Основы обеспечения сетевой безопасности предприятий малого и среднего бизнеса

Что такое сетевая безопасность?

Обеспечение сетевой безопасности – это любые действия, направленные на поддержание удобства использования и целостности сети и данных. Сетевую безопасность обеспечивают аппаратные и программные технологии. Эффективная система сетевой безопасности управляет доступом к сети. Она противодействует различным угрозам, блокируя их проникновение и распространение в сети.

Как работает система сетевой безопасности?

Система сетевой безопасности включает в себя несколько уровней защиты как внутри сети, так и на ее периметре. На каждом уровне сетевой безопасности внедряются политики и средства контроля. Авторизованные пользователи получают доступ к сетевым ресурсам, а использование эксплойтов и внедрение угроз злоумышленниками блокируется.

Каковы преимущества использования системы сетевой безопасности?

Цифровизация изменила мир. Изменения коснулись нашего стиля жизни, досуга, подхода к работе и обучению. Каждая организация, которая хочет предоставлять услуги, необходимые заказчикам и сотрудникам, должна защищать свою сеть. Система сетевой безопасности также помогает вам защитить конфиденциальную информацию от атак. В конечном итоге речь идет и о защите репутации.

6 этапов обеспечения безопасности сети

1. Проводите мониторинг входящего и исходящего трафика на межсетевом экране и внимательно изучайте отчеты. При выявлении опасных действий не полагайтесь на оповещения. Кто-либо из команды должен уметь анализировать данные и быть готов принять необходимые меры.
2. Следите за новыми угрозами по мере их обнаружения и публикации информации о них в Интернете. Например, веб-сайт TrendWatch от Trend Micro отслеживает текущую активность угроз.
3. Регулярно обновляйте ПО межсетевого экрана и антивирусное ПО.
4. Регулярно проводите обучение сотрудников, предоставляя им информацию обо всех изменениях в политике допустимого использования. Кроме того, поощряйте «соседский дозор» для обеспечения безопасности. Если сотрудник замечает что-либо подозрительное (например, не удалось с первого раза войти в учетную запись электронной почты), то должен сразу же уведомить соответствующее лицо.
5. Установите решение для защиты данных. Устройства этого типа помогут защитить бизнес от потери данных в случае нарушения безопасности сети.
6. Обратите внимание на дополнительные решения безопасности, которые усилят защиту сети, а также расширят возможности компании.

Основы обеспечения сетевой безопасности предприятий малого и среднего бизнеса

Типы сетевой безопасности

Управление доступом

Не у каждого пользователя должен быть доступ к сети. Для защиты от потенциальных хакеров необходимо распознавать каждого пользователя и каждое устройство. После этого вы сможете обеспечить соблюдение политик безопасности. Можно блокировать не соответствующие установленным требованиям оконечные устройства или предоставить им только ограниченный доступ. Этот процесс называется контролем доступа к сети (NAC).

Антивирусы и ПО для защиты от вредоносных программ

Термин «вредоносное ПО» (сокращение от «вредоносное программное обеспечение») относится к вирусам, интернет-червям, троянам, вирусам-вымогателям и шпионскому ПО. Иногда вредоносное ПО может заражать сеть, но бездействовать несколько дней или даже недель. Лучшие антивредоносные программы не только сканируют на наличие вредоносного ПО входящий трафик, но также непрерывно отслеживают файлы впоследствии для поиска аномалий, удаления вредоносного ПО и устранения ущерба.

Безопасность приложений

Любое программное обеспечение, которое вы используете в своей организации, необходимо защищать независимо от того, было оно создано ИТ-специалистами организации или приобретено. К сожалению, любое приложение может содержать лазейки, или уязвимости, которые хакеры могут использовать для проникновения в сеть. Система обеспечения безопасности приложений включает в себя аппаратное и программное обеспечение и процессы, которые вы используете для устранения этих уязвимостей.

