КОМПЛЕКСНЫЕ МЕТОДЫ ОРГАНИЗАЦИИ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СЕТЯХ

COMPLEX METHODS OF ORGANIZING SECURITY IN CORPOTATE NETWORKS



УДК 004.056.53

DOI: 10.24411/2658-4964-2021-10338

Курдюков Дмитрий Станиславович, студент, 2 курс, магистр, кафедра КБ-1 «Защита информации», Институт комплексной безопасности и специального приборостроения, РТУ МИРЭА, Россия, г.Москва

Kurdiukov Dmitry Stanislavovich, student, 2 course, magistrature, department CS-1 «Data protection», Institute for Integrated Security and Special Instrument Engineering, RTU MIREA.

Аннотация: Обеспечение безопасности - одна из главных задач всех отделов информационных технологий в мире. Причем речь не только утечке информации, так и о ее непосредственной модификации на серверах предприятий. Для того чтобы учесть все аспекты и при необходимости принять меры для обеспечения безопасности, необходимо четко понимать функционирование и назначение современных сетей, а также методы их защиты.

Annotation: Ensuring security is one of the main tasks of all departments of information technology in the world. Moreover, it is not only about information leakage, but also about its modifications on enterprise servers. For this, it is necessary to clearly understand how modern networks function and are defined, as well as how to protect them.

Ключевые слова: информационная безопасность, сетевая безопасность, защита информации, предприятия.

Key words: information security, network security, information protection, enterprises.

Введение

Ежегодно большое количество крупных компаний проводит титаническую аналитическую работу в сфере компьютерных преступлений. Согласно исследованиям за 2018-2019 года, подавляющее большинство инцидентов связано с халатностью собственных сотрудников компаний. Данные исследования ясно указывают на то, что предприятиям необходимо организовывать максимально комплексную защиту как от внешних, так и от внутренних источников.

Методы защиты компьютерных сетей от внутренних угроз

Зачастую самыми распространенными механизмами защиты информации в локальных сетях выступают:

Электронные цифровые подписи;

Шифрование информации;

VLAN или виртуальные локальные сети.

Шифрование — это процесс превращения открытой информации в зашифрованный вид. Обратный процесс называется - дешифрование. Процедура шифрования выполняется по строгим математическим алгоритмам, обязательной частью процессов шифрования и дешифрования является создание или генерация ключа.

Определение ключа по ГОСТ 28147-89 «Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований». Другими словами, ключ — это уникальный элемент, позволяющий зашифровать информацию и дешифровать до первоначального вида пользователям, имеющим доступ к ключу. На данный момент используются два типа шифрований: симметричное и асимметричное.

Симметричное шифрование - в процессе шифрования и дешифрования участвует одинаковый ключ. Для работы с данным типом шифрования, шифруется и дешифрующая сторона должна иметь одинаковый ключ, который

должен оставаться в секрете, в противном случае в случае его утери информация может так и остаться зашифрованной или при получении ключа сторонними лицами может быть ими расшифрована.

Асимметричное шифрование - в отличии от симметричного использует для работы два ключа:

закрытый - генерируемый владельцем информации и хранящийся у него. Данный ключ не должен быть доступен другим пользователям;

открытый - вычисляется по специальным алгоритмам из закрытого и отправляться всем желающим отправлять зашифрованные сообщения.

Любой пользователь может зашифровать информацию с помощью открытого ключа, однако расшифровать ее сможет только владелец закрытого.

Обязательным требованием к любому виду шифрования - является генерация случайных ключей на основе генератора случайных чисел. Это служит гарантом того, что потенциальный злоумышленник не сможет прогнозировать последующие ключи. Государственные организации Российской Федерации в качестве шифрования описанный в ГОСТ 28147-89 алгоритм симметричного шифрования.

Электронная цифровая подпись - служит гарантом целостности данных и подтверждает подлинность автора информации по методу сравнивания хеш суммы оригинала информации и подлежащей проверке. Электронная цифровая подпись основана на алгоритме асимметричного шифрования. Основным преимуществом данного метода проверки подлинности является практическая невозможность фальсификации хэш-суммы. В РФ существует собственный стандарт хэш функций размером 256 бит описываемый в ГОСТ Р 34.11-94.

Зачастую подпись отправляют вместе с присущим ей файлом и помещают в его конец. После получения получатель сравнивает хеш сумму, полученную им и заявленную адресатом по специальным алгоритмам.

