POSITIVE TECHNOLOGIES

АТАКИ НА КОРПОРАТИВНЫЙ WI-FI

2017

Атаки на корпоративный Wi-Fi

Беспроводные сети являются неотъемлемой частью корпоративной инфраструктуры большинства современных компаний. Использование Wi-Fi позволяет разворачивать сети без прокладки кабеля, а также обеспечивает сотрудников мобильностью: подключение возможно из любой точки офиса с самых разных устройств. Определенное значение имеет и удобство клиентов компании, которым, например, необходим высокоскоростной доступ в Интернет. Развернутая беспроводная сеть позволяет организовать его быстро и комфортно.

Однако небезопасное использование или администрирование беспроводных сетей внутри организации влечет за собой серьезные угрозы. Успешный взлом Wi-Fi позволяет не только перехватывать чувствительную информацию, атаковать пользователей беспроводной сети, но и развивать атаку для получения доступа к внутренним ресурсам компании. Организация поддельных точек доступа, выход из гостевой Wi-Fi-сети в корпоративную или эксплуатация уязвимостей небезопасных протоколов аутентификации — лишь часть возможных атак из арсенала злоумышленников, эксплуатирующих беспроводные сети. Учитывая популярность таких сетей в корпоративном сегменте ущерб для бизнеса и отдельных пользователей может быть огромным.

В данном исследовании представлен обзор наиболее распространенных уязвимостей, с которыми сталкивались эксперты Positive Technologies в ходе работ по анализу защищенности беспроводных сетей в 2016 году. Работы проводились для компаний из различных сфер экономики, но как показала практика — профиль организации не влияет на уровень безопасности беспроводных сетей, который практически во всех исследованных компаниях оценивался в 2016 году либо как «низкий», либо как «крайне низкий».

В исследовании также разобраны популярные сценарии атак на Wi-Fi и представлены рекомендациями по защите от них. Демонстрируемые сценарии — далеко не все возможные, но они позволяют проследить основную цепочку действий нарушителя. Стоит также учитывать, что приведенные кейсы могут одновременно встречаться в одной и той же системе: открытая гостевая беспроводная сеть может сочетаться с использованием поддельной точки доступа, а атаки на подбор ключа безопасности нередко проводятся в сетях, доступных за пределами контролируемой зоны.