Поведенческая аналитика

Для обнаружения аномального поведения сети необходимо знать, как выглядит нормальное. Средства поведенческой аналитики автоматически выделяют действия, отличающиеся от нормы. Это поможет отделу информационной безопасности более эффективно выявлять индикаторы компрометации, которые создают потенциальные проблемы, и быстро блокировать угрозы.

Предотвращение утечки данных

Организации должны быть уверены, что их сотрудники не передают конфиденциальную информацию за пределы сети. Технологии предотвращения утечки данных (DLP) могут препятствовать небезопасной загрузке, переадресации или даже печати важной информации пользователями.

Защита эл. почты

Шлюзы электронной почты являются первоочередной целью для злоумышленников, которые хотят проникнуть в сеть. Хакеры анализируют личную информацию и прибегают к методам социальной инженерии для организации продвинутых фишинговых кампаний, чтобы обмануть получателей и направить их к сайтам, содержащим вредоносное ПО. Приложение для защиты электронной почты блокирует входящие атаки и контролирует исходящие сообщения для предотвращения потери конфиденциальных данных.

Межсетевые экраны

Межсетевые экраны создают барьер между надежной внутренней сетью и ненадежными внешними сетями, такими как Интернет. Они используют набор определенных правил, чтобы разрешить передачу или блокировать трафик. Межсетевой экран может быть аппаратным, программным или смешанного типа. Cisco предлагает устройства для унифицированного управления угрозами (UTM) и межсетевые экраны нового поколения, ориентированные на предотвращение угроз.

Системы предотвращения вторжений

Система предотвращения вторжений (IPS) сканирует сетевой трафик, чтобы активно блокировать атаки. Устройства Cisco IPS нового поколения (NGIPS) сопоставляют огромные объемы информации, полученной с помощью глобальной аналитики угроз. Это позволяет не только блокировать вредоносную активность, но и отслеживать путь подозрительных файлов и вредоносного ПО во всей сети для предотвращения распространения эпидемий и повторного заражения.

Основы обеспечения сетевой безопасности предприятий малого и среднего бизнеса

Безопасность мобильных устройств

Киберпреступники все чаще нацеливают атаки на мобильные устройства и приложения. В течение ближайших 3 лет 90 % ИТ-организаций смогут обеспечить поддержку корпоративных приложений на личных мобильных устройствах. Конечно, вам необходимо контролировать доступ различных устройств к сети. Вам также потребуется настраивать их подключения, чтобы сохранить конфиденциальность сетевого трафика.

Сегментация сети

Программно-определяемая сегментация классифицирует сетевой трафик и упрощает применение политик безопасности. В идеале классификация должна быть основана на идентификации оконечных устройств, а не просто на IP-адресах. Можно назначать права доступа на основе ролей, расположения и других факторов таким образом, чтобы предоставить необходимый уровень доступа авторизованным пользователям, изолировать подозрительные устройства и устранить угрозу.

Сеть VPN

Сеть VPN шифрует подключение оконечных устройств к сети, часто выполняемое через Интернет. Как правило, сети VPN для удаленного доступа используют протокол IPsec или SSL для аутентификации взаимодействия между устройством и сетью.

Безопасность веб-трафика

Решение для обеспечения безопасности веб-трафика будет контролировать использование Интернета сотрудниками, блокировать веб-угрозы и запрещать доступ к вредоносным веб-сайтам. Оно обеспечит защиту веб-шлюза на объекте или в облаке. «Безопасность веб-трафика» также относится к действиям, которые помогут вам защитить свой веб-сайт.

Безопасность беспроводного доступа

Беспроводные сети не являются настолько же безопасными, как проводные. Без строгих мер безопасности создание беспроводной локальной сети может быть похоже на размещение Ethernet-портов повсюду, включая автомобильные парковки. Для того чтобы предотвратить появление эксплойтов, необходимы продукты, специально предназначенные для защиты беспроводных сетей.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465