О ВОЗМОЖНОСТЯХ ПРЕДОТВРАЩЕНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ НА ОСНОВЕ WI-FI ТЕХНОЛОГИЙ

Калинин Денис Дмитриевич
Бусыгин Сергей Евгеньевич
Московский технологический университет (119454, г. Москва, Проспект Вернадского, д.78) e-mail:rector@mirea.ru

На сегодняшний день беспроводные компьютерные сети получили широкое распространение. Одновременно повысилась актуальность создания методик по противодействию угрозам безопасности для этого вида сетей. В данной статье проведена классификация основных типов угроз безопасности беспроводного подключения и предложена методика защиты от возможных атак и угроз для компании, реализующей прямые продажи.
Ключевые слова: Беспроводные сети, угрозы, безопасность

About the possibility of preventing information security threat NETWORKS FOR WI-FI TECHNOLOGY BASED

Kalinin Denis Dmitrievich
Busygin Sergey Evgenyevich
Moscow University of Technology (119454, Moscow, Vernadsky Prospekt d.78) e-mail: rector@mirea.ru

Today, wireless computer networks became widespread. At the same time it increased the urgency of creating Address Threats to Security methods for this type of networks. In this paper, the classification of the main types of wireless security threats and proposed methods of protecting against possible attacks and threats to a company that sells direct sales
The Key Words:Wireless network, threats, security

Введение

На сегодняшний день компьютерные сети стали привычным средством коммуникации, а также инструментом для обмена информацией. Наибольшее распространение получили беспроводные сети на основе технологии IEEE 802.11, известной как Wi-Fi. Сеть стандарта IEEE 802.11 – это тип локальной вычислительной сети, который с целью передачи данных использует высокочастотные радиоволны.

Преимуществами сетей Wi-Fi являются несложное построение локальной сети, гибкость установки (сеть можно построить там, где нет возможности протянуть кабели), возможность перемещения пользователей в области действия сигнала, при этом оставаясь подключенными к сети. Также данная технология обеспечивает в одно и то же время доступ большого количества абонентов к сети Интернет. Таким образом, технология Wi-Fi ориентирована, в первую очередь, на организацию точек быстрого доступа в Интернет для пользователей мобильных устройств. Беспроводные сети часто используются в общественных местах (аэропорты, метро, вокзалы, кафе, торговые центры и т.д.). Сети Wi-Fi применяют крупные и мелкие предприятия для создания внутрикорпоративных сетей или подсетей. С распространением сетей с беспроводным доступом возникли и угрозы безопасности этого вида сетей. В данной статье проведена классификация основных типов угроз безопасности беспроводного подключения и предложена методика защиты от возможных атак и угроз для компании, реализующей прямые продажи.

Компании, занимающиеся прямыми продажами, обычно имеют множество агентов, которые имеют прямой доступ к базе данных информационной системы компании со своих мобильных устройств. Это накладывает определенные требования на формирование политики информационной безопасности компании.

Для построения методики по выстраиванию политики информационной безопасности рассмотрим возможные источники возникновения угроз, классифицируем их с точки зрения минимизации потерь и определим основные мероприятия по защите от информационных угроз.

Классы угроз

Под угрозой информационной безопасности понимается совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействием на нее. Угрозы информационной безопасности, возникающие в связи с использованием сетей Wi-Fi, можно разделить на два класса: прямые и косвенные. Прямые угрозы

Прямые угрозы информационной безопасности возникают непосредственно при передаче данных по беспроводному стандарту IEEE 802.11.

К этому классу относятся, например, такие угрозы, как подбор злоумышленником пароля к точке доступа, перехват пакетов в сети Wi-Fi и их последующая расшифровка, блокирование информации, а также ее возможное искажение. В технологии Wi-Fi предусмотрены аутентификация и шифрование, но данные элементы защиты не всегда обеспечивают надежную безопасность сети. На данный момент зачастую используется WPA2 - протокол шифрования, представляющий собой улучшенную разработку WPA, представленный в 2004 году компанией Wi-Fi Alliance.