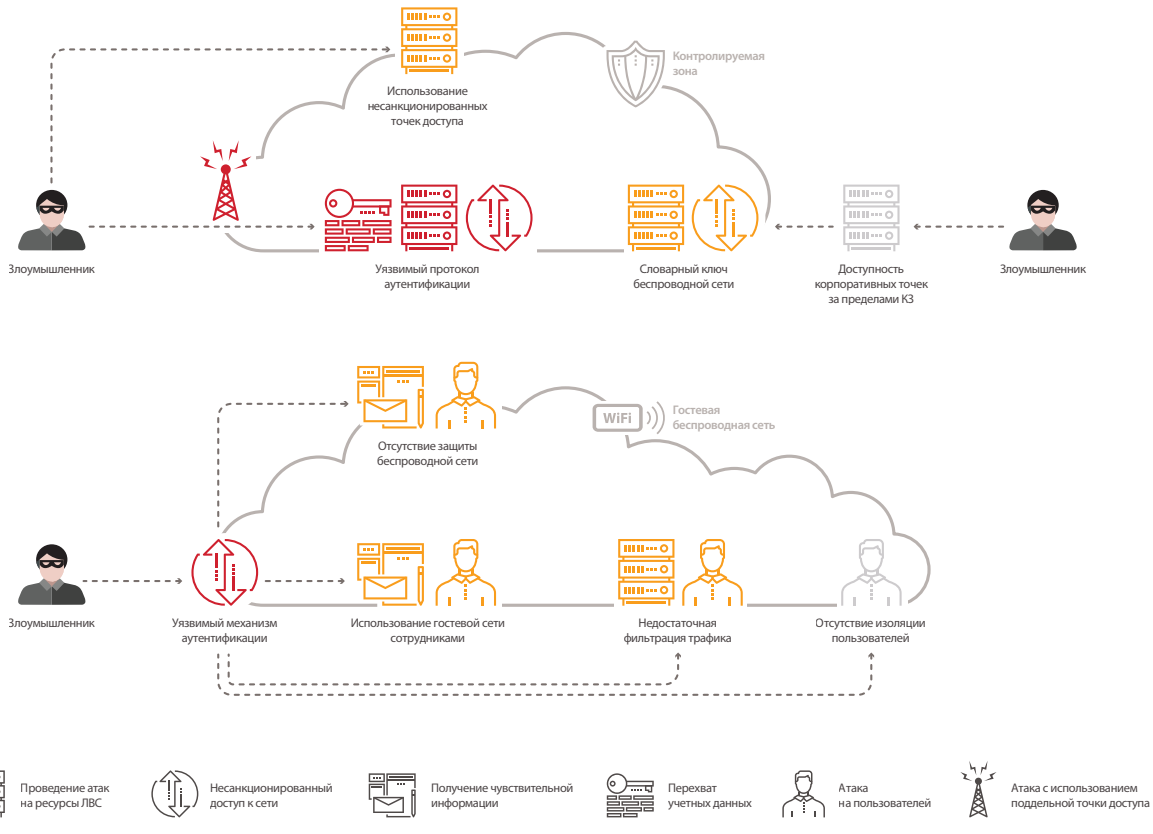


Рис. 1. Основные недостатки защиты

ИЗБЫТОЧНОЕ ПОКРЫТИЕ СЕТИ

Злоумышленник, целью которого является атака на корпоративную инфраструктуру, помимо достаточного уровня квалификации может располагать набором специализированных инструментов. В его арсенале могут быть мощные Wi-Fi-адаптеры для работы в различных частотных диапазонах, всенаправленные антенны, микрокомпьютеры для создания поддельной точки доступа, оборудование для скрытного анализа беспроводных сетей и всевозможное ПО, позволяющее проводить активный анализ безопасности Wi-Fi-сетей.

На первоначальном этапе злоумышленника могут заинтересовать данные об используемых механизмах безопасности, применяемых алгоритмах шифрования и механизмах аутентификации. Вся полученная информация в дальнейшем может быть использована непосредственно для проведения атак на инфраструктуру организации. Но это все возможно лишь в том случае, если организация беспроводного доступа проводилась без учета понятия «контролируемая зона».

Безопасное использование Wi-Fi-сетей предполагает, что они доступны только сотрудникам компании, находящимися в пределах контролируемой зоны. Но в случае если ограничения по мощности сигнала на используемых маршрутизаторах отсутствуют, доступ к беспроводным сетям может осуществляться, например, из соседнего здания или с общественной парковки. В ходе анализа защищенности беспроводных сетей специалисты Positive Technologies регулярно выявляют доступность корпоративных точек беспроводного доступа за пределами контролируемой зоны.

Злоумышленник может использовать эту возможность для проведения различных атак на ЛВС из-за пределов контролируемой зоны, в том числе атак, требующих значительных временных затрат — например, для подбора ключа безопасности. При этом нарушитель может чувствовать себя относительно спокойно — местоположение позволяет. Кроме того, он может проводить атаки с использованием поддельной точки доступа: устройства сотрудников будут переключаться на базовую станцию с более высоким уровнем сигнала (см. раздел «Поддельная точка доступа»).

Для предотвращения подобных ситуаций рекомендуется ограничивать доступность корпоративных беспроводных сетей из-за пределов контролируемой зоны. Для этого необходимо снизить мощность сигнала в настройках маршрутизатора. При отсутствии в настройках оборудования подобной конфигурации желательно использовать маршрутизаторы, в которых такая возможность предусмотрена. Другой вариант — перенести маршрутизаторы в другие внутренние помещения, чтобы их сигнал не выходил за пределы контролируемой зоны.

ПОДДЕЛЬНАЯ ТОЧКА ДОСТУПА

Мобильные телефоны, планшеты, ноутбуки при подключении к беспроводным сетям, как правило, автоматически запоминают SSID сети (ее название). А пользователи очень часто используют небезопасную настройку «Автоматическое подключение к сети Wi-Fi». Это безусловно удобно, но несет в себе потенциальную угрозу. Когда устройство окажется в зоне покрытия другой Wi-Fi-сети с тем же SSID, к ней будет автоматически осуществлена попытка подключения.

