

УЯЗВИМОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2018

СОДЕРЖАНИЕ

Введение	3
1. Резюме	4
2. Исходные данные	5
3. Статистика за 2017 год	6
3.1. Общие результаты анализа защищенности	6
3.2. Результаты анализа защищенности сетевого периметра	7
3.3. Результаты анализа внутренних ресурсов	14
4. Результаты оценки осведомленности сотрудников в вопросах информационной безопасности	16
5. Результаты оценки защищенности корпоративных беспроводных сетей	17
6. Интересные факты о словарных паролях	19
Заключение	20

ВВЕДЕНИЕ

Корпоративная IT-инфраструктура — это сложный многокомпонентный механизм, предназначенный для автоматизации бизнес-процессов компании. Доменная инфраструктура, почтовые сервисы, веб-приложения, бизнес-системы — все это является основой любой корпоративной информационной системы. В зависимости от масштаба компании и численности ее сотрудников будет различаться и размер IT-инфраструктуры. Но, несмотря на это, большая часть компаний имеет общие проблемы, связанные с обеспечением информационной безопасности информационных систем. Так, в период распространения вируса-шифровальщика WannaCry пострадало более 500 тысяч компьютеров, принадлежащих, в числе прочего, правительственным учреждениям, крупным компаниям и небольшим коммерческим организациям. Этот инцидент подтверждает, что от атак злоумышленников может пострадать абсолютно любая организация.

Данное исследование определяет основные тенденции в области анализа защищенности корпоративных информационных систем и позволяет определить:

- + каковы наиболее вероятные векторы атак, которые может использовать нарушитель для получения доступа к ресурсам корпоративной сети;
- + какие уязвимости наиболее распространены на сетевом периметре;
- + насколько опасны действия злоумышленника, имеющего доступ к ресурсам ЛВС;
- + какие недостатки безопасности позволяют злоумышленнику получить максимальные привилегии в корпоративной инфраструктуре;
- + сохраняют ли свою актуальность атаки с использованием методов социальной инженерии;
- + как с помощью атак на беспроводные сети получить доступ к ресурсам внутренней сети.

В качестве основы для подготовки данного исследования мы использовали статистические данные за 2017 год, полученные по результатам анализа защищенности корпоративных информационных систем, проведенных специалистами Positive Technologies. Сделанные выводы могут не отражать актуальное состояние защищенности информационных систем в других компаниях. Цель исследования — обратить внимание специалистов по ИБ на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

1. РЕЗЮМЕ

Анализ защищенности сетевого периметра:

- + успешно преодолеть сетевой периметр и получить доступ к ресурсам ЛВС было возможно в 68% проектов по анализу защищенности корпоративных информационных систем;
- + подбор словарных учетных записей к ресурсам на сетевом периметре и эксплуатация уязвимостей веб-приложений являются основными векторами атак для проникновения во внутреннюю сеть;
- + по результатам инструментального сканирования ресурсов сетевого периметра было установлено, что 31% компаний был подвержен риску заражения вирусом-шифровальщиком WannaCry.

Анализ защищенности внутренних ресурсов:

- + при тестировании на проникновение от лица внутреннего злоумышленника полный контроль над всей инфраструктурой удалось получить во всех системах;
- + в 60% корпоративных систем, протестированных в период с 14 апреля по 31 декабря 2017 года, обнаружена уязвимость MS17-010, что говорит о несвоевременной установке критически важных обновлений безопасности ОС;
- + недостаточная защита от восстановления учетных записей из памяти ОС — основная уязвимость, которая позволяет получить полный контроль над корпоративной информационной системой.

Оценка осведомленности сотрудников:

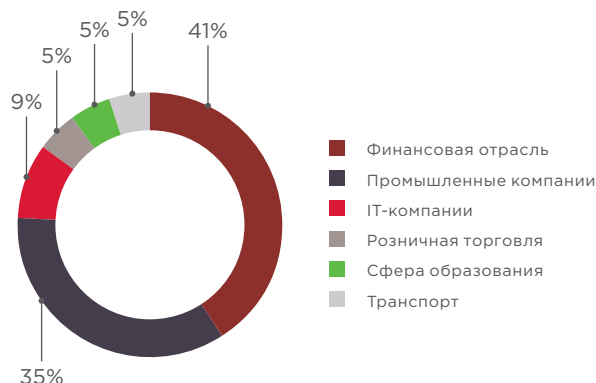
- + 26% сотрудников осуществляют переход по ссылке на фишинговый веб-ресурс, причем практически половина из них в дальнейшем вводят свои учетные данные в поддельную форму аутентификации;
- + каждый шестой сотрудник подвергает корпоративную инфраструктуру риску вирусного заражения.

Анализ защищенности беспроводных сетей:

- + в 75% случаев злоумышленник через атаки на беспроводные сети может получить доступ к ресурсам внутренней сети, а также получить чувствительную информацию (например, доменные учетные записи пользователей).

2. ИСХОДНЫЕ ДАННЫЕ

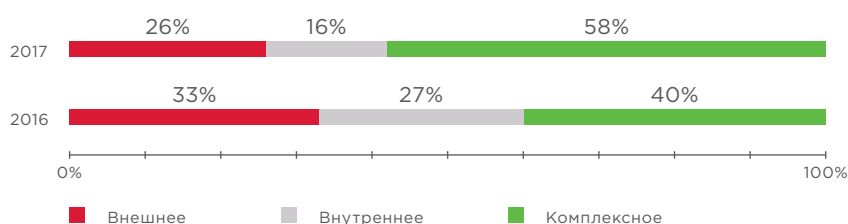
Статистика по итогам 2017 года основывается на результатах анализа защищенности 22 корпоративных систем, принадлежащих как российским, так и зарубежным компаниям из различных сфер экономики. При отборе проектов для исследования учитывалась информативность полученных результатов. Проекты, которые по просьбе заказчиков проводились на ограниченном количестве узлов, не были включены в исследование, так как не отражают реального состояния защищенности корпоративной информационной системы в целом. Как и в 2016 году, основная часть работ по тестированию на проникновение выполнялась для финансовых организаций и промышленных компаний. Успешные атаки на корпоративные системы финансового и промышленного сектора, как правило, приносят злоумышленникам максимальную выгоду. Успешная атака на инфраструктуру банка часто напрямую приводит к хищению денежных средств. Проникновение злоумышленника во внутреннюю сеть промышленной компании может не только привести к утечке чувствительной информации, которую в дальнейшем можно продать компаниям-конкурентам, но и к нарушению технологического процесса.