Еще не так давно казалось, что беспроводная сеть, защищенная с помощью технологии WPA2, вполне безопасна. Подобрать простой ключ для подключения действительно возможно. Но если установить по-настоящему длинный ключ, то взломать его не помогут ни радужные таблицы, ни даже ускорения за счет GPU. Но, оказалось, что подключиться к беспроводной сети можно и без этого — воспользовавшись недавно найденной уязвимостью в протоколе WPS. Задумка создателей WPS хороша. Механизм автоматически задает имя сети и шифрование. Таким образом, пользователю нет необходимости лезть в веб-интерфейс и разбираться со сложными настройками. А к уже настроенной сети можно без проблем добавить любое устройство (например, ноутбук): если правильно ввести PIN, то он получит все необходимые настройки. Это очень удобно, поэтому все крупные игроки на рынке (Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL) сейчас предлагают беспроводные роутеры с поддержкой WPS.

PIN-код состоит из восьми цифр — следовательно, существует 10 в восьмой степени (100 миллионов) вариантов для подбора. Однако количество вариантов можно существенно сократить. Дело в том, что последняя цифра PIN-кода представляет собой некую контрольную сумму, которая высчитывается на основании семи первых цифр. В итоге

получаем уже 10 в седьмой степени вариантов. Но и это еще не все! Оказывается, проверка PIN-кода осуществляется в два этапа. Он делится на две равные части, и каждая часть проверяется отдельно! Время полного перебора PIN-кодов составит от нескольких часов до нескольких суток, в зависимости от реализации WPS на роутере.

Методы аутентификация

Аутентификация - это процесс установления подлинности и подтверждения запроса клиента (обычно это ноутбук) для доступа к сети или сетевой точке доступа. После выполнения аутентификации и предоставления доступа клиент получает доступ к сети. В таблице 1 приведены базовые методы аутентификации, а в таблице 2 - классы атак.

Таблица 1. Базовые методы аутентификации.

Открытая аутентификация (англ. Open Authentication)	Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, т.е. по сути это защита беспроводной Wi-Fi сети на основе ограничения доступа, что не безопасно. Используемые шифры: без шифрования, статический WEP, CKIP.
Аутентификация с общим ключом (англ. Shared Key Authentication)	Необходимо настроить статический ключ шифрования алгоритма WEP (англ. Wired Equivalent Privacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети. Схема аутентификации с общим ключом уязвима к атакам «Man in the middle». Алгоритм шифрования WEP – это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа. Используемые шифры: без шифрования, динамический WEP, CKIP.

Аутентификация по MAC-адресу	Данный метод не предусмотрен в IEEE 802.11, но поддерживается большинством производителей оборудования, например D-Link и Cisco. Происходит сравнение MAC-адреса клиента с таблицей разрешённых MAC-адресов, хранящейся на точке доступа, либо используется внешний сервер аутентификации. Используется как дополнительная мера защиты. IEEE начал разработки нового стандарта IEEE 802.11i, но из-за трудностей утверждения, организация WECA (англ. Wi-Fi Alliance) совместно с IEEE анонсировали стандарт WPA (англ. Wi-Fi Protected Access). В WPA используется TKIP (англ. Temporal Key Integrity Protocol, протокол проверки целостности ключа), который использует усовершенствованный способ управления ключами и покадровое изменение ключа.
Wi-Fi Protected Access (WPA)	После первых успешных атак на WEP было принято разработать новый стандарт 801.11i. Но до него был выпущен “промежуточный” стандарт WPA, который включал в себя новую систему аутентификации на базе 801.1x и новый метод шифрования TKIP. Существуют два варианта аутентификации: с помощью RADIUS сервера(WPA-Enterprise) и с помощью предустановленного ключа (WPA-PSK) Используемые шифры: TKIP (стандарт), AES-CCMP (расширение), WEP (в качестве обратной совместимости).
WI-FI Protected Access2 (WPA2, 801.11I)	WPA2 или стандарт 801.11i – это финальный вариант стандарта безопасности беспроводных сетей. В качестве основного шифра был выбран стойкий блочный шифр AES. Система аутентификации по сравнению с WPA претерпела минимальные изменения. Также как и в WPA, в WPA2 есть два варианта аутентификации WPA2-Enterprise с аутентификацией на RADIUS сервере и WPA2-PSK с предустановленным ключом. Используемые шифры: AES-CCMP (стандарт), TKIP (в качестве обратной совместимости).

Cisco Centralized Key Managment (CCKM)	Вариант аутентификации от фирмы CISCO. Поддерживает роуминг между точками доступа. Клиент один раз проходит аутентификацию на RADIUS-сервере, после чего может переключаться между точками доступа. Используемые шифры: WEP, CKIP, TKIP, AES-CCMP

Таблица 2. Классы атак.