Используя эту возможность, злоумышленник создает поддельную точку доступа, после чего устройства сотрудников, оказавшиеся в зоне ее покрытия, автоматически отправляют запросы на аутентификацию. В случае если используется протокол PEAPv0/EAP-MsCHAPv2, а на стороне клиента не проверяется или проверяется некорректно сертификат точки доступа, злоумышленник может успешно проводить атаки с поддельной точкой доступа на перехват значений пары Challenge + Response, используемых в запросах на аутентификацию. Эти данные, в свою очередь, могут быть использованы для последующего получения хеша пароля методом перебора. Сами сотрудники могут и не догадываться, что становятся жертвами атаки.

Несмотря на кажущуюся сложность и множество условий, на практике подобные атаки встречаются регулярно. В рамках работ по анализу защищенности беспроводных сетей специалисты Positive Technologies успешно перехватывали аутентификационные данные с помощью подобных атак в 75% проектов.

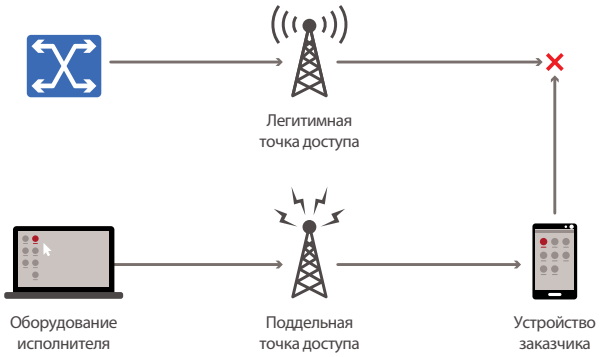


Рис. 2. Атака с применением поддельной точки доступа

Главная опасность заключается в том, что нарушителю достаточно установить свою точку доступа там, где потенциально могут находиться сотрудники атакуемой компании. Это может быть первый этаж бизнес-центра, кафе, ближайшая к офису станция метро — устройство сотрудника попытается подключиться к оборудованию злоумышленника, обнаружив сеть с сохраненным ранее значением SSID. Степень риска уязвимости достаточно высока, так как применяя данную технику, злоумышленник может получить аутентификационные данные для доступа к корпоративным ресурсам, используя массовую атаку на различные устройства за пределами контролируемой зоны.

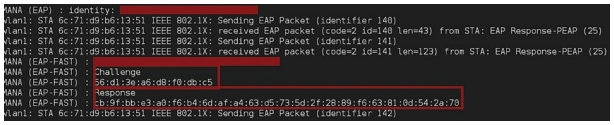


Рис. 3. Перехват пары Challenge + Response

Перехватив значение пары Challenge + Response, нарушитель может использовать суперкомпьютер для перебора 2^{56} ключей, основанных на алгоритмах DES и SHA1, и получить хеш пароля (что достаточно для аутентификации в беспроводной сети). При этом подбор будет успешным со стопроцентной вероятностью. Также злоумышленник может использовать сторонние сервисы расшифровки (цена услуги составляет порядка 200 долларов) либо провести атаку прямого перебора пароля, используя полученные значения Challenge + Response, с применением современных видеокарт (GPU) — но в таком случае успех не гарантирован.

Если беспроводная сеть подключена к ЛВС, а для доступа используется доменная учетная запись, то в случае успешного подбора пароля злоумышленник сможет развивать атаку уже во внутренней сети, получая доступ к критически важным ресурсам атакуемой инфраструктуры (например, к почте).