Распределение исследованных систем по отраслям экономики

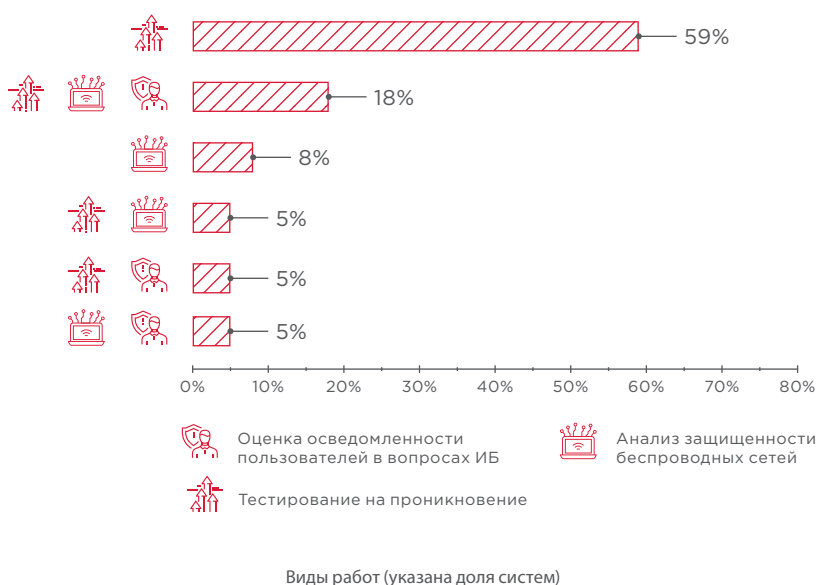
Анализ защищенности корпоративных сетей проводился путем внешнего, внутреннего и комплексного тестирования на проникновение (последнее включает в себя как внешнее, так и внутреннее). Тестирование на проникновение — эффективный метод анализа защищенности, который позволяет выявить уязвимые места в корпоративной инфраструктуре и получить объективную, независимую оценку ее уровня защищенности. В ходе тестирования моделируются действия потенциального нарушителя, осуществляющего атаки как со стороны интернета, так и из сегментов внутренней сети компании. Такой подход позволяет воссоздать условия, в которых обычно действуют нарушители, и оперативно устранить недостатки защиты.

Второй год подряд мы наблюдаем интерес к комплексным услугам. Наши заказчики стремятся не только защитить свой сетевой периметр от атак со стороны внешнего злоумышленника, но и снизить риски, связанные с компрометацией ЛВС внутренним злоумышленником.



Виды тестирования на проникновение (доля систем)

Помимо работ по тестированию на проникновение для многих заказчиков проводились также работы по анализу защищенности беспроводных сетей и оценке осведомленности сотрудников в вопросах информационной безопасности.

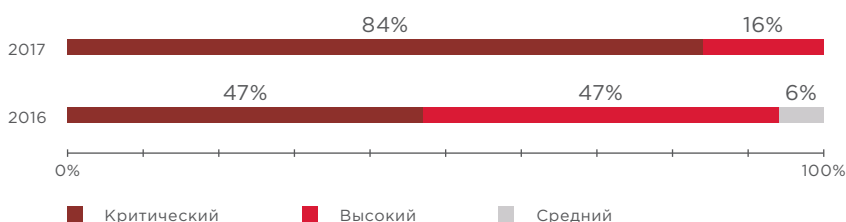


В этом году результаты анализа защищенности сетевого периметра, полученные в ходе внешнего тестирования на проникновение, сравниваются не только с итогами прошлогогоднего исследования, но и со статистикой, полученной в ходе инструментального исследования, которое проводилось в период активного распространения вируса-шифровальщика WannaCry. Во втором квартале 2017 года компания Positive Technologies предлагала бесплатное сканирование внешнего периметра с целью выявления уязвимых сервисов. Заявки оставили 26 компаний из разных сфер экономики. Статистика по внешнему тестированию на проникновение в сравнении с результатами инструментального исследования будет подробно рассмотрена далее в соответствующем разделе.

3. СТАТИСТИКА ЗА 2017 ГОД

3.1. Общие результаты анализа защищенности

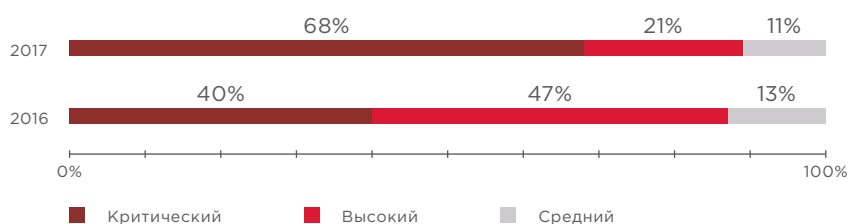
Как правило, при анализе защищенности в каждой системе наши специалисты обнаруживают те или иные уязвимости и недостатки механизмов защиты, которые, среди прочего, позволяют развить вектор атаки вплоть до полной компрометации инфраструктуры компании, получить доступ к чувствительной информации, проводить атаки на отказ в обслуживании и т. п. Все уязвимости мы делим на три категории: связанные с недостатками конфигурации; связанные с отсутствием обновлений безопасности; связанные с ошибками в коде веб-приложений. Для каждой выявленной уязвимости определяется степень ее опасности в соответствии с системой классификации CVSS версии 3.0.



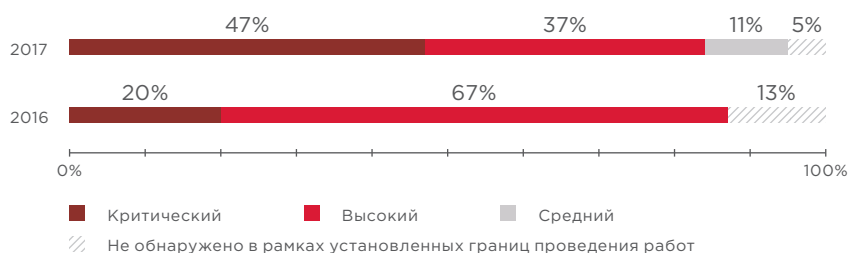
Доля систем по максимальному уровню опасности уязвимостей

