ЗАЩИТА WI-FI В ПРОМЫШЛЕННОЙ СРЕДЕ

БРЮС БИЛЛЕДО (BRUCE BILLEDEAUX)

Беспроводные сети сейчас используются повсеместно, включая и производственные объекты. Это очень удобно, однако возникает вопрос, насколько надежно они защищены.

В настоящее время Wi-Fi является основой коммуникаций, он вытесняет традиционный проводной Ethernet даже в узлах с активным интернет-трафиком. Благодаря своей низкой стоимости, высокой производительности и лучшей безопасности, в большинстве применений он становится даже более предпочтительным, чем сотовая связь. Wi-Fi предоставляет множество возможностей для коммуникации, но при этом открывает и новые направления для потенциальных кибератак. Защита сети — не самая сложная задача, однако она требует особой ответственности от тех, кто производит установку оборудования.

НЕМНОГО ИСТОРИИ

Если говорить в общем, то Wi-Fi — это беспроводная локальная сеть (Local Area Network, LAN), которая использует стандарты IEEE 802.11. Собственно, Wi-Fi — это торговая марка, которой владеет разработчик системы Wi-Fi Alliance. В 1999 г. IEEE (Institute of Electrical and Electronics Engineers, Институт инженеров по электротехнике и электронике) опубликовал стандарт 802.11b, который описывал первый механизм беспроводной передачи данных с относительно высокой скоростью (по крайней мере, на то время) от 1 до 2 Мбит/с. Стандарт быстро получил широкое распространение, так как все основные соединения до этого были проводными.

Для промышленных приложений Wi-Fi предоставил огромный потенциал для внедрения удобной высокоскоростной коммуникации, хотя конечные устройства все равно использовали собственные запатентованные последовательные протоколы. О безопасности на тот момент никто не задумывался. В то время связь была в основном по принципу «точка–точка», и для этого использовались удаленные терминалы Modbus или им подобные. Возможно, хакеры и хотели бы взломать систему для создания точки подключения, однако в то время в сети не было данных, которые представляли бы для них интерес.

РАЗВИТИЕ ТЕХНОЛОГИИ

В то время как персональные компьютеры и другие информационные технологии находили все большее применение в промышленной автоматизации, Ethernet не подвергался никаким изменениям. Нормой стало использование TCP/IP (Transmission Control Protocol/Internet Protocol), но по-прежнему поверх него использовались специализированные протоколы, такие как EtherNet/IP, Modbus TCP/IP, Profinet и др. В то же время корпоративные сети предприятий требовали подключений к индустриальной части сети, однако большие расстояния по-прежнему этого не позволяли. Теперь стало возможным создать прямую связь между низкоуровневыми устройствами на производстве и корпоративной сетью.

Хакеры быстро осознали, что производственные сети являются менее защищенными, чем корпоративная сеть предприятия. Похищение данных из производственной сети было очень простым делом, поскольку злоумышленники могли и здесь использовать методы, разработанные ими для локальных сетей, но в большинстве производственных сетей по-прежнему просто не было ничего для них интересного.

ПРОДВИЖЕНИЕ ТЕХНОЛОГИИ WI-FI В РАМКАХ ПРЕДПРИЯТИЯ

Развертывание Wi-Fi в большинстве промышленных сред сразу привело к возникновению специфических проблем. В целом, это по-прежнему были простые соединения «точка–точка», где организация проводного соединения оставалась нецелесообразной или слишком дорогой. Новая технология была развернута там, где ранее применялись только оригинальные протоколы и методы связи, поскольку была дешевле и проще в использовании. Корпоративные ИТ-специалисты обычно не имели представления о том, что нужно предпринять, когда после сканирования сетевого окружения новые беспроводные сети внезапно появились в списке доступных.

Ранние сети Wi-Fi уже имели предусмотренную возможность защиты, но чаще всего, чтобы не возиться со «скучными» паролями, сеть оставалась незащищенной. До 2003 г. доступной системой безопасности оставался алгоритм WEP (Wired Equivalent Privacy), который включили в стандарт IEEE 802.11, и тогда он уже был нацелен на широкий потребительский рынок (таблица).

Поначалу этого было вполне достаточно, чтобы соседи не вошли в вашу домашнюю сеть, но инструменты для взлома нашлись достаточно быстро. В 2003 г. появилась защита сетей Wi-Fi с помощью алгоритма WPA, который использовал протокол TKIP (Temporal Key Integrity Protocol — «протокол целостности временного ключа»). Он оказался достаточно эффективным, а дальнейшая его замена на расширенный протокол защиты AES (Advanced Encryption Standard) привнесла еще больше улучшений в защиту. Но вскоре эти протоколы также были взломаны.