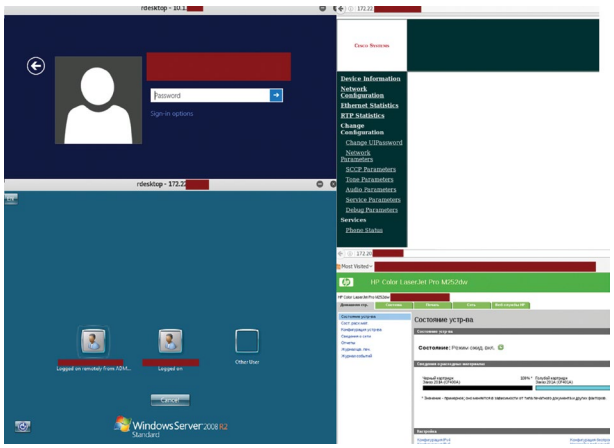


Рис. 4. Доступ к ряду ресурсов ЛВС из гостевой беспроводной сети

Для предотвращения подобной ситуации рекомендуется использовать в корпоративной инфраструктуре безопасные методы аутентификации — например, EAP-TLS с использованием клиентского сертификата и проверкой сертификата сервера. Данный протокол требует установки клиентских сертификатов на каждое беспроводное устройство, в случае атаки с использованием поддельной точки доступа проверка сертификата будет провалена и злоумышленник не получит аутентификационные данные.

ИЗ ГОСТЕВОЙ СЕТИ В КОРПОРАТИВНУЮ

Получить ключ доступа к гостевому Wi-Fi в большинстве организаций достаточно просто. Это обычная практика, удобство клиентов или посетителей — важный аспект бизнеса, но такое удобство зачастую создается в ущерб безопасности. Как показывает опыт работ по анализу защищенности, во многих случаях после подключения к гостевой сети может быть получен доступ к другим сетевым сегментам, в том числе к ресурсам ЛВС. Некоторые системы, к которым удавалось получить доступ из гостевой беспроводной сети организаций, представлены на рис. 4.

Интересен тот факт, что сотрудники компаний сами регулярно используют гостевую сеть, не подозревая, что это небезопасно. Для гостевой сети не всегда используются механизмы шифрования. А если при этом точка доступа не изолирует пользователей друг от друга, то злоумышленник, получивший доступ к гостевой сети, может атаковать сотрудников компании, прослушивать их трафик и перехватывать чувствительную информацию, в том числе учетные данные для доступа к различным системам. Нарушитель может также сочетать эксплуатацию данного недостатка с использованием поддельной точки доступа (см. раздел «Поддельная точка доступа»).

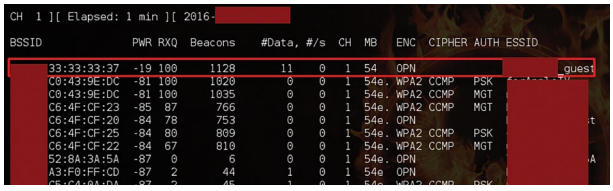


Рис. 5. Отсутствие механизмов шифрования для гостевой сети

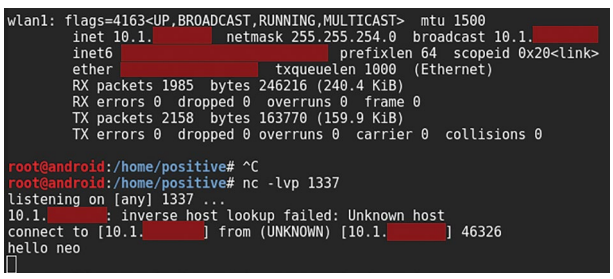


Рис. 6. Демонстрация возможности прямого обмена информации между клиентами гостевой сети

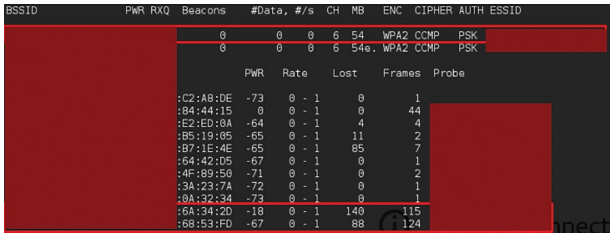
Для повышения безопасности гостевой сети необходимо использовать режим изоляции пользователей точки доступа, запрет на использование гостевой сети сотрудниками компании, а также надежные механизмы шифрования (WPA2).

