Предотвращение утечек информации
Методы обеспечения информационной безопасности

Предотвращение утечек информации

Предотвращение утечек (англ. *Data Leak Prevention, DLP*) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

Используются также следующие термины, обозначающие приблизительно то же самое:

- Data Loss Prevention (DLP);
- Data Leak Prevention (DLP);
- Data Leakage Protection (DLP);
- Information Protection and Control (IPC);
- Information Leak Prevention (ILP);
- Information Leak Protection (ILP);
- Information Leak Detection & Prevention (ILDP);
- Content Monitoring and Filtering (CMF);
- Extrusion Prevention System (EPS).

Из этой группы пока не выделился один термин, который можно было бы назвать основным или самым распространённым.

Методы

- Распознавание конфиденциальной информации в DLP-системах производится двумя способами:
- ***анализом формальных признаков*** (например, грифа документа, специально введённых меток, сравнением хеш-функции)
- ***анализом контента***.

Первый способ позволяет избежать ложных срабатываний (ошибок первого рода), но зато требует предварительной классификации документов, внедрения меток, сбора сигнатур и т. д.

Пропуски конфиденциальной информации (ошибки второго рода) при этом методе вполне вероятны, если конфиденциальный документ не подвергся предварительной классификации. Второй способ даёт ложные срабатывания, зато позволяет выявить пересылку конфиденциальной информации не только среди грифованных документов. В хороших DLP-системах оба способа сочетаются.

Компоненты

- В состав DLP-систем входят компоненты (модули) ***сетевого уровня*** и компоненты ***уровня хоста***.
- Сетевые компоненты контролируют трафик, пересекающий границы информационной системы. Обычно они стоят на прокси-серверах, серверах электронной почты, а также в виде отдельных серверов.
- Компоненты уровня хоста стоят обычно на персональных компьютерах работников и контролируют такие каналы, как запись информации на компакт-диски, флэш-накопители и т. п. Хостовые компоненты также стараются отслеживать изменение сетевых настроек, инсталляцию программ для туннелирования, стеганографии и другие возможные методы для обхода контроля.

DLP-система должна иметь компоненты обоих указанных типов плюс модуль для ***централизованного управления.***

Задачи

- передачи конфиденциальной информации за пределы информационной системы. Такая передача (утечка) может быть намеренной или ненамеренной. Практика показывает, что большая часть ставших известными утечек (порядка 75%) происходит не по злому умыслу, а из-за ошибок, невнимательности, безалаберности, небрежности работников. Выявлять подобные утечки проще. Остальная часть связана со злым умыслом операторов и пользователей информационных систем. Понятно, что инсайдеры, как правило, стараются преодолеть средства DLP-систем. Исход этой борьбы зависит от многих факторов. Гарантировать успех здесь невозможно.

Кроме основной перед DLP-системой могут стоять и вторичные (побочные) задачи. Они таковы:

- архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;
- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, запрещенный фото-видео материал, излишних объёмов данных и т. п.);
- предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;
- предотвращение использования работниками казённых информационных ресурсов в личных целях;
- оптимизация загрузки каналов, экономия трафика;
- контроль присутствия работников на рабочем месте.

Что такое методы защиты информации?

- К методам защиты информации относят средства, меры и практики, которые должны защищать информационное пространство от угроз — случайных и злонамеренных, внешних и внутренних.
- Цель деятельности по обеспечению информационной безопасности — защитить данные, а также спрогнозировать, предотвратить и смягчить последствия любых вредоносных воздействий, которые могут нанести ущерб информации (удаление, искажение, копирование, передача третьим лицам и т. д.).

Какие существуют методы обеспечения информационной безопасности

- **Технические**

К техническим средствам защиты относятся межсетевые экраны, антивирусные программы, системы аутентификации и шифрования, регламентирование доступа к объектам (каждому участнику открывается персональный набор прав и привилегий, согласно которым они могут работать с информацией — знакомиться с ней, изменять, удалять).

- **Технические**
- К техническим средствам защиты относятся межсетевые экраны, антивирусные программы, системы аутентификации и шифрования, регламентирование доступа к объектам (каждому участнику открывается персональный набор прав и привилегий, согласно которым они могут работать с информацией — знакомиться с ней, изменять, удалять).

