Анализ проблем информационной безопасности в компьютерных сетях

Андрей Гавриленко, Владимир Караваев

Кафедра безопасности информационных технологий,
Харьковский национальный университет радиоэлектроники,
УКРАИНА, г. Харьков, пр. Науки, 14,
E-mail: andrii.havrylenko@nure.ua,
E-mail: volodymyr.karavaiev@nure.ua

Краткая аннотация – This article is devoted to information security in computer networks. The article discusses the security problems of computer networks and describes the recommendations for fixing vulnerabilities.

Ключевые слова – сеть, безопасность, кибербезопасность, политики безопасности, MikroTik, Ubiquiti, шифрование, VPN, IDS, Firewall.

I. Введение

Компьютеры и интернет стали неотъемлемой частью работы любой организации. Вся информация об организации, а так же результаты ее деятельности хранятся на компьютерах, что делает их интересными для злоумышленников, желающих каким-либо образом полчить выгоду из хранящейся на них информации.

Именно поэтому каждая организация должна контролировать свою информационную систему, чтобы обеспечить ее защиту и предотвратить возможные несанкционированные вторжения и атаки.

II. Актуальность проблемы

Когда компьютерная сеть не защищена должным образом, она становится уязвима для злонамеренного использования или случайного повреждения. Хакеры, недовольные сотрудники или плохая цифровая гигиена в организации может положительно повлиять на утечку персональных данных, включая коммерческие секреты и личные данные клиентов.

Например, потеря конфиденциальных исследований может потенциально обойтись организации в миллионы долларов, лишив ее конкурентных преимуществ. В то время как хакеры крадут данные клиентов и продают их для мошенничества, это создает негативную рекламу и общественное недоверие к организации.

Большинство распространенных атак на сети предназначены для получения доступа к информации, следя за коммуникациями и данными пользователей, а не для нанесения ущерба самой сети.

Но злоумышленники могут сделать больше, чем украсть данные. Они могут повредить устройства пользователей или манипулировать системами для получения физического доступа к объектам. Это оставляет имущество организации и членов группы под угрозой причинения вреда.

Грамотные процедуры обеспечения безопасности сети обеспечивают безопасность данных и блокируют уязвимые системы от внешних помех. Это позволяет пользователям сети оставаться в безопасности и сосредоточиться на достижении целей организации.

Более того, это означает, что клиенты и партнеры также могут уверенно взаимодействовать с организацией.

III. Решение проблемы

Ключевым этапом в обеспечении информационной безопасности сетей является грамотный подход к составлению политики безопасности сети.

Политика безопасности сети - это документ, котором прописаны рекомендации и методы обеспечения безопасности конкретной компании.

В конечном итоге для защиты сети необходимо реализовать различные уровни безопасности, чтобы злоумышленник должен был взломать две или более систем, другими словами, стоимость получения доступа к критически важным ресурсам, должна привышать стоимость этой информации.

Первым шагом в применении политик является определение политик, которые будут применяться. Сетевые политики определяют, как сеть должна быть реализована и настроена для оптимизации работы сотрудника, а также определяют, как реагировать при возникновении отклонений.

В контексте безопасности устройства, помимо разработки безопасности сети, разграничений доступа, компания так же должна подписать соглашение с каждым сотрудником о неразглашении сведений о развернутых устройствах внутри периметра, так же необходимо поддерживать ACL, чтобы разрешить или запретить трафик TCP и UDP, проводить регулярные исправления и обновления безопасности и т.д. [1].

Политики доступа в Интернет должны включать автоматическую блокировку всех веб-сайтов, которые были признаны неприемлемыми для пользователей компании. Кроме того, доступ в Интернет должен основываться на характере работы сотрудника.

VPN должен быть предназначен только для использования сотрудником принадлежащей организации компьютерной системы. Все виды удаленного доступа к корпоративной сети должны маршрутизироваться через VPN с действующей корпоративной лицензией, стандартной операционной системой и соответствующими исправлениями безопасности. [2]

Чтобы остановить возможное злоупотребление беспроводной сетью, должна быть обеспечена надлежащая аутентификация пользователя вместе с соответствующей заменой WEP и механизма отслеживания аномалий в беспроводной локальной сети. Кроме того, для шифрования должны использоваться меры безопасности 802.11i. [1]

IDS следует размещать для обнаружения аномалий и мониторинга несанкционированного доступа, так

как для экстремальной линии защиты брандмауэр или антивирус не достаточны. Администратор безопасности должен постоянно проверять файлы журналов системы и безопасности на предмет чего-либо подозрительного. Например, можно использовать Advance Antivirus, который имеет встроенную функцию IDS/IPS, для контроля несоответствующих прав аудита, повышенных привилегий, неправильных групп, измененных разрешений, изменений в реестре, неактивных пользователей и многого другого [3].