НЕСАНКЦИОНИРОВАННЫЕ ТОЧКИ ДОСТУПА

Человеческий фактор всегда играет важную роль в обеспечении безопасности любой инфраструктуры, в том числе беспроводных сетей. Многие сотрудники используют Интернет для личных целей (социальные сети, почта, мессенджеры), но не в любой компании они могут получить доступ к этим ресурсам на рабочем месте — а в некоторых организациях Интернет и вовсе запрещен. Поэтому сотрудники зачастую подключаются к интересующим их ресурсам со смартфона либо, для большего удобства, разворачивают на смартфоне беспроводную точку доступа, к которой подключают рабочую станцию, и пользуются интернет-ресурсами через такое несанкционированное соединение.

В среднем три несанкционированные точки доступа выявлялись в ходе работ по анализу защищенности беспроводных сетей на каждом объекте в 2016 году. В одной из компаний обнаружено сразу 7 таких точек.

При успешной атаке на такие беспроводные сети злоумышленник способен получить доступ к ресурсам ЛВС, а также проводить атаки на пользователей этих точек доступа. Так, в одном из проектов была выявлена беспроводная сеть, которая не входила в число корпоративных сетей.



```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                     0        0    0   6  54   WPA2 CCMP   PSK
                     0        0    0   6  54e. WPA2 CCMP   PSK

                   PWR  Rate    Lost    Frames  Probe

:C2:A8:DE   -73    0 - 1      0        1
:B4:44:15     0    0 - 1      0       44
:E2:ED:0A   -64    0 - 1      4        4
:B5:19:05   -65    0 - 1     11        2
:B7:1E:4E   -65    0 - 1     85        7
:64:42:D5   -67    0 - 1      0        1
:4F:89:50   -71    0 - 1      0        2
:3A:23:7A   -72    0 - 1      0        1
:0A:32:34   -73    0 - 1      0        1
:6A:34:2D   -18    0 - 1    140      115
:68:53:FD   -67    0 - 1     88      124
```

Рис. 7. Информация о выявленной защищенной беспроводной сети

Наши специалисты перехватили значение рукопожатия (handshake) клиента и точки доступа, получив возможность проводить локально атаки на подбор пароля к данной точке доступа. Используя подобранный по словарю пароль и информацию о доступном сетевом окружении, нам удалось выяснить, что внешний IP-адрес устройства принадлежал к сети одной из сотовых компаний. В связи с этим была осуществлена успешная попытка входа в приложение «Личный кабинет» на сайте оператора сотовой связи без пароля. Оказалось, что это корпоративная учетная запись компании. При этом доступ к личному кабинету позволял устанавливать переадресацию звонков, отправлять SMS-сообщения, а также получить доступ ко входящим SMS-сообщениям.

Для предотвращения подобных ситуаций рекомендуется проводить регулярное выявление несанкционированных точек доступа в контролируемой зоне, с их последующим отключением. Рекомендуется также довести соответствующие правила безопасности до всех категорий сотрудников. Для этого необходимо разработать программу повышения осведомленности сотрудников в вопросах информационной безопасности и проводить периодическое обучение с контролем его эффективности, сделав акцент на практических аспектах обеспечения безопасности.

СЛОВАРНЫЕ КЛЮЧИ БЕЗОПАСНОСТИ

Использование словарных паролей — одна из самых распространенных уязвимостей, которую можно встретить практически в любой инфраструктуре (см. «Статистику уязвимостей корпоративных информационных систем»[1]). То же самое касается и беспроводных сетей. Используемые ключи безопасности в ряде случаев имеют недостаточную длину или сложность и могут быть без труда подобраны нарушителем. Злоумышленник может перехватить значения handshake для атакуемой точки доступа и получить возможность локально (без подключения к сети) подбирать пароль по этому значению. Успешный подбор словарных или простых комбинаций может быть произведен за несколько секунд.