Пассивная	К пассивным атакам относится анализ трафика, отслеживание незащищенных сеансов обмена данными, расшифровка плохо зашифрованного трафика и перехват данных аутентификации (например, паролей). Пассивный перехват сетевых операций позволяет злоумышленникам спланировать будущие действия. Пассивные атаки позволяют злоумышленнику получить доступ. к информации или файлам данных незаметно для пользователя или без его согласия. Примеры таких атак: раскрытие личной информации (номер кредитной карты или данные о состоянии здоровья).
Активная.	К активным атакам относятся попытки обойти или нарушить средства защиты, внедрить злонамеренный программный код, украсть или изменить информацию. Эти атаки нацелены на магистраль сети, они включают расшифровку информации в процессе ее передачи, электронное проникновение в закрытые области или атаку на авторизированного удаленного пользователя, когда он пытается подключиться к закрытой области. Активные атаки приводят к раскрытию и распространению файлов данных, отказу в обслуживанию или модификации данных.
С близкого расстояния	При атаках с близкого расстояния группа лиц находится в непосредственной близости от сетей, систем или технических средств с целью изменения и сбора информации, либо для провокации отказа в доступе к информации. Непосредственная физическая близость к сети достигается путем тайного проникновения в сеть, открытого доступа или сочетания обоих методов.

Внутренняя.	Внутренние атаки могут быть злонамеренными или случайными. Злонамеренные внутренние пользователи намеренно перехватывают, воруют или повреждают информацию, используют информацию с целью мошенничества или отказывают в доступе другим авторизированным пользователям. Случайные атаки обычно являются результатом беспечности, отсутствия знаний или намеренного обхода системы безопасности для выполнения задания.
Распреде-ленная	Распределенные атаки нацелены на злонамеренную модификацию аппаратного или программного обеспечения во время производства и распространения. Во время таких атак злонамеренный программный код (черный ход) внедряется в продукт для получения неавторизованного доступа к информации или функциям системы на будущее.

Угрозы и меры противодействия им

Следующие угрозы считаются физическими:

1.Угрозы аппаратного обеспечения. Это угрозы физического повреждения аппаратной части маршрутизатора или коммутатора. Сетевое оборудование Cisco, предназначенное для решения ответственных задач, следует располагать в коммутационных отсеках или в компьютерных залах, соответствующих следующим минимальным требованиям:

1. Помещение должно запираться, и доступ к нему должен иметь только уполномоченный персонал.
2. К помещению не должно быть доступа через подвесной потолок, фальшпол, окна, воздуховоды или любую другую точку, кроме защищенного входа.
3. По возможности используйте электронный контроль доступа, причем все попытки входа должны заноситься системой безопасности в журнал и отслеживаться службой безопасности.
4. По возможности сотрудники службы безопасности должны контролировать происходящее в помещении с использованием камер слежения с автоматической записью.

2.Угрозы со стороны окружающей среды. К ним относятся такие угрозы, как предельные температуры (слишком высокие или слишком низкие) или крайние значения влажности (слишком низкая или слишком высокая). Для предотвращения повреждения сетевых устройств Cisco по условиям окружающей среды предпримите следующие шаги:

1. Установите в помещении надежную систему контроля температуры и влажности.
2. Всегда проверяйте рекомендуемые параметры окружающей среды для всего сетевого оборудования Cisco в документации по изделию, поставляемой в комплекте с ним.
3. Удалите из помещения все источники электростатических и магнитных помех.

4. По возможности дистанционно отслеживайте параметры окружающей среды в помещении и предусмотрите подачу предупреждающего сигнала.

3.Электрические угрозы. К ним относятся такие угрозы как всплески напряжения, недостаточное напряжение в сети (провалы напряжения), колебания напряжения (шум) и полное отключение питания. Проблемы электропитания можно свести к минимуму, выполняя следующие рекомендации:

1. Установите системы бесперебойного питания для критически важных сетевых устройств Cisco.

2. Установите аварийный генератор электрического тока для критически важного оборудования.

3. Планируйте и выполняйте регулярные процедуры тестирования и технического обслуживания систем бесперебойного питания и генераторов с учетом предложенного производителем расписания профилактического обслуживания.

4. Установите для важных устройств избыточные системы электропитания.

5. Отслеживайте все параметры, связанные с электропитанием, на уровне источника питания и на уровне устройства, и предусмотрите подачу предупреждающего сигнала.