В 2006 г. проблема была решена введением WPA2. В качестве замены TKIP был использован AES с дополнительным блоком, обеспечивающим режим сцепления счетчика с протоколом блочного шифрования с кодом аутентичности сообщения

ТАБЛИЦА. СТАНДАРТЫ БЕЗОПАСНОСТИ IEEE 802.11

Период использования, гг.	Протокол	Эффективность
1999–2003	WEP	Просто взломать, используя обычные инструменты
2003–2006	WPA совместно с TKIP или AES	Лучше, чем WEP, но может быть взломан
С 2006 и до настоящего времени	WPA2 совместно с AES и CCMP	Трудно взломать

(CCMP). Но даже для этого протокола была доказана возможность взлома, хотя это уже требовало крайне много времени и усилий.

ПРЕНЕБРЕЖЕНИЕ БЕЗОПАСНОСТЬЮ

Хотя WPA2 отчасти и решает проблемы хакерских атак, по крайне мере технически, этот протокол не всегда подходит для решения практических вопросов. Большинство Wi-Fi-маршрутизаторов (роутеров) имеют возможность обратной совместимости, что позволяет пользователю сконфигурировать настройки устройства для использования устаревшей технологии безопасности.

Высококачественный промышленный защищенный маршрутизатор может работать много лет в жестких условиях эксплуатации, характерных для промышленных предприятий, потому даже сейчас достаточно просто найти устройства, продолжающие работать еще с 2002 г. Но маршрутизаторы, выпущенные более десяти лет назад, имели только один метод защиты беспроводного трафика (WEP). Большинство тех, кто внедрял в те годы данное оборудование на предприятиях, были обычным обслуживающим персоналом, а не специалистами ИТ-подразделения. Они устанавливали новые маршрутизаторы и включали шифрование WEP как на новом, так и на существующем оборудовании, не особо вникая в нюансы обеспечения безопасности. Безопасность есть безопасность, правильно? Беспроводная сеть появилась в списке доступных сетей как защищенная, стало быть, мы защищены, значит все сделано правильно…

Некоторые компании даже не устанавливали беспроводные сети на предприятии. Поэтому, чтобы решить проблему, обслуживающий персонал должен был подключать маршрутизатор непосредственно к программируемому логическому контроллеру (ПЛК) или к локальной сети предприятия. Компании, придерживающиеся политики максимальной защиты, запрещали такие манипуляции, однако во многих фирмах это было обычным делом. Добросовестный технический персонал всегда убедится, что, когда работа выполнена, маршрутизатор будет отключен от сети. Но если было пропущено отключение одного из таких устройств, сеть становилась незащищенной. Если хакер обнаруживал эту небольшую и незащищенную сеть, он мог совершить вторжение в нее, что потенциально давало ему доступ к корпоративной сети в целом.

ПОЧЕМУ БЕЗОПАСНОСТЬ ТАК ВАЖНА

Хакеры пытаются проникнуть в сеть предприятия, используя наиболее уязвимые места, и незащищенная или минимально защищенная беспроводная сеть является замечательным средством достижения их преступных замыслов. Основной трудностью для хакеров является возможность подобраться к заводу так близко, чтобы можно было перехватить радиосигнал.

Если хакер сможет получить доступ только к изолированной части сети предприятия, количество причиненного ущерба, скорее всего, будет ограниченным. Гораздо более серьезные проблемы возникнут, когда через производственную сеть будет получен доступ к корпоративной сети предприятия, где хранятся наиболее важные данные.

Одной из самых обсуждаемых тем, касающихся кибербезопасности, является необходимость защиты важных данных на производстве. Информация, хранящаяся на предприятии, на самом деле может быть очень ценной, если она, к примеру, включает в себя программы для станков с ЧПУ, изготавливающих детали для авиалайнеров, или важные данные для химических процессов.

Однако данные, доступные на большинстве производств, будь то температура реактора или количество деталей, которые должны выйти из-под пресса за определенное время, не настолько ценны, что бы их воровать. Тогда зачем же хакерам взламывать промышленные сети?

Некоторые хакеры просто «из спортивного интереса» хотят нанести вред производству в любом виде, например отключить важную часть оборудования, повредить управляющую программу на ПЛК или открыть не тот клапан, чтобы создать аварийную ситуацию или панику. Эти действия вполне возможны, так что следует быть готовыми к ним.

ПРИНЦИП РАЗУМНОГО И ДОСТАТОЧНОГО

Что самое худшее может сделать хакер? Если системы управления на предприятии могут работать с вероятностью причинения вреда здоровью или безопасности, то они должны быть пересмотрены.

Это может показаться странным, однако если работа оператора в контрольном зале или проникновение киберпреступника снаружи могут действительно создать угрожающую ситуацию, а система безопасности при этом не сработала и не перевела предприятие в защищенный режим, то очевидно наличие ошибок в разработке. В правильно сконструированной системе управления хакер, может быть, и создаст опасную ситуацию, однако она не будет иметь продолжительного негативного эффекта.