[1] www.ptsecurity.com/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf

В некоторых организациях при настройке беспроводной сети задается пароль, связанный с названием компании или другими похожими данными. Для нарушителей это вовсе не преграда. Используя различное специализированное ПО (например, CeWL и RSMangler), можно провести «персонализированную» атаку на подбор. В таком случае словарь возможных паролей будет специально создан для атакуемой организации. В рамках одного из проектов специалисты Positive Technologies смогли получить доступ в ЛВС в результате атаки, в которой первым шагом был именно подбор пароля, схожего по написанию с названием компании-владельца.

```
                    Aircrack-ng 1.2 rc4

[00:00:00] 8/9822768 keys tested (102.97 k/s)

Time left: 1 day, 2 hours, 45 minutes, 1 second                0.00%

                        KEY FOUND! [ 12345678 ]

Master Key     : 9B E0 20 EF 21 4F 5D 7D 1C 7A 06 93 F1 85 86 6F
                 4B D9 D1 F1 5A 70 2F 16 05 F9 2E 71 9C 81 DF 88

Transient Key  : EB B3 2E 39 CE F2 F3 65 6A A3 D6 54 85 73 93 E2
                 29 0F 9E CE BA 66 2D 83 37 3B 76 49 86 D7 1A AF
                 1D 8F 9A DA 61 08 96 9A 20 6C A5 07 FD 29 1A E4
                 6E 49 A1 C3 E0 AB 63 7F 79 0F A1 F4 B1 DC 52 BD

EAPOL HMAC     : 6E 6C 38 2C 89 D3 C5 BE 79 55 D5 B5 5C 8B FE 2D
```

Рис. 8. Подбор пароля для доступа беспроводной сети. ПО Aircrack

Рекомендации по защите в данном случае общеизвестны: строгая парольная политика, которая требует использования стойких к подбору ключей безопасности.

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА WPS

Очередной случай, когда удобство таит в себе угрозу. Механизм WPS (Wi-Fi Protected Setup) предназначен для упрощения процесса настройки беспроводной сети. Имя сети и тип шифрования задаются автоматически, для подключения к точке доступа используется специальный PIN-код, состоящий только из цифр. Нет необходимости заниматься конфигурацией сети. При этом PIN-код может быть написан прямо на роутере. Что самое интересное — в большинстве роутеров возможность настройки по технологии WPS изначально активирована. Нарушитель может подобрать PIN-код и подключиться к точке доступа. Существует даже специализированное ПО, позволяющее не только идентифицировать точки доступа с включенным WPS, но и проводить на них атаки. Данное ПО распространяется свободно, то есть любой нарушитель может, не затрачивая никаких средств, скачать соответствующий набор утилит и приступать ко взлому.

Проблема уже неоднократно освещалась исследователями в области информационной безопасности. Тем не менее в ходе работ по анализу защищенности наши специалисты по-прежнему выявляют беспроводные точки доступа, использующие механизм WPS. В ряде случаев это позволяло получить доступ к ресурсам ЛВС.

```
[+] Sending M2 message
[P] E-Hash1: b1:98:e4:a3:34:15:55:01:1b:29:ca:47:16:23:de:b9:8e:cd:9c:a5:7e:92:f9:40:bb:f2:b3:2f:93:cf:b5:b5
[P] E-Hash2: b9:53:d3:a9:5d:bb:d4:e4:9d:b0:a5:c1:1a:0f:be:03:83:9a:d9:a5:92:54:c0:5e:4a:a7:00:ca:72:95:d5:04
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 60 seconds
[+] WPS PIN: '24301626'
[+] WPA PSK: '0890641373'
[+] AP SSID: [redacted]
```

Рис. 9. Успешный подбор PIN-кода точки доступа

Рекомендация по защите от подобных атак простая: отключать функцию WPS в настройках точки доступа.

НЕБЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ

В некоторых случаях при развертывании беспроводной сети может использоваться фильтрация по MAC-адресам подключаемых устройств. Это решение является небезопасным, позволяя проводить атаки типа «человек посередине» (MITM).

В рамках одного из проектов мы выявили беспроводную сеть, для доступа к которой реализована аутентификация с использованием веб-интерфейса, доступного по протоколу HTTPS. После успешной аутентификации запоминался MAC-адрес подключенного устройства для идентификации пакетов в сети. При последующем подключении пользователя аутентификация происходила по MAC-адресу.

Для демонстрации атаки наши специалисты, используя поддельную точку доступа, передавали запросы от пользователей к действительной точке доступа через собственное оборудование. Планшет одного из сотрудников подключился к поддельной точке доступа, а затем пользователь ввел в ложную форму аутентификации свои учетные данные, которые были перехвачены. Далее все запросы от пользователя к точке доступа передавались через наше оборудование, что позволило в скрытном режиме прослушивать трафик сотрудника, а также записать MAC-адрес рабочей станции «злоумышленника» в таблицу аутентифицированных устройств. При этом доступ к беспроводной сети позволил обращаться к другим сетевым сегментам.