3. Эксплуатационные угрозы. К эксплуатационным угрозам относится неправильное обращение с основными электронными компонентами, отсутствие важных запасных частей, плохая прокладка кабеля, небрежная маркировка и т. д. Эксплуатационные угрозы образуют большую группу, которая охватывает множество ситуаций. Для предотвращения эксплуатационных угроз выполняйте общие правила, перечисленные ниже:

1. Все кабели оборудования должны иметь четкую маркировку и крепиться на стойках с оборудованием для предотвращения случайного повреждения, отключения или нештатного прерывания.

2. Используйте кабелепроводы и направляющие для прокладки кабеля между стойкой и потолком или между стойками.

3. При замене внутренних компонентов маршрутизаторов и коммутаторов или при работе с ними всегда следуйте процедурам по предотвращению электростатического разряда.

4. Храните запас важных запчастей для аварийных ситуаций.

5. Не оставляйте консоль, если она подключена к любому консольному порту и зарегистрирована на нем. Покидая станцию, всегда выполняйте выход из интерфейса администратора.

6. Помните, что закрытость помещений не может быть единственной необходимой защитой устройств. Всегда помните, что ни одна комната не может обеспечить полную безопасность. Когда злоумышленники окажутся в защищенном помещении, ничто не сможет

помешать им подключить терминал к консольному порту маршрутизатора или коммутатора Cisco.

4. Получение доступа. При проведении атак с целью получения доступа используются известные уязвимые места в службах аутентификации, службах FTP и сетевых службах для получения доступа к учетным записям в сети, конфиденциальным базам данных и другой защищаемой информации.

5. Атаки подбором пароля. «Атакой подбора пароля» называют многократные попытки вычислить учетную запись пользователя, пароль или то и другое. Эти многократные попытки называются «переборным криптоанализом». Атаки подбором пароля также осуществляются с использованием других методов, например, программ типа «троянский конь», фальсификации IP-адреса и анализа пакетов.

Риск нарушения безопасности возникает, когда пароли хранятся в незашифрованном виде. Для устранения рисков необходимо шифровать пароли. В большинстве систем пароли обрабатываются алгоритмом шифрования, в результате чего для паролей генерируется односторонняя хэш-функция. Из одностороннего хэша невозможно получить исходный текст. Большинство систем не дешифруют сохраненный пароль во время аутентификации: они хранят одностороннюю хэш-функцию. При входе в систему вводится учетная запись и пароль, и алгоритм шифрования пароля генерирует одностороннюю хэш-функцию. Алгоритм сравнивает эту хэш-функцию с хэш-функцией, сохраненной в системе. Если они совпадают, алгоритм делает вывод, что пользователь ввел правильный пароль.

Помните, что при обработке пароля этим алгоритмом получается хэш пароля. Хэш это не зашифрованный пароль, а результат работы алгоритма. Преимущество хэша заключается в том, что значение хэша можно восстановить только при наличии сведений об исходном пользователе и пароле, а получение исходной информации из хэша невозможно. Это преимущество делает использование хэшей идеальным для хранения паролей. При выполнении авторизации сравниваются и вычисляются не пароли, а их хэши.

Для уменьшения угроз атак с подбором пароля можно использовать следующие рекомендации:

1. Не позволяйте пользователям применять одинаковый пароль в разных системах. Большинство пользователей применяет один пароль для доступа ко всем системам, включая личные системы.

2. Отключайте учетные записи после некоторого числа неудавшихся попыток входа в систему. Это помогает предотвратить попытки подбора пароля.

3. Не используйте незашифрованные пароли. Используйте либо одноразовые пароли, либо зашифрованные пароли.

4. Используйте «сильные» пароли. Сильные пароли состоят по меньшей мере из восьми символов и содержат заглавные и прописные буквы, цифры и специальные символы. Многие современные системы время поддерживают сильные пароли и могут потребовать от пользователя использования только такого пароля.

