиты данных. Это позволит программе четко понимать процессы, происходящие с данными (простое хранение, копирование, шифрование, какая-либо обработка или передача). Второе требование — гибкость продукта в ответ на стремительное развитие способов утечки информации. Третье требование — направленность продукта на защиту данных от сотрудников компании, способные осуществить преднамеренную или непреднамеренную утечку информации.

Продуктом, отвечающим этим требованиям, являются DLP-системы (Data Leak Prevention System) — системы предотвращения утечек данных. Они работают с данными, покидающими информационную систему предприятия. В случае обнаружения конфиденциальной информации в исходящем запросе активный компонент DLP-системы прерывает запрос, и сообщение не доставляется, а отдел безопасности немедленно уведомляется о попытке совершения утечки информации с указанием рабочего места.

Архитектура DLP-решений от разных разработчиков может различаться, но в целом можно выделить три основных модуля:

• модули-перехватчики и контроллеры на разные каналы передачи информации;

• локальные клиенты, устанавливающиеся на рабочие места сотрудников;

• центральный сервер управления.

Перехватчики изучают данные, выходящие за рамки корпоративной сети, находят секретные, собирают их и отправляют для обработки на управляющий сервер.

Контроллеры для изучения хранимых данных инициализируют процессы нахождения в сети конфиденциальной информации. Варианты инициализации могут быть разными: от запроса сервера контроллера до активации определенных программных агентов на разных серверах или рабочих станциях.

Также контроллеры следят за действиями пользователей на рабочих местах, изучают манипуляции сотрудников, имеющие связь с конфиденциальной

информацией, и отправляют данные потенциального факта утечки на управляющий сервер.

Агентские компоненты на рабочих местах пользователей проверяют данные в обработке и следят за выполнением правил сохранения на сменный носитель информации, отправки, печати, вставки через буфер обмена.

Управляющий сервер сравнивает приходящие от перехватчиков и контроллеров данные, прорабатывает инцидент и строит отчет.

Для точного понимания, какая информация является конфиденциальной, а какая — открытой, в систему DLP необходимо внедрить логику, на основе которой будет происходить классификация. Исходные алгоритмы DLP способствуют максимальной автоматизации и облегчению процессов самообучаемости системы. В решениях DLP имеется большой набор комбинированных методов:

- цифровые отпечатки документов (занесение сотен тысяч данных с помощью одной команды);
- цифровые отпечатки баз данных (занесение выгрузки из баз данных клиентов и другой структурированной информации);
- статистические методы (повышение обучаемости системы при повторном нарушении) [2].

Приведем пример работы DLP-системы: сотрудник Иванов предприятия «Ломаем моторы» имеет доступ к документу в виде текстового файла с содержанием ноу-хау компании (Ноу-хау «Изысканный способ сломать мотор»). Документ имеет гриф секретности выше обычного («секретно»), сотрудник имеет соответствующий уровень доступа. Совершается попытка умышленной утечки информации за пределы информационной системы организации — сотрудник Иванов отправляет со своего рабочего места с рабочей почты этот файл на почту, не подписанную грифом секретности. После нажатия кнопки «Отправить» происходит следующее:

1. Почтовый клиент формирует запрос для отправки письма на сервер;
2. После формирования письмо с содержанием проходит через перехватчик DLP-системы;
3. Перехватчик проверяет содержание письма и обнаруживает в нем куски документа грифа секретности «секретно», что сигнализирует об утечке информации;
4. Запрос почтового клиента отменяется DLP-системой;
5. Модуль отчетности оповещает соответствующий отдела компании о попытке просачения информации за пределы организации.

Из вышеизложенного сценария, несмотря на его модельность, можно увидеть, что DLP-система способна предотвратить умышленную передачу информации за пределы компании в момент совершения этой передачи. Стоит отметить, что утечка может быть и неумышленной ввиду неаккуратного пользования сотрудника своим рабочим местом — в конечном итоге на этапе «извлечения информации за периметр» система также перехватит запрос.

Однако DLP-системы не являются панацеей от утечек информации, так как следят только за активностью, связанной с конфеденциальной информацией, и не предназначены для сопоставления попыток произведения утечек. Для существенного усиления защиты информации их необходимо использовать в совокупности с т.н. SIEM-системами (Security Information and Event Management System). Технология SIEM изучает сообщения от всех подсистем информационной безопасности и находит смысловые связи, что позволяет судить о попытках неправомерного использования информации.