18 лет

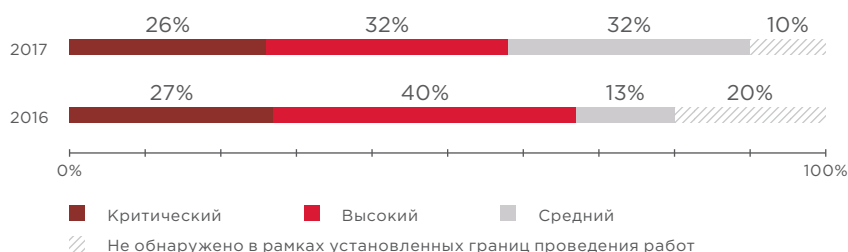
Возраст самой старой уязвимости CVE-1999-0532, обнаруженной при инструментальном анализе ресурсов сетевого периметра



Максимальный уровень риска уязвимостей, связанных с недостатками конфигурации (доля систем)



Максимальный уровень риска уязвимостей, связанных с отсутствием обновлений безопасности (доля систем)



Максимальный уровень риска уязвимостей, связанных с ошибками в коде веб-приложения (доля систем)

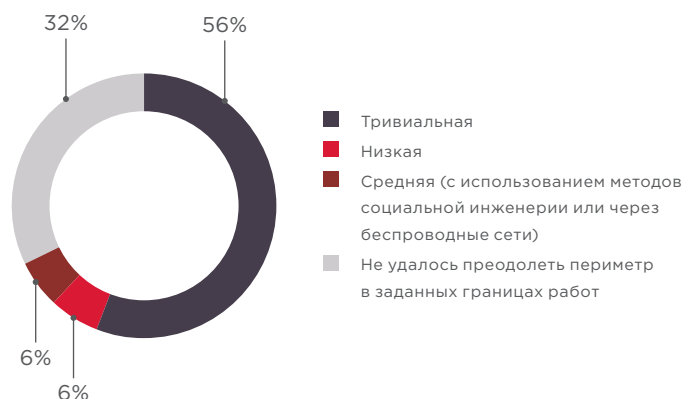
По сравнению с прошлым годом доля корпоративных систем, в которых были обнаружены уязвимости критической степени риска ($CVSS \geq 9,0$) выросла практически в два раза. В основном это связано с публикацией информации о критически опасной уязвимости MS17-010 в SMB-сервисе узлов, функционирующих под управлением Windows. После публикации общедоступных эксплоитов во многих проектах по внутреннему тестированию на проникновение наши специалисты использовали эту уязвимость для получения полного контроля над узлами ЛВС и развития атаки вплоть до получения максимальных привилегий в домене.

Для систем, в которых не были выявлены ошибки в коде веб-приложений и недостатки, связанные с отсутствием обновлений безопасности, стоит учитывать, что тестирование на проникновение проводится методом черного ящика, и в рамках границ проведения работ невозможно выявить все имеющиеся уязвимости. Основная цель тестирования на проникновение — получение объективной оценки защищенности корпоративной системы от атак нарушителей.

3.2. Результаты анализа защищенности сетевого периметра

Результаты внешнего тестирования на проникновение

По итогам 2017 года защищенность сетевого периметра корпоративных информационных систем осталась на уровне 2016 года. Однако при этом наблюдается тенденция к снижению сложности преодоления сетевого периметра. Если в 2016 году только в 27% проектов сложность получения доступа к ресурсам ЛВС оценивалась как тривиальная, то к концу 2017 года этот показатель вырос в два раза, до 56%.



Сложность преодоления сетевого периметра (доля систем)

10

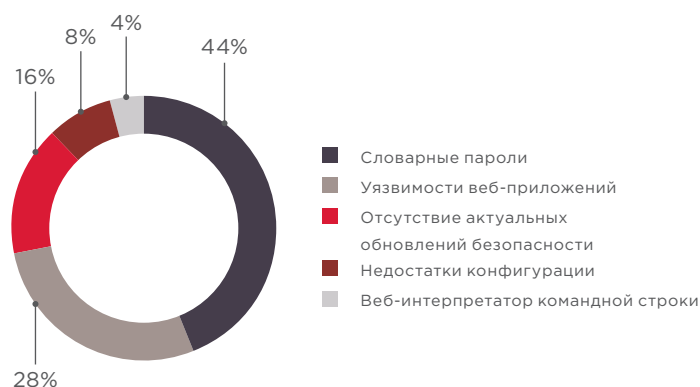
Максимальное число векторов проникновения во внутреннюю сеть, выявленное при тестировании одной корпоративной информационной системы в 2017 году

Такое распределение объясняется тем, что злоумышленнику для получения доступа к ресурсам ЛВС требуется в среднем выполнить два шага: например, подобрать словарные учетные данные для авторизации в веб-приложении и использовать его уязвимости для получения возможности выполнять команды ОС на атакуемом узле.

По результатам анализа защищенности корпоративных информационных систем в среднем в каждой компании выявляются два вектора проникновения во внутреннюю сеть, максимальное число обнаруженных векторов для одной компании — 10.

Можно разделить все успешные векторы проникновения во внутреннюю сеть по категориям:

- + 44% векторов успешной атаки основаны на подборе словарных учетных данных для доступа к веб-приложениям, СУБД и другим сервисам, доступным для подключения на сетевом периметре. Затем злоумышленник может получить возможность выполнять команды ОС на атакуемом узле;
- + 28% векторов атак основаны на эксплуатации уязвимостей веб-приложений. Сразу в ходе нескольких внешних тестирований были выявлены уязвимости, которые позволяют в один шаг, без необходимости авторизации, удаленно выполнять команды ОС с привилегиями веб-приложения;
- + в 16% случаев получить доступ к ресурсам внутренней сети злоумышленник может при эксплуатации уязвимостей в устаревших версиях ПО (например, в CMS-платформах);
- + в остальных случаях для атаки злоумышленник может использовать недостатки конфигурации, связанные с выявлением учетных данных для доступа к системам на сетевом периметре в открытом доступе, например на страницах веб-приложения. Кроме того, были выявлены случаи, когда на веб-ресурсе тестируемой компании наши специалисты находили загруженный ранее веб-интерпретатор командной строки, что свидетельствует об успешных проведенных атаках со стороны внешних злоумышленников.