Эта концепция основана на пропорциональности, но и это не причина

оставлять сеть производства незащищенной, особенно беспроводную сеть. План по осуществлению киберзащиты должен быть соизмерим с объемом того, что нужно защищать. Правильно разработанной системой управления является такая система, работу которой практически невозможно нарушить, неважно, преднамеренно это делается или нет.

РАЗДЕЛЕНИЕ КОРПОРАТИВНОЙ И ПРОИЗВОДСТВЕННОЙ СЕТЕЙ

Соединение между промышленной частью сети и корпоративной ее частью обычно допускает прохождение данных вверх по цепочке. Чтобы избежать любого вмешательства кого-либо из офисных работников в деятельность производственной сети и защитить ее от вторжения хакеров со стороны корпоративной сети, обратное сообщение должно быть ограничено. Однако некоторым компаниям требуется как входящее, так и исходящее сообщение с сетью производства, например для загрузки инструкций, необходимых для осуществления производственного процесса.

Большинство ИТ-подразделений компаний могут создать барьер между корпоративной и производственной сетью. Как правило, это файервол (межсетевой экран, обеспечивающий сетевую безопасность путем контроля входящего и исходящего трафика), демилитаризованная зона DMZ (Demilitarized Zone — сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных) или VPN-сервер для контроля прохождения данных. Однако, как упоминалось выше, эти средства предназначены для контроля трафика, проходящего из корпоративной сети в производственную. Они не могут быть использованы для контроля за потоком данных из производственной сети в корпоративную.

Кроме того, помимо индивидуальной надежности конфигурации, корпоративные системы имеют высокий уровень совместимости с производственными сетями и большинством производимого оборудования, поэтому правила контроля трафика редко настроены именно так, как того требуют соображения безопасности. Таким образом, если хакер хочет проникнуть в большую корпоративную сеть, используя Wi-Fi, ему потребуется всего лишь оказаться достаточно близко, чтобы установить соединение. Если он расширит свое проникновение до уровня корпоративной сети, то сможет создать лазейку и в дальнейшем проникнуть туда уже через Интернет.

Если специалисты ИТ-подразделения беспокоятся о безопасности, они могут установить недалеко от предприятия небольшие устройства, которые имеют возможность соединяться с производственной сетью через Wi-Fi и передавать в дальнейшем информацию в важные места, используя сотовую сеть связи. Так или иначе, существует множество путей организации взаимодействия между корпоративной сетью предприятия и Wi-Fi-сетью производства.

ВАРИАНТЫ РЕШЕНИЯ ПРОБЛЕМ

Конечно же, всегда первоочередным фактором являются внимательность и ответственное поведение персонала предприятия. Но мы также рекомендуем не пренебрегать следующими действиями:

- Замените все маршрутизаторы, выпущенные до 2006 г., на более современные.
- Настройте все сети на использование WPA2.
- Используйте сложные пароли.

Рассмотрим данные меры подробнее.

Маршрутизаторы с годом выпуска до 2006 г. все еще могут отлично работать, однако если они не поддерживают защищенный доступ с использованием WPA2, то должны быть заменены на более новые. Более того, если маршрутизатор был выпущен позднее 2006 г., это еще не означает, что он будет поддерживать шифрование WPA2, потому обязательно проверьте наличие этой опции. Если все маршрутизаторы, установленные в вашей компании, имеют поддержку WPA2, сделайте этот протокол используемым по умолчанию и принудительно выставьте его использование на всех маршрутизаторах. Далее, следует помнить, что критичным при создании пароля являются его длина и разнообразие символов, включая цифры, использование литер верхнего и нижнего регистра и т. д. В большинстве случаев для доступа к беспроводной сети требуется пароль не менее чем из 13 символов различного типа. Кроме того, следует понимать, что пароль, каким бы сложным он ни был, совершенно бесполезен, если написан на клочке бумаги, приклеенном к маршрутизатору.

Управление паролями должно быть организовано самым серьезным образом. Единственный сотрудник, который может (и должен) знать все пароли доступа, — это системный администратор конкретной сети. В его обязанности входит немедленная их смена (блокировка), как только соответствующий работник увольняется. Не забывайте: недовольный сотрудник гораздо более опасен, чем самый квалифицированный хакер, потому что он/она могут обладать очень важными знаниями о том, как все работает и как оно настроено. Отстраненный от работы сотрудник может предоставить такие данные квалифицированному хакеру, и это будет наихудшим вариантом развития событий.

Упомянутые меры безопасности эффективны, просты в реализации и недороги. Персонал, ответственный за Wi-Fi и другие сети на предприятии, может и должен поддерживать соответствующий уровень безопасности, внося, тем самым, важнейший вклад в работу компании.