Методика противодействия угрозам для компании прямых продаж

Данный анализ был проведен с целью выбора оптимального решения для определенной компании. Компания занимается продажей компьютерного оборудования, имеет свой интернет магазин, склад выдачи заказов, с возможностью контроля статуса заказа через внутренний интернет ресурс. Клиент может, находясь на складе, подключиться к внутренней беспроводной сети (используя данные выданные после оплаты заказа) и в режиме реального времени следить на какой стадии находится процесс сборки его заказа, а также получить уведомление о готовности выдачи компьютерного оборудования. Рассматриваемая компания состоит из 10 сотрудников компании, которые пользуются ноутбуками, телефонами, портативными компьютерами, а также неограниченное количество клиентов, прибывшие получать заказ. Компания располагается в одноэтажном офисе-складе площадью в 140 кв.м. Содержит 2 точки доступа Wi-Fi. В данной компании содержится достаточное количество информации, которую нужно обезопасить от угроз злоумышленников. Например, личная информация о клиентах (паспортные данные, телефон и т.д.). Для данного решения, учитывая проведённый анализ, были выделены следующие рекомендации для предотвращения угроз потери данных через Wi-Fi:

Первым делом после организации Wi-Fi точки доступа, нужно выбрать шифрование передаваемой информации. В основном идет выбор между WPA и WPA2. Настоятельно рекомендую использовать WPA2, потому что WPA, на сегодняшний день, легко поддаётся атакам, следовательно, ведет к угрозе потери или утраты конфиденциальности данных.

Использую WPA2 вам потребуется установить пароль-ключ от 8 до 63 символов. Следует внимательно отнестись к данной процедуре и не указывать какое-то слово, или набор цифр формата “12345678…”, так как при взломе первым делом будут подбирать пароль через так называемый “словарь”. Словарь – это библиотеки содержащие часто используемые комбинации символов или слов. Лучше всего использовать генератор паролей и в нем задать количество символов, содержащие заглавные и прописные буквы, числа, символы.

Если злоумышленник получил пароль-ключ к вашей сети Wi-Fi, он может, использую web интерфейс, изменить внутренний параметры маршрутизатора , и настроить его как ему будет угодно, в зависимости от тех задач ,которое были поставлены. Чтобы обезопасить себя от данной угрозы, нужно установить логин и пароль на вход во внутренний интерфейс маршрутизатора (также часто бываю случаи, когда логин и пароль бывает «стандартным»,

например, admin-admin). Логин и пароль лучше всего, как и в случае выше, выбрать используя генератор.

Чтобы войти во внутренний интерфейс маршрутизатора в браузерной строке поиска нужно ввести IP адрес данного устройства. В большинстве случаев этот IP адрес – 192.168.1.1 или 192.168.0.1 , что без труда позволяет обратиться к интерфейсу маршрутизатору и приступить в подбору пароля для входа в него злоумышленнику. Исходя из данной информации, меняем IP адрес для входа в внутренний интерфейс маршрутизатора на любой другой.

Данные рекомендации помогут без лишних денежных затрат обезопасить компанию от перехвата важной информации. Так как, у данной компании нет прямых обязанностей в защите информации своих клиентов (законодательство), а есть только внутренние установки, связанные с потерей имиджа компании, то достаточно будет выполнить выше приведенный список рекомендаций.

Заключение

Мировые производители сетевого оборудования активно занимаются продвижением новых аппаратных и программных решений для беспроводной передачи данных. При разработке новых беспроводных продуктов приоритеты будут отдаваться безопасности, повышению удобства для пользователя в плане настроек и т.д., увеличению пропускной способности. Решение проблемы безопасности в сетях Wi-Fi сможет реально расширить круг пользователей и поднять их доверие к беспроводным сетям на принципиально новый уровень. Но проблема эта не может быть решена только посредством принятия стандартов и за счет унификации оборудования. Значительные усилия в этом направлении должны приложить поставщики услуг, требуется гибкая система безопасности, необходима настройка политик доступа, большую роль играет и грамотная работа администратора беспроводной сети. Короче говоря, следует принимать все необходимые меры и использовать все возможные способы для обеспечения безопасности. После анализа всех видов угроз и атак, была подготовлена методика защиты компании по продажи компьютерного оборудования.

Список использованной литературы:

1. Лихоносов А. Словарь-справочник по информационной безопасности. – М.: МФПА, 2010. — 390 с.

2. Олифер В. Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010 – 944 с.

3. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2012 – 960 с.

4. WPA2 на защите беспроводных сетей Wi-Fi http://www.technorium.ru/cisco/wireless/wpa2.shtml

5. Стандарты IEEE 802.11//Национальный открытый университет http://www.intuit.ru/studies/courses/1004/202/lecture/5238

6. lnterconnecting Cisco Networking Devices Part 1 2008 – 984 c.