МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»

Институт математики, механики и компьютерных наук им. И.И. Воровича

Кафедра информатики и вычислительного эксперимента

КУРСОВАЯ РАБОТА

по предмету: «»

Выполнил:
Студент 3 курса, 8 группы Д.Ю. Проскурин

Проверил:
кем работает Кто

Ростов-на-Дону
2017

Оглавление

Введение

Глава 1

DLP системы

1.1 Что такое DLP системы

Для решения проблемы утечек данных обычно используют специальные технологии, предотвращающие возможность кражи данных из информационной системы. Эти системы получили название DLP (Data Leak Prevention, что переводится на русский как предотвращение утечек данных). Обычно под DLP-системами принимают некоторое программное обеспечение, предотвращающее потерю данных, путем обнаружения возможных нарушений доступа к конфиденциальной информации при ее передаче за пределы информационной системы. Как правило, большая часть утечек происходит благодаря человеческому фактору. Люди редко задумываются о безопасности своих действий. Этим и пользуются злоумышленники, пытающиеся получить конфиденциальную информацию некоторой фирмы. Как показывает статистика, лишь незначительная часть всех утечек происходит по злому умыслу работника или пользователя информационной системы.

Для борьбы с нежелательным копированием информации используются различные технологии. Условно их можно разделить на несколько категорий:

- стандартные меры безопасности;
- интеллектуальные (продвинутые) меры;
- контроль доступа и шифрование;
- специализированные системы DLP.

Стандартные меры безопасности

К таким мерам безопасности относится формирование Private Network (PN - частная сеть или локальная), которая позволяет создать внутреннюю сеть в внутри информационной системы, не позволяя получить доступ к информации извне и из внутренней сети к глобальной сети. Таким образом можно достаточно надежно защитить данные, при условии, что сотрудники не станут копировать данные. Однако мы живем в современном мире, в котором есть глобальная сеть — Интернет, которая во многом облегчает нам жизнь. Без нее уже трудно представить себе работу. А данный подход не предполагает доступ к всемирной паутине, иначе возникнет возможность утечки данных. Поэтому появилось расширение данной защиты — VPN (Virtual Private Network). Сеть также остается локальной, но существует некоторый сервер, через который пользователи получают доступ в Интернет, тем самым защищая себя от хакерских атак, которые возьмет на себя VPN сервер. Казалось бы все хорошо. Только нельзя забывать о вредоносном ПО, которое без проблем похитит все данные, попав на компьютер из глобальной сети. Обеспечив контроль трафика для VPN,

при которой сервер сам решает, пропускать ли ему тот или иной пакет в зависимости от выбранной политики безопасности, получаем следующую стандартную технологию защиты — Межсетевой экран (другие известные названия: сетевой экран Firewall, Брандмауэр). Для ее реализации используются специализированные программные обеспечения, которым задаются шаблоны зепрещенных соединений и правила обработки всего трафика. Однако и здесь есть проблемы с безопасностью данных. Те же самые вирусы уже давно научились передавать данные в зашифрованном или скрытом виде, применив методы стеганографии (это алгоритмы, позволяющие скрыть одну информацию в другой) . Обнаружить скрытую информацию достаточно тяжело и не всегда оказывается возможным, поэтому данную систему защиты в современном мире корректно настроить трудно.

К мерам стандартной безопасности также относят системы обнаружения вторжений (Intrusion Detection System). Это некоторое программное или аппаратное обеспечение, предназначенное для выявления неавторизованного доступа в информационную систему, в основном, через Интернет. Такие системы предназначены для обнаружения некоторых типов вредоносной активности, нарушающей безопасность системы. Обычно к такой активности относят сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Одной из самой популярной системой системой защиты является антивирусное программное обеспечение, способное найти и обезвредить программы, наносящие вред компьютеру или информационной системе. В последнее время такие средства оказывают комплексную защиту от вирусов, помогая не только исправить проблему, но и предотвратить ее появление. Поэтому такие программные обеспечения обычно содержат в себе ранее описанные средства защиты, то есть VPN, IDS, межсетевой экран. Однако нужно понимать, что на самом деле антивирусы не способны найти все вредоносное ПО, которое попадет/попало на компьютер. Они всего лишь сравнивают поведение той или иной программы с поведением уже известных вирусов. Если программа не похожа ни на один популярный зловред, то антивирусы никак не реагируют. Но это не значит, что данная программа не является вирусом. К примеру, ориентировочно в 2011 году появился вирус ProjectSauron (Trojan.Multi.Remsec.gen), ворующий данные с зараженного компьютера. Основное его направление атак — правительственные компьютеры, на которых установлены различные системы защиты, включая антивирусы. Однако до сентября 2015 года ни один антивирус не считал его опасным.

Еще одной популярной системой защитой информации является организация клиент-серверной информационной системы. Такая архитектура предполагает хранение всей важной информации на защищенном сервере, обычно в виде базы данных, а все пользователи получают к ней доступ через специальные программы-клиенты, обычно передающие информацию в зашифрованном виде и не хранящие данные на компьютерах. Таким образом возможность утечки информации достаточна минимальна, но не исключает её.

. . . . . .

О DLP, но это чуть далее.

. . . . . .

Системы подобного рода строятся на анализе потоков исходящих данных, через которые может произойти несанкионированная передача важной информации. Если некоторая программа/пользователь пытается получить несанкционированный доступ к данным, которые защищены DLP, то такая система защиты срабатывает на попытку доступа, блокируя ее и сообщая администратору данной системы защиты.

Кроме основной перед DLP-системой могут стоять и вторичные (побочные) задачи. Обычно к ним относят:

- архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;

- предотвращение передачи вовне не только конфиденциальной, но и другой нежелательной информации (обидных выражений, спама, эротики, 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;
- отслеживание благонадёжности сотрудников, их политических взглядов, убеждений, сбор компромата.

Для корректного функционирования DLP системы используют различные методы распознавания конфиденциальной информации, среди которых выделяется анализ формальных меток и контента. Первый метод защищает всю информацию, удовлетворяющую некоторым формальным условиям, к которым можно отнести тип охраняемого файла (например tex, cpp, doc), метки, устанавливаемые на требуемые файлы или значения хеш-функций. При этом требуется предварительная классификация информации и выставление меток. Однако данный метод не гарантирует максимальную защиту от утечек информации, поскольку вполне возможен пропуск новой информации, не прошедшей классификацию. Поэтому часто применяют второй метод — анализ контента. Данный метод ищет в передаваемой информации заранее установленные ключевые слова и фразы. Недостаток данного метода заключается в ложных срабатываниях, зато он является более гибким по сравнению с первым методом.

Глава 2

Классификация вирусов

2.1 Что такое вирус

Глава 3

Анализ надежности DLP систем

Заключение

Литература

[1] *Стив Макконнелл* Совершенный код. Издательство: Питер.

[2] *Джоуан Роулинг* Гарри Поттер и Узник Азкабана.

[3] *Гуссенс М., Миттельбах Ф., Самарин А.* Путеводитель по пакету LaTeXи его расширению LaTeX 2_ε. М.: Мир, 1999.

[4] *Жуков М. Ю., Ширяева Е. В.* LaTeX 2_ε: искусство набора и вёрст- ки текстов с формулами. Ростов н/Д : Изд-во ЮФУ, 2009.

[5] *Кошкин М. М.* Компьютерное моделирование супермышелов- ки // Математическое моделирование. 2009. Т. 125, No 13. С. 838– 848.