Рис. 12. Форма аутентификации поддельной точки доступа

Для предотвращения подобных ситуаций рекомендуется использовать безопасные методы аутентификации (см. раздел «Поддельная точка доступа»).

Рис. 10. Форма аутентификации в беспроводной сети

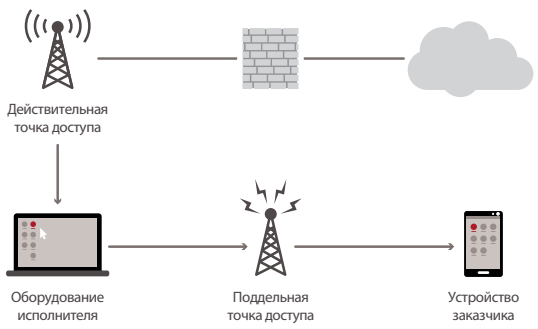


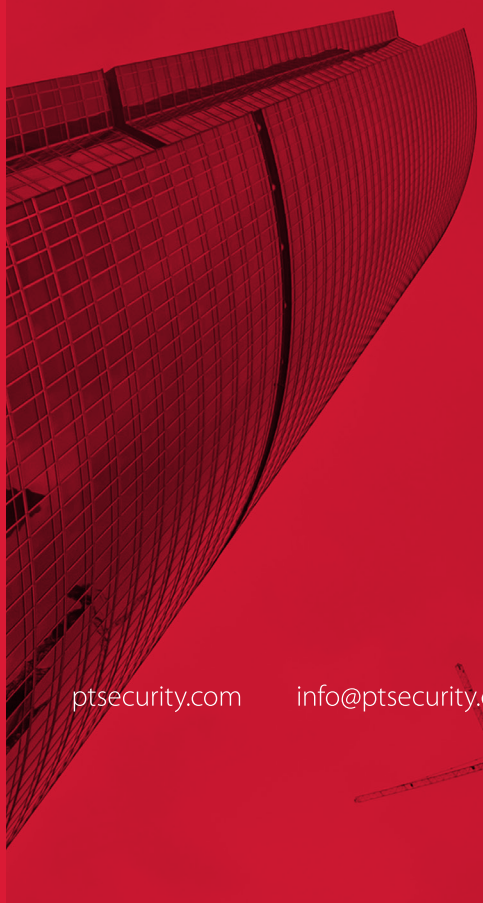
Рис. 11. Атака типа «человек посередине»

ЗАКЛЮЧЕНИЕ

Полученные результаты позволяют утверждать, что большинство компаний, в инфраструктуре которых используются беспроводные сети, не предпринимают достаточных мер по их защите. Во всех без исключения проектах по анализу защищенности специалисты Positive Technologies выявляли те или иные проблемы безопасности, и что самое важное — во всех проектах была выявлена возможность проведения через беспроводные сети атак на ресурсы ЛВС.

На практике по-прежнему регулярно встречаются случаи, когда одна ошибка ведет к компрометации всей системы. Так, в одной из компаний для корпоративных беспроводных сетей использовалась доменная аутентификация, одна из учетных записей была обнаружена в открытом виде на официальном сайте организации. При этом подключение к беспроводным сетям могло быть осуществлено из-за пределов контролируемой зоны.

Однако напрашивающийся вывод о полном отказе от использования Wi-Fi-сетей — в корне неверен. Описанные проблемы можно решить, используя комплексный подход к обеспечению информационной безопасности. Это подразумевает безопасную конфигурацию и сегментацию беспроводных сетей, безопасные методы аутентификации с проверкой сертификатов, ограничение доступа клиентов гостевой сети к ЛВС, регулярный анализ защищенности беспроводных сетей и выявление несанкционированных точек доступа с их последующим отключением. И конечно, необходимо регулярно проводить мероприятия для повышения осведомленности сотрудников в вопросах информационной безопасности.



POSITIVE TECHNOLOGIES

ptsecurity.com info@ptsecurity.com