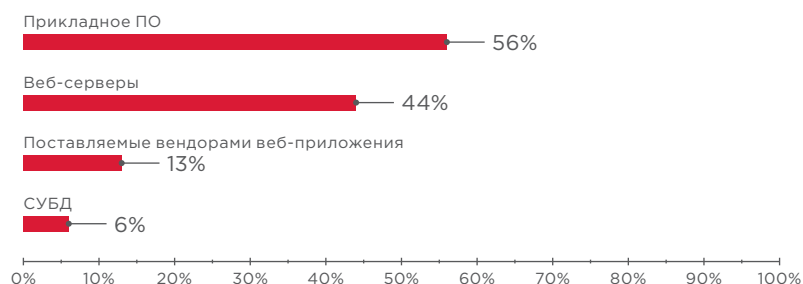
Векторы атак для преодоления сетевого периметра

В первую пятерку наиболее распространенных уязвимостей на сетевом периметре входят те же уязвимости, что и в 2016 году, однако поменялось их процентное соотношение. Можно отметить общую тенденцию к снижению среднего количества уязвимостей, выявляемых при внешнем тестировании на проникновение. Например, в 2016 году во всех протестированных системах были выявлены уязвимости, связанные с использованием словарных учетных данных, в 2017 году этот показатель снизился в два раза. Такие результаты связаны с тем, что для многих компаний ранее проводились работы по анализу защищенности их корпоративных систем. По результатам таких работ заказчики успешно исправляли большую часть выявленных уязвимостей и недостатков конфигурации и начинали более строго контролировать соблюдение внутренних парольных политик. Соответственно, при повторном проведении внешнего тестирования на проникновение через год-полтора было обнаружено меньше уязвимостей, что в итоге положительно сказалось на общих результатах в 2017 году.

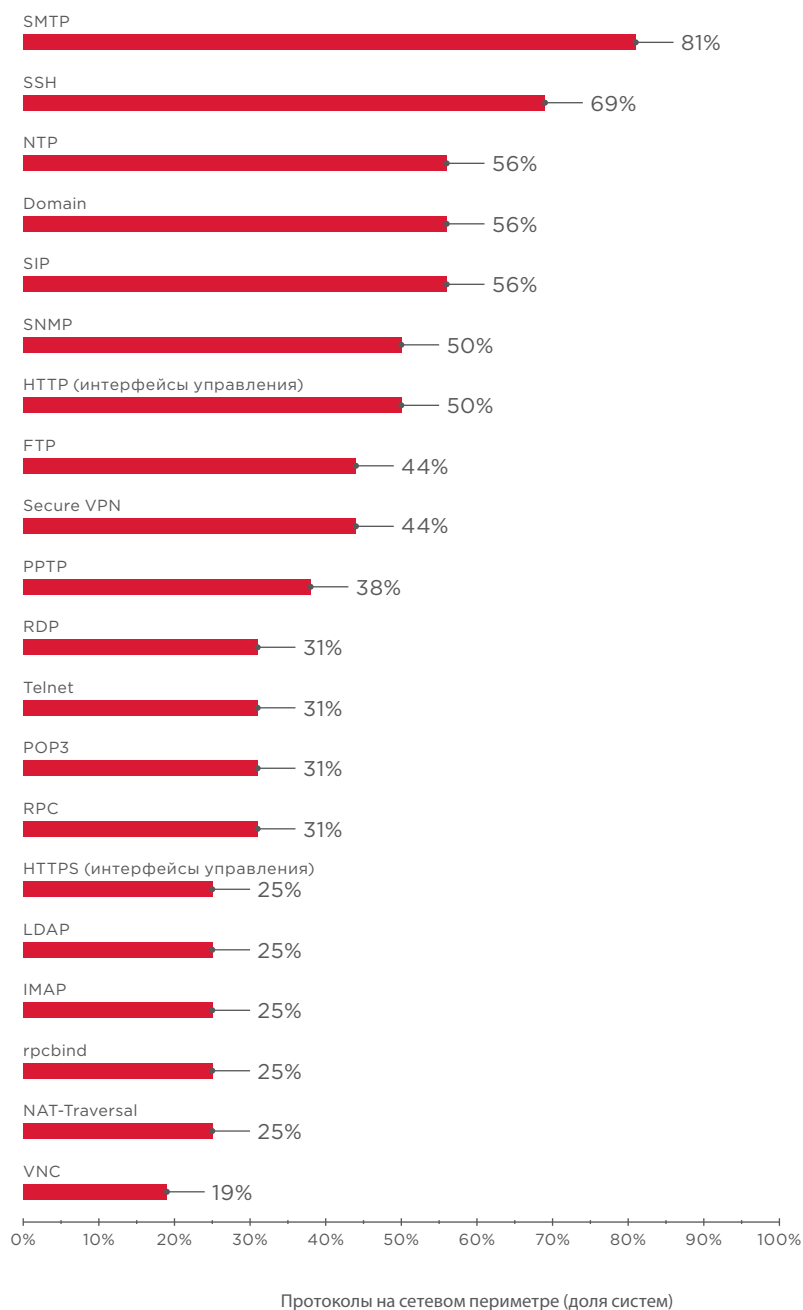


Наиболее распространенные уязвимости на сетевом периметре (доля систем)

Как и в 2016 году, чаще всего на сетевом периметре уязвимости выявляются в прикладном программном обеспечении и в веб-серверах.



Уязвимые версии ПО на сетевом периметре (доля систем)

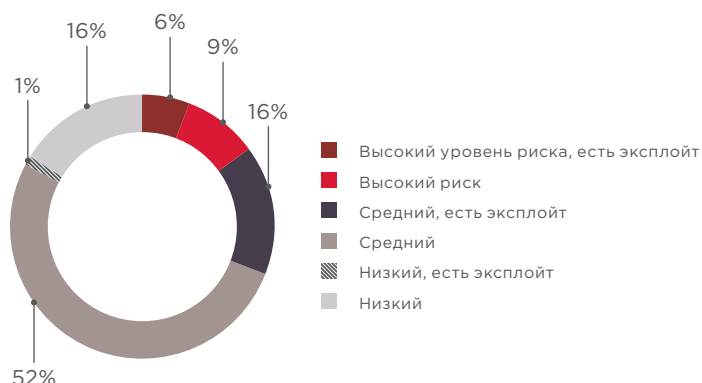


Результаты инструментального анализа защищенности сетевого периметра

Как упоминалось ранее, во втором квартале 2017 года компания Positive Technologies проводила акцию по бесплатному сканированию внешнего периметра ряда компаний с целью выявления уязвимых сервисов. Основной целью было противодействие распространению вируса-шифровальщика WannaCry. Заявки на инструментальное сканирование ресурсов сетевого периметра оставили 26 компаний из разных сфер экономики: IT- и телеком-компании, крупные представители розничной торговли, компании из финансового сектора и нефтегазовой промышленности.