Функционирование SIEM-системы можно разбить на несколько уровней:

− сбор отчетов работы компонентов системы и формирование необходимых данных от различных источников;

− нормализация данных, заключающаяся в приведении событий с одинаковым смыслом к общему формату;

− корреляция событий системы, важных для обеспечения безопасности, путем нахождения связей между ними, например, подбор паролей, заражение вредоносным кодом, аномальная активность в системе, изменение критических параметров системы и т.п.;

− организация хранения лог-файлов;

− реагирование на инциденты, в том числе уведомления о важных событиях для информационной безопасности;

− визуализация инцидентов, формирование отчетных документов

Универсальность SIEM достигается благодаря ее концепции. Но для решения требуемых задач необходимы источники событий и правила корреляции. Любое событие (например, в определенной аудитории включился свет) может быть обработано системой.

Решение SIEM включает в себя, как правило, несколько компонентов:

- агенты, устанавливаемые на рабочие места сотрудников; представляют собой программное средство, собирающее журналы событий и передающее их на сервер;
- коллекторы на агентах, представляющие собой библиотеки «понимания» конкретного журнала событий или системы;
- серверы-коллекторы, предназначенные для сбора событий от множества источников;
- сервер-коррелятор, отвечающий за получение информации от агентов и обработку по правилам и алгоритмам корреляции;
- сервер баз данных и хранилища, работающий с журналами событий.

Основная цель работы SIEM — своевременное обнаружение, пресещение угроз и быстрое реагирование на них. Для этого необходимо составление правил корреляции — с учетом рисков, которые определяются компанией. Эти правила непостоянны и нуждаются в постоянном приведении к актуальности. Как и в случае с правилами для систем защиты от внешних атак, своевременно не прописанное правило для обнаружения той или иной угрозы, может привести к ее реализации и, как следствие, к утечке информации [3].

Приведем теперь пример работы SIEM-системы. Вернемся к предыдущей ситуации: сотрудник Иванов планирует вынести информацию о ноу-хау за пределы организации. Он осведомлен о DLP-системе, которая пресечет попытку передачи письма на другой почтовый адрес. Однако DLP-система ничего не сможет сделать с визуальным каналом утечки информации — ведь сотрудник может просто-напросто сфотографировать экран монитора или иным способом путем визуального снятия информации заполучить документ для передачи за пределы компании. В этой ситуации спасти предприятие от инсайдера может только SIEM-система, которая обнаружит не только факт обращения к конфеденциальной информации, но и уведомит о простое сотрудника (работа с одним документом на протяжении определенного времени), и сформирует результат сопоставления этих событий: Иванов обратился к файлу с ноу-хау, по какой-то причине держит его открытым и то и дело проматывает мышью. Благодаря словарям корреляции система пометит такое поведение как подозрительное и оповестит об этом компанию.

SIEM-системы позволяют определять связь между подозрительными событиями, в то время, когда DLP-системы работают с отдельно взятыми случаями взаимодействия с важными данными. Современной тенденцией является их совместное использование, где DLP-системы являются источниками событий для SIEM-систем.

Таким образом, построение защиты корпоративной сети от утечки информации является основополагающим фактором обеспечения комплексной безопасности предприятия. Безусловно, продукты категорий DLP-систем и SIEM-систем смогут существенно снизить риск утечки информации и предотвратят возможность упущения выгод.

СПИСОК ЛИТЕРАТУРЫ

1. Глобальное исследование утечек конфиденциальной информации в 2016 году. [Текст] / Аналитический центр Info Watch. — 2016. — URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_half_year.pdf (дата обращения: 25.03.2017).
2. Боридько И. С. Применение DLP-систем для защиты персональных данных [Текст] / И. С. Боридько, А. А. Забелиский, Ю. И. Коваленко // Безопасность информационных технологий. — 2012. — № 3. — С. 20-24.
3. Шелестова О. Что такое SIEM? [Текст] / О. Шелестова // Security Lab.ru — 2012. URL: http://www.securitylab.ru/analytics/430777.php (дата обращения: 25.03.2017).