Виртуальные локальные сети VLAN (Virtual Local Area Network) - представляют виртуальные подсети, созданные внутри локальных сетей или групп сетей. Устройства внутри подобных сетей могут взаимодействовать друг с

другом на канальном уровне, даже находясь на большом расстоянии друг от друга. И наоборот, устройства, подключенные к одному коммутатору, но находящиеся в разных VLAN сетях не могут взаимодействовать друг с другом и не видимы друг для друга до получения соответствующих разрешений для подключения к другой VLAN.

Современные виртуальные локальные сети — это главный механизм создания логических сетевых топологий, не зависимых от их физического прародителя.

Разделение сетей по технологии VLAN имеет большее значение в сетевой безопасности благодаря четкому разграничению устройств в строго выделенным для них сегменте. Данная технология является одним из лучших средств борьбы с перехватом и подменой трафика.

Основные предназначения VLAN:

Гибкое и удобное распределение сетевых устройств по виртуальным под сетями для связи друг с другом. Одному VLAN - соответствует одно сетевое пространство. Устройства, подключенные к одному VLAN, зачастую могут находиться на огромных расстояниях друг от друга и получать защищенный

Уменьшение количества широковещательного трафика в сети - каждая виртуальная подсеть позволяет разбить один коммутатор на несколько широковещательных доменов. В случае если VLAN находиться на нескольких коммутаторах, порты этих коммутаторов также будут образовывать один широковещательный домен.

Повышение уровня сетевой безопасности и управляемости сети - с разбиением сети на VLANы, задача применения политик и правил безопасности значительно упрощается. С использованием технологии виртуальных локальных сетей политики безопасности становиться возможно применять к целым сетевым сегментам, а не к отдельным устройствам, находящимся в них. Кроме того, существует возможность применения правил и политик безопасности, разрешающих и запрещающих доступ из одного VLAN в другой.

Методы защиты компьютерных сетей от внешних угроз

В настоящее время разработано немало методов противодействия практически против всех перечисленных опасностей. Для обеспечения безопасного соединения через сеть Ethernet часто используют межсетевые экраны и виртуальные частные сети (VPN — Virtual Private Network) использующие криптографические методы шифрования трафика, передаваемого в глобальной сети Internet.

Технологии виртуальных частных сетей показали себя крайне эффективными в защите сетевого трафика. Внедрение которой в многие структуры лишь вопрос короткого времени. В большинстве современных операционных систем, а в частности, от фирмы Microsoft уже давно встраивают в свои продукты поддержку данной технологии. VPN представляет собой эмуляцию локальной сети в пространстве Internet. Для построения сети необходимо чтобы на каждом устройстве или участке сети присутствовал так называемый VPN - агент. VPN - агент представляет из себя программное средство, позволяющее устройству подключиться к виртуальной сети. Данное программное обеспечение служит для создания виртуальных каналов между устройствами или защищенными сетями так называемые «туннели» в них автоматически происходит контроль целостности и шифрование трафика, проходящего через них. Пользователи, работающие в сетях VPN при обращении к другому компьютеру, могут даже не знать, что он находится в другом городе или регионе, - разница между локальным и удаленным устройством будет только в скорости передачи данных.

В глобальной сети интернет абсолютно вся передаваемая информация представлена в виде пакетов, обрабатываемых по протоколу IP. VPN - агенты участвуют в преобразовании IP пакетов. В кратком виде работу агентов во время отправки пакетов можно представить так:

1.Анализируется получатель и выбираются алгоритмы шифрования

2.Пакет проходит обработку VPN - агентом и шифруется.

При получении пакета происходят обратные действия.

VPN-агенты работают незаметно для пользователя в автоматическом режиме, единственной сложностью является их правильная настройка, которую могут выполнить лишь очень опытными пользователями.

Межсетевые экраны - специальные программно-аппаратные или программные комплексы предназначены для фильтрации трафика. На основе установленных правил фильтрации, основанных на политиках безопасности каждой организации, межсетевые экраны принимают решение касательно каждого проходящего через них пакета информации: разрешить дальнейшую передачу или запретить.