- **Административные**
- К этой группе защитных мер относят, например, запрет на использование сотрудниками собственных ноутбуков для решения рабочих задач. Простая мера, но благодаря ей снижается частота заражения корпоративных файлов вирусами, сокращаются случаи утечки конфиденциальных данных.

- **Правовые**
- Пример хорошей превентивной меры из сферы законодательства — ужесточение наказаний за преступления в области информационной безопасности. Также к правовым методам относится лицензирование деятельности в области обеспечения инфобезопасности и аттестация объектов информатизации.

- **Физические**
- К физическим средствам защиты относятся охранные системы, замки, сейфы, камеры наблюдения. Достаточно сравнить, какая информация защищена лучше — та, которая записана на жестком диске компьютера, работающего в сети или та, что записана на съемный носитель, запертый в сейфе.

Стройте комплексную защиту

- Чтобы поддерживать информационную безопасность на высоком уровне, необходим комплексный подход. В большинстве случаев недостаточно просто установить на рабочие компьютеры антивирусы, а на входе предприятия поставить камеру видеонаблюдения. Для эффективной защиты нужно комбинировать и применять различные средства защиты (административные, технические, правовые, физические).
- Стоит отдельно сказать ***о резервном копировании***. Благодаря ему можно быстро восстановить исходные данные, если они были утеряны или искажены в результате кибератаки или ошибки сотрудника. Резервное копирование — простой и универсальный инструмент, повышающий стабильность любой системы.

Обычно резервные копии записывают на съемные носители (которые хранят отдельно и под замком) или сохраняют в облаке, либо совмещают оба способа. В качестве дополнительной меры защиты часто применяется ***шифрование***.

Политика безопасности

- Основные принципы политики информационной безопасности:
- Предоставлять каждому сотруднику минимально необходимый уровень доступа к данным — ровно столько, сколько ему нужно для выполнения должностных обязанностей. Этот принцип позволяет избежать многих проблем, таких как утечка конфиденциальных данных, удаление или искажение информации из-за нарушений в работе с ней и т. д.
- Многоуровневый подход к обеспечению безопасности. Разделение сотрудников по секторам и отделам, закрытые помещения с доступом по ключу, видеонаблюдение, регламент передачи сведений, многократное резервирование данных — чем больше уровней защиты, тем эффективнее деятельность по обеспечению информационной безопасности. Важная роль в такой защитной системе отводится межсетевым экранам. Это «контрольно-пропускные пункты» для трафика, которые будут еще на входе отсеивать многие потенциальные угрозы и позволят установить правила доступа к ресурсам, которыми пользуются сотрудники.

- Соблюдение баланса между потенциальным ущербом от угрозы и затратами на ее предотвращение. Определяя политику безопасности на предприятии, надо взвешивать потери от нарушения защиты информации и затраты на ее защиту.
- **Важно понимать, что ни одна система безопасности не способна дать 100% гарантию на защиту данных. Но многоуровневая комплексная система защиты информации однозначно эффективнее, чем применение отдельных методов обеспечения информационной безопасности.**

DLP-системы и закон

- Практически во всех странах охраняется законом право на тайну связи и право на тайну частной жизни (приватность, privacy). Использование DLP-систем может противоречить местным законам в некоторых режимах или требовать особого оформления отношений между работниками и работодателем. Поэтому при внедрении DLP-системы необходимо привлекать юриста на самом раннем этапе проектирования.
- Взаимоотношения DLP-систем с российским законодательством рассмотрены в ряде работ
- Информационная безопасность также описывается в ГОСТ, например, в ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

Список DLP-систем

- Существует ряд списков DLP-систем, в которых могут упоминаться некоторые из следующих продуктов[4][5]
- Dell EMC RSA DLP
- DeviceLock DLP
- Digital Guardian TrueDLP
- Fidelis Network
- Infowatch Traffic Monitor DLP
- Kaspersky DLP
- McAfee DLP
- StaffCop Enterprise
- SearchInform DLP
- SecureTower DLP
- Solar Dozor DLP
- Symantec DLP
- Trend Micro DLP
- Zecurion DLP

- Спасибо за внимание