Данные, которые проходят по многим каналам, включая коммутатор, маршрутизаторы в сети в незашифрованном виде, уязвимы для многих атак, таких как спуфинг, переполнение SYN, сниффинг, изменение данных и перехват сеансов. Хотя вы не контролируете устройства, через которые могут передаваться ваши данные, но вы можете защитить конфиденциальные данные или защитить канал связи от доступа к данным в некоторой степени. Следовательно, использование многочисленных тактик шифрования, таких как SSL, TLS или IPSec, PGP, SSH, может зашифровать все виды связи, такие как POP, HTTP, POP3 или IMAP и FTP, поскольку пакеты SSL можно передавать через брандмауэры, серверы NAT и другие сетевые устройства без каких-либо особых соображений, кроме проверки наличия надлежащих портов на устройстве.

Определенная система или сервер, например, электронная почта, веб-сервер, база данных и т.д., которым требуется доступ к общедоступному Интернету, должны быть развернуты в выделенной подсети, которая отделена от внутренней системы извне, поскольку общедоступная система подвергается прямой атаке со стороны хакеров.

После составления политики безопасности сети, следует провести инструктаж всем пользователям сети. Так же, должен проводиться регулярный аудит политик безопасности.

Если коснуться технической реализации этого вопроса, то рынок предлагает массу вариантов, начиная от маршрутизаторов 3-4-го уровня, заканчивая системами предотвращения вторжений, сетевых фильтров от именитых производителей. Но чаще всего для руководства среднего и малого бизнеса остро стает вопрос цены обеспечения безопасности на предприятии, ведь, объективно, не все себе могут позволить покупать решения, например, тех же Cisco или Juniper, стоимость которых может достигать сотен тысяч долларов.

Но есть решения в более дешевом сегменте, с помощью которых можно реализовать практически все меры безопасности, описанные выше, это MikroTik и Ubiquiti - два известных конкурента в своем сегменте.

Среди специалистов нет однозначного ответа, что же лучше, MikroTik или Ubiquiti: все зависит от конкретного проекта, ведь если взять к примеру необходимость покрытия офиса точками доступа Wi-Fi и организацию бесшовного роуминга, то преимущество будет на стороне Ubiquiti, ведь точки доступа у них снабжены более мощными передатчиками и как показывает практика, даже при очень зашумленном эфире, они отлично справляются с передачей данных. С другой стороны, если для проекта важно не только покрытие беспроводной сетью, а еще и безопасная организация маршрутизации, настройка NAT, Firewall, создание безопасных VPN-тунелей между офисами организации, здесь, роутеры MikroTik имеют преимущество перед Ubiquiti.

Основные преимущества MikroTik: стоимость; функциональность - можно сравнивать с передовыми Cisco или Juniper; гибко конфигурируемая ОС; огромное количество документации и простое обновление; маштабируемость; единая операционная система RouterOS на всех устройствах.

К недостаткам можно отнести сложную настройку, ограничение пропускаемого трафика в 10 Гбит/с, так же отсутствует прямая гарантийная поддержка.

Выводы

В связи с ростом количества атак, осуществляемых на различные фирмы и корпорации по всему миру, сейчас, как никогда, возникает острая потребность в организации безопасного взаимодействия в сети компании. Для этого необходимо постоянно проводить аудит безопасности и вовремя устранять существующие потенциальные или реальные угрозы.

Но когда становится вопрос, с помощью чего же строить безопасность сети, зачастую ответ на этот вопрос лежит в платежеспособности фирмы и ценности охраняемой информации. Для больших корпораций, это однозначно Cisco, Juniper и другие известные бренды, что касается малого и среднего бизнеса, рекомендация остановиться на производителе MikroTik, как на самом функциональном и перспективном, в данной ценовой категории.

Литература

[1] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. / В.Ф. Шаньгин // ИД «ФОРУМ» - ИНФРА-М. – Москва, 2011.– С.383-384.

[2] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. / В.Ф. Шаньгин // ИД «ФОРУМ» - ИНФРА-М. – Москва, 2011.– С.300-306.

[3] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. / В.Ф. Шаньгин // ИД «ФОРУМ» - ИНФРА-М. – Москва, 2011.– С.258-263.

[4] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. / В.Ф. Шаньгин // ИД «ФОРУМ» - ИНФРА-М. – Москва, 2011.– С.343.