Межсетевые экраны обычно работают на одном из следующих принципов:

Запрет доступа внешнего трафика из сети Internet или сторонней Сети и разрешение доступа в обратном порядке;

Разрешение ограниченного доступа из внешних сетей во внутренние определенных служб или авторизированных систем, таких как почтовые сервера или хранилища данных;

На данный момент не существует единой или общепризнанной классификации межсетевых экранов, однако их можно выделить по их функционалу:

фильтрующие маршрутизаторы;

шлюзы сеансового уровня;

шлюзы уровня приложений.

Фильтрующие маршрутизаторы - представляют собой серверное программное обеспечение или модифицированные маршрутизаторы, сконфигурированные на фильтрацию входящих и исходящих пакетов. Фильтрация осуществляется на основе содержащейся в заголовках TCP и IP информации такой как:

IP-адрес отправителя;

IP-адрес получателя;

порт отправителя;

порт получателя.

Шлюзы сеансового уровня - представляют собой ретрансляторы TCP - соединения. Шлюзы способны принимать запросы от авторизованного клиента и после проверки разрешений устанавливают соединение с местом запроса. После чего шлюз копирует пакеты в обоих направлениях и не препятствует нормальной передаче информации. Данные устройства позволяют заранее сконфигурировать доступ для любого сервиса и впоследствии вести мониторинг передаваемых данных.

Шлюзы сеансового уровня приложений - используется для фильтрации на прикладном уровне. И служит как своеобразный буфер между клиентом и приложением, с которым он устанавливает связь. И может быть сконфигурирован для выбранных приложений.

Подобные устройства позволяют обеспечить надежную защиту, поскольку взаимодействия с внешним миром происходит через несколько контролируемых и уполномоченных приложений. Однако стоит отметить, что шлюзы уровня приложений для корректной работы требуют отдельное приложение для каждого контролируемого сетевого сервиса.

Заключение

В данной статье было рассмотрено обеспечение безопасности в локальных сетях. Для начала были выделены основные цели сетевой безопасности, что в свою очередь дало возможность рассмотреть вероятные угрозы, а также методы их противодействию. На основе проведенного анализа были выделены необходимые базовые компоненты для построение защищенных корпоративных телекоммуникационных сетей:

сети должны быть поделены на сегменты VLAN;

на границах сетевых сегментов должно присутствовать специальное защитное оборудование в виде межсетевых экранов;

должны быть разработаны требования и инструкции для повышения технической грамотности персонала что положительно скажется, уменьшив вероятность совершения ошибок с их стороны.

Само собой, некоторые решения выглядят слегка параноидальными, однако их реализация не сильно повышает стоимость развертки систем безопасности и не требует каких-либо особых умений от специалистов безопасности.

Литература

1. Максимов. В Межсетевые экраны. Способы организации защиты // Безопасность. - 2003. - N 3. - С. . 68 ; КомпьютерПресс. - s, 2003, , rus. - НТБ СГТУ.
2. Куроуз.Д. Росс.К Компьютерной сети. Настольная книга системного администратора // Эксмо. 2016г.
3. Сергеев А. Н. С 32 Основы локальных компьютерных сетей // Учебное пособие. — СПб.: Издательство «Лань», 2016. — 184 с.: ил. — (Учебники для вузов. Специальная литература).
4. Таненбаум. Э, Уезролл. Д Компьютерные сети // 5-е изд. СПБ.: Питер, 2012. -960с.
5. В.Г. Грибунин, В.В. Чудовский. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений // М.: Издательский центр «Академия», 2009.
6. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
7. ГОСТ Р 34.11-94 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования.

Literature

1. Maksimov. In Firewalls. Methods of organizing protection // Security. - 2003. - N 3. - S. 68; ComputerPress. - s, 2003,, rus. - NTB SSTU.
2. Courage D. Ross. To the Computer Network. System administrator's handbook // Eksmo. 2016
3. Sergeev AN With 32 Fundamentals of local computer networks // Textbook. - SPb .: Publishing house "Lan", 2016. - 184 p .: ill. - (Textbooks for universities. Special literature).

4. Tanenbaum. Uh, Wesroll. D Computer networks // 5th ed. SPB .: Peter, 2012. - 960s.
5. V.G. Gribunin, V.V. Chudovsky. Integrated information security system at the enterprise: textbook. manual for stud. higher. study. institutions // M .: Publishing Center "Academy", 2009.
6. GOST R 28147-89. Information processing systems. Cryptographic protection. Algorithm for cryptographic transformation.
7. GOST R 34.11-94 Information technology (IT). Cryptographic information protection. Hash function.