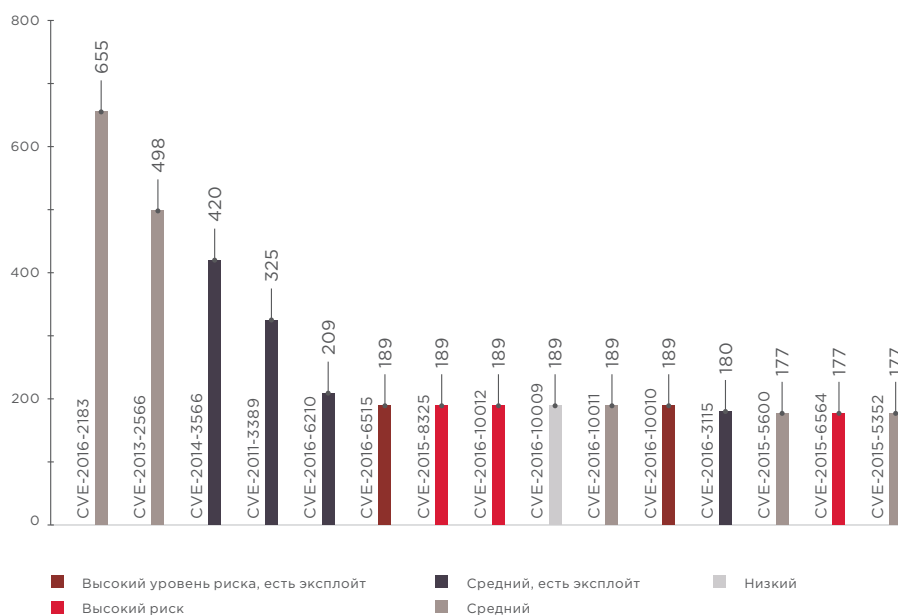
Все компании вначале должны были определить границы своих корпоративных систем. Уже на данном этапе у некоторых участников возникли затруднения: 23% не смогли определить границы своего сетевого периметра или определили их некорректно. Неспособность определить границы сетевого периметра уже является свидетельством низкой защищенности корпоративной информационной системы от атак со стороны внешнего нарушителя — еще до получения результатов ручного или инструментального анализа корпоративной системы.

Сканирование сетевых периметров проводилось с помощью автоматизированной системы анализа защищенности и контроля соответствия стандартам MaxPatrol и дополнительного ПО. По результатам сканирования было обнаружено множество уязвимостей: 15% из них имеют высокий уровень риска по шкале CVSS версии 2.0, причем для эксплуатации части уязвимостей существуют общедоступные эксплойты.



Распределение уязвимостей по уровню риска

Отдельно можно рассмотреть статистику по самым популярным уязвимостям, выявленным при инструментальном сканировании сетевого периметра. Среди этих уязвимостей наибольшую опасность представляет [CVE-2016-6515](#) в сервисе OpenSSH. При вводе пароля для аутентификации в приложении отсутствует ограничение на количество вводимых символов. Данный недостаток позволяет удаленному злоумышленнику проводить атаки, направленные на отказ в обслуживании сервиса. Также для эксплуатации данной уязвимости существует общедоступный эксплойт¹. Кроме того, если злоумышленник сможет подобрать учетные данные для подключения по SSH и получить пользовательские привилегии в UNIX-системе, то наличие уязвимости [CVE-2016-10010](#) в OpenSSH позволит ему с помощью другого эксплойта² локально повысить свои привилегии до максимальных на скомпрометированном узле, а затем развивать атаку на ресурсы ЛВС.

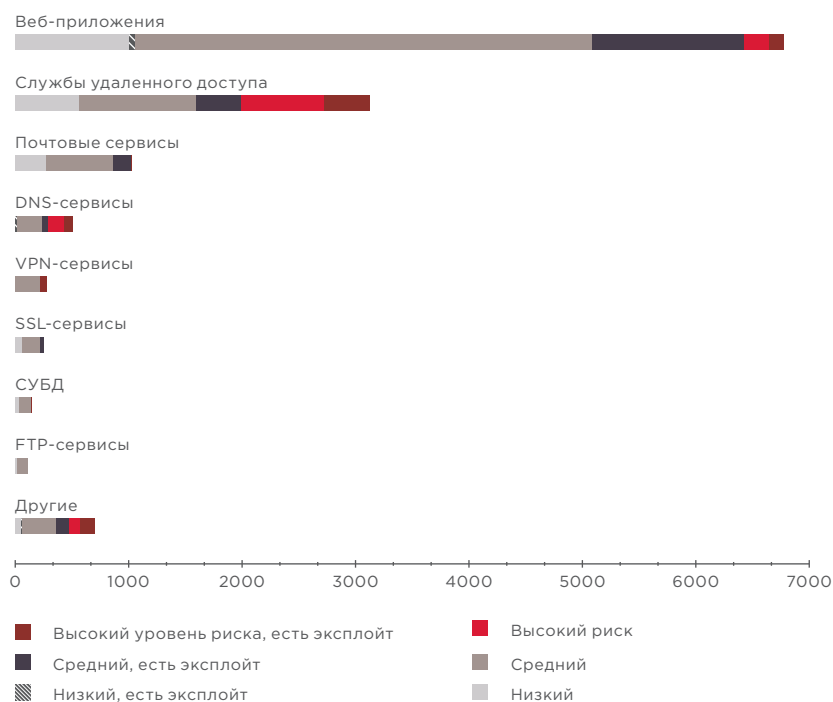


Самые распространенные уязвимости на сетевом периметре (инструментальный анализ)

¹ exploit-db.com/exploits/40888/

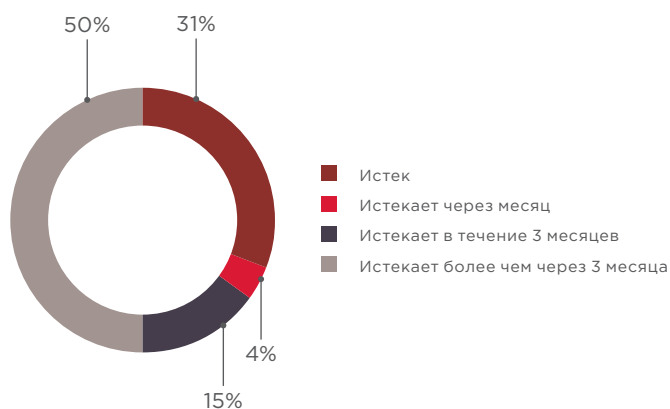
² exploit-db.com/exploits/40962/

При анализе доступных служб на периметре наибольшее количество уязвимостей выявлено в веб-приложениях и службах удаленного доступа (SSH). Данные результаты инструментального анализа совпадают со статистикой, полученной в ходе внешнего тестирования на проникновение, где уязвимости и недостатки конфигурации веб-приложений в большинстве случаев являлись отправной точкой для получения доступа к ресурсам ЛВС.

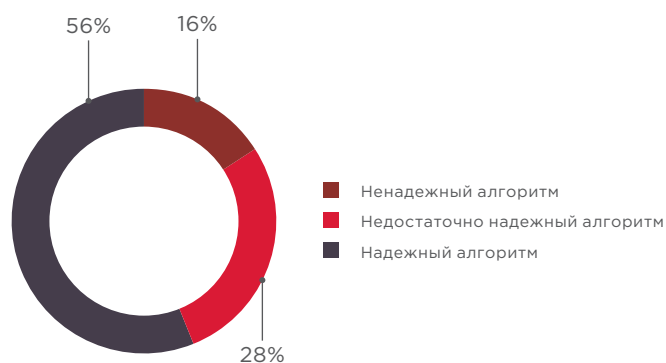


Количество уязвимостей в зависимости от используемых сервисов

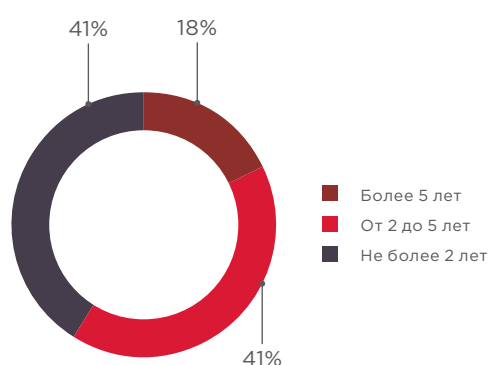
При инструментальном анализе доступных веб-приложений отдельно собиралась статистика по состоянию SSL-сертификатов. Более чем у четверти сертификатов на момент сканирования закончился срок действия, в 15% использовались ненадежные криптографические алгоритмы (например, SHA-1), и каждый шестой сертификат был выдан на срок более 5 лет.



Сроки действия SSL-сертификатов



Алгоритмы шифрования в SSL-сертификатах



Сроки использования SSL-сертификатов

Использование просроченных SSL-сертификатов несет репутационные риски для компаний, так как пользователь после получения предупреждения в окне браузера об использовании в приложении невалидного сертификата может отказаться от посещения веб-ресурса.

Использование ненадежных алгоритмов шифрования сводит к нулю весь смысл применения SSL-сертификатов, поскольку злоумышленник может перехватить сетевой трафик и затем успешно расшифровать полученные данные. Кроме того, нарушитель может подменить SSL-сертификат и создать свой собственный фишинговый сайт, с помощью которого заражать пользователей вредоносным ПО и похищать их учетные данные. При этом пользователи могут думать, что заражение их компьютеров произошло после посещения легитимного сайта компании.

В случае если SSL-сертификат выдается на срок более 5 лет, возникают риски, связанные с возможностью подбора ключа шифрования.

Вернемся к основной цели инструментального сканирования ресурсов сетевого периметра. В 8 компаниях из 26 были обнаружены внешние узлы с открытым портом 445/TCP с запущенным SMB-сервисом. Таким образом, инфраструктура практически каждой третьей компании была подвержена риску заражения вирусом-шифровальщиком WannaCry.

3.3. Результаты анализа внутренних ресурсов

В случае успешной атаки на ресурсы сетевого периметра внешний злоумышленник может получить доступ к внутренней сети и дальше развивать атаку вплоть до полного контроля над всей IT-инфраструктурой компании.

Как и в 2016 году, при тестировании на проникновение от лица внутреннего злоумышленника (например, рядового сотрудника компании, имеющего доступ к пользовательскому сегменту сети) полный контроль над всей инфраструктурой удалось получить во всех протестированных системах. Только в 7% проектов сложность получения доступа к критически важным ресурсам со стороны внутреннего злоумышленника оценивалась как «средняя». Во всех остальных случаях скомпрометировать всю корпоративную систему мог нарушитель низкой квалификации.

Типовой вектор атаки во внутренней сети строился на получении максимальных привилегий на одном из узлов ЛВС с последующим запуском специализированного ПО для извлечения учетных данных других пользователей, которые ранее подключались к данному узлу. Повторяя эти шаги на разных узлах, злоумышленник в конечном итоге может найти узел сети, на котором хранится учетная запись администратора домена и получить его пароль в открытом виде.

В 2017 году задача по получению максимальных привилегий на узле внутренней сети для злоумышленника значительно упростилась после публикации информации об уязвимости MS17-010. 14 марта 2017 года компания Microsoft опубликовала обновление, которое устраняет данную уязвимость, а ровно через месяц 14 апреля хакерская группировка Shadow Brokers опубликовала эксплойт EternalBlue³ для ее эксплуатации. Наши специалисты в период с середины апреля до конца года успешно использовали эксплойт в 60% работ по внутреннему тестированию на проникновение, что говорит о несвоевременной установке критически важных обновлений безопасности ОС в большинстве корпоративных систем.

Ближе к концу 2017 года стали чаще встречаться корпоративные системы, в которых установлены обновления, устраняющие критически опасную уязвимость MS17-010. Но в нескольких проектах на узлах с Windows для локального повышения привилегий удалось использовать другую критически опасную уязвимость, описанную в бюллетене безопасности MS17-018. Для данной уязвимости также есть эксплойт, который отсутствует в публичном доступе.

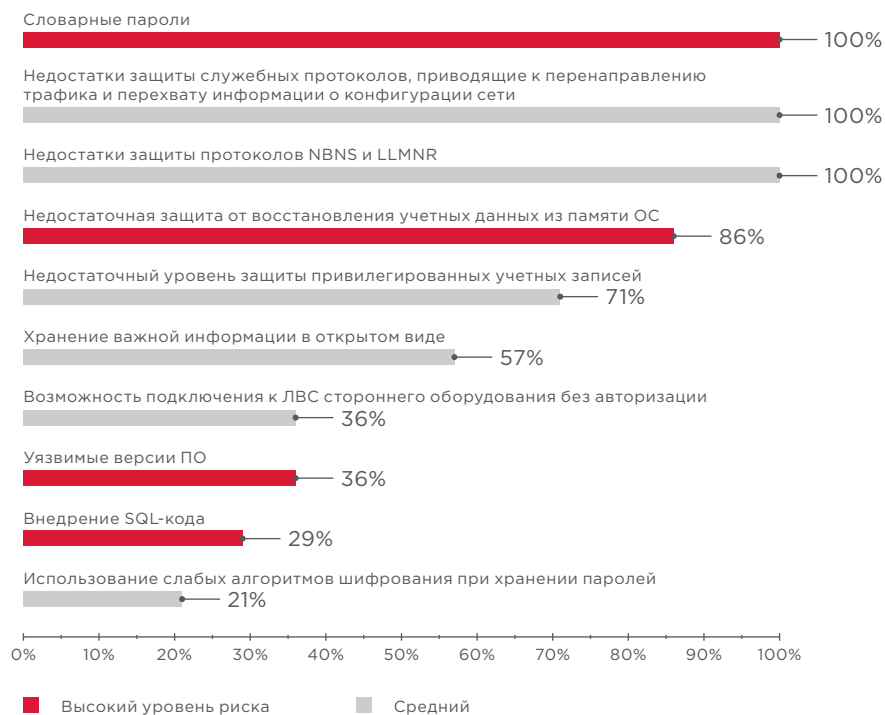
Статистика самых распространенных уязвимостей во внутренней сети по сравнению с 2016 годом практически не изменилась. Исключение составляет новая категория «Недостаточная защита от восстановления учетных записей из памяти ОС». На узлах ЛВС под управлением Windows возможно получение паролей в открытом виде (или их хеш-сумм) из памяти системы с помощью специального ПО — если нарушитель обладает привилегиями локального администратора. Ранее данную уязвимость мы относили к недостаткам антивирусного ПО, которое должно блокировать запуск любых вредоносных утилит для извлечения учетных данных. Однако за последнее время вышли модификации таких утилит, написанные на языке PowerShell, которые предназначены специально для обхода блокировки запуска со стороны любого антивирусного ПО. Теперь для обеспечения защиты от извлечения учетных данных из памяти ОС необходимо использовать комплексный подход, включающий запрет на сохранение кэшированных данных, ускорение очистки памяти процесса lsass.exe от учетных записей пользователей, завершивших сеанс, и отключение механизма wdigest. Кроме того, можно использовать современные версии Windows 10, в которых реализована система Remote Credential Guard, позволяющая изолировать и защитить системный процесс lsass.exe от несанкционированного доступа. Таким образом, в 2017 году для объективной оценки состояния механизмов защиты корпоративной сети мы ввели отдельную метрику для сбора статистики по запуску утилит, предназначенных для извлечения учетных данных.

В 14% корпоративных систем, где не была найдена уязвимость «Недостаточная защита от восстановления учетных записей из памяти ОС», использовались другие векторы атак для получения полного контроля над корпоративной инфраструктурой.

В 60%

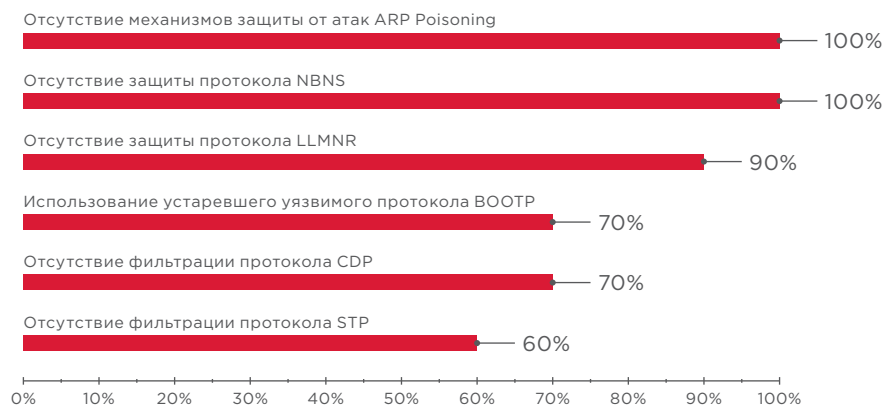
корпоративных систем, протестированных в период с 14 апреля по 31 декабря 2017 года, обнаружена уязвимость MS17-010

³ vulners.com/seebug/SSV:92952

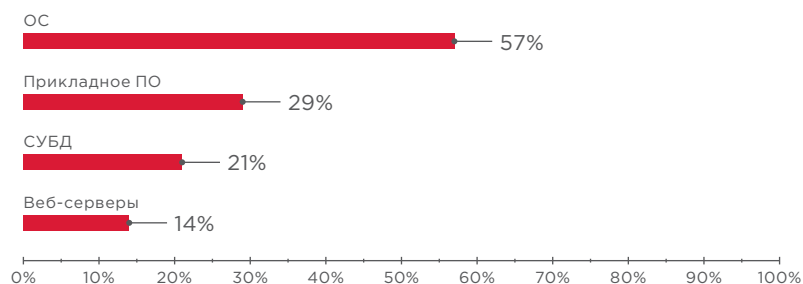


Наиболее распространенные уязвимости внутренней сети (доля систем)

Статистика по недостаткам защиты служебных протоколов была построена на основе тех проектов, где проводился анализ сетевого трафика ЛВС (71% компаний). В некоторых проектах заказчики были против таких проверок, так как они могут привести к нарушению непрерывной работы сети.



Недостатки защиты служебных протоколов (доля систем)



Уязвимые версии ПО во внутренней сети (доля систем)

По результатам внутренних тестирований установлено, что основные проблемы корпоративных информационных систем — несвоевременная установка критически важных обновлений безопасности и недостаточная защита от восстановления учетных записей из памяти ОС с помощью специализированных утилит.

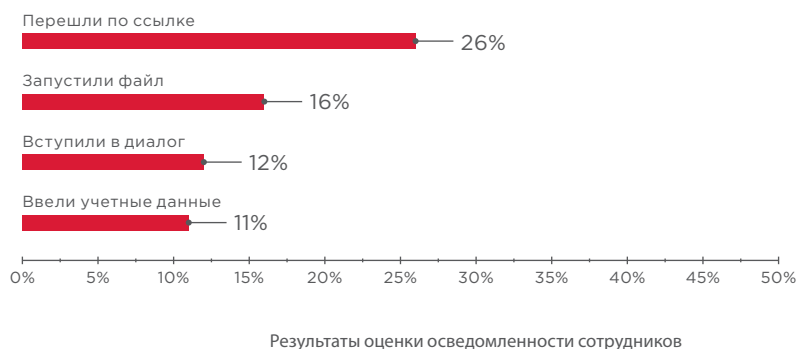
4. РЕЗУЛЬТАТЫ ОЦЕНКИ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В дополнение к работам по тестированию на проникновение корпоративных информационных систем для ряда компаний проводилась оценка осведомленности сотрудников в вопросах информационной безопасности. Такие работы проводятся по заранее согласованным с заказчиком сценариям, в которых имитируются реальные атаки злоумышленников с использованием методов социальной инженерии и отслеживается реакция сотрудников на эти атаки.

Тестирование сотрудников проводилось двумя методами — при помощи рассылки электронных писем и в телефонном взаимодействии. Для получения объективной оценки уровня осведомленности сотрудников анализировались следующие контролируемые события:

- + переход по ссылке на веб-ресурс злоумышленника;
- + ввод учетных данных в заведомо ложную форму аутентификации;
- + запуск приложенного к письму файла;
- + факт взаимодействия со злоумышленником по телефону или электронной почте.

По результатам работ установлено, что 26% сотрудников осуществляют переход по ссылке на фишинговый веб-ресурс, причем практически половина из них в дальнейшем вводят свои учетные данные в поддельную форму аутентификации. Каждый шестой сотрудник подвергает корпоративную инфраструктуру риску вирусного заражения путем запуска приложенного к письму файла. Кроме того, 12% сотрудников готовы вступить в диалог с нарушителем и раскрыть информацию, которая в дальнейшем может быть использована при проведении атак на корпоративную информационную систему.



Всего при оценке осведомленности сотрудников в 2017 году было отправлено более 1300 писем, половина из которых содержала ссылку на фишинговый ресурс, а вторая — файл со специальным скриптом, который отправлял нашим специалистам информацию о времени открытия файла, а также адрес электронной почты сотрудника. Настоящий злоумышленник в содержимое файла может добавить набор эксплойтов, направленных на эксплуатацию различных уязвимостей, в том числе [CVE-2013-3906](#), [CVE-2014-1761](#) и [CVE-2017-0199](#). Подобная атака может привести к получению злоумышленником контроля над рабочей станцией соответствующего пользователя, распространению вредоносного кода, отказу в обслуживании и иным негативным последствиям.

Типовой пример атаки с использованием методов социальной инженерии:

- 1) злоумышленник размещает на подконтрольном ресурсе набор эксплойтов под различные версии ПО;
- 2) ссылка на этот ресурс массово рассылается в фишинговых письмах;
- 3) сотрудник организации переходит по ссылке из письма, и после открытия страницы в браузере происходит эксплуатация уязвимостей.

Подобная атака может привести к заражению рабочей станции пользователя вредоносным ПО. Кроме того, при использовании устаревшей версии браузера может быть реализовано удаленное выполнение кода (например, CVE-2016-0189). Таким образом, злоумышленник может получить доступ к узлу внутренней сети и развивать атаку вплоть до максимальных привилегий в корпоративной инфраструктуре. Более подробно со сценариями атак с применением методов социальной инженерии можно ознакомиться в нашем исследовании «Как социальная инженерия открывает хакеру двери в вашу организацию»⁴.

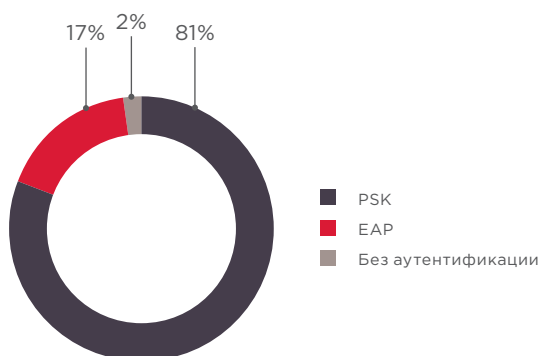
5. РЕЗУЛЬТАТЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ БЕСПРОВОДНЫХ СЕТЕЙ

40%

компаний используют
словарный ключ для
беспроводной сети

Атаки на беспроводные сети для внешнего нарушителя являются альтернативным способом получения доступа к ресурсам внутренней сети. В случае неудачи при попытке преодолеть сетевой периметр, например, через атаки на веб-приложения — злоумышленник может воспользоваться уязвимостями беспроводных сетей компании. Для успешной атаки ему потребуется заранее приобрести недорогое оборудование и попасть в зону покрытия беспроводной сети. Причем злоумышленнику для проведения атак не обязательно заходить в пределы контролируемой зоны компании: по результатам наших работ установлено, что 75% беспроводных сетей доступны за ее пределами. То есть атаки на беспроводные сети можно проводить незаметно с близлежащей территории, например с парковки рядом с офисным зданием.

В 2017 году практически во всех протестированных беспроводных сетях использовался протокол WPA2 с различными методами аутентификации, самым распространенным из которых был PSK (pre-shared key).



Методы аутентификации в беспроводных сетях

В зависимости от используемого метода аутентификации для атак на беспроводные сети можно использовать различные сценарии. В 2017 году для получения доступа к ресурсам внутренней сети чаще всего использовались следующие два сценария:

- + перехват handshake между точкой доступа и легитимным клиентом (подходит только для метода PSK);
- + атаки на клиентов беспроводной сети с использованием поддельной точки доступа (подходит для всех методов аутентификации).

В первом сценарии проводится подбор пароля к перехваченному значению handshake. Успех зависит от сложности используемого пароля. При этом важно учитывать, что подбирать его злоумышленник может уже вне зоны действия исследуемой точки доступа. Если в рамках границ проведения работ нашим специалистам не всегда удается успеть подобрать по значению handshake пароль, то у злоумышленника больше времени, что в разы увеличивает его шансы.

⁴ ptsecurity.com/upload/corporate/ru-ru/analytics/Social-engineering-rus.pdf

После подбора пароля и подключения к точке доступа установлено, что в 75% беспроводных сетей отсутствует изоляция между пользователями. Таким образом, злоумышленник может атаковать устройства пользователей, например эксплуатировать уязвимость MS17-010 на их личных и корпоративных ноутбуках.



Перехват handshake между точкой доступа и легитимным клиентом

В случае если подобрать пароль к точке доступа так и не удалось, можно использовать второй сценарий с установкой поддельной точки доступа.

Во-первых, злоумышленник вместе с поддельной точкой доступа может использовать фишинговую страницу аутентификации с целью получения учетных данных и перехвата чувствительной информации, передаваемой по открытым протоколам передачи данных (например, HTTP, FTP).

В 2017 году в рамках одного из проектов по анализу защищенности беспроводной сети, проводимых в Москве, специалисты Positive Technologies использовали поддельную точку доступа с ESSID (Extended Service Set Identification) MT_FREE, которая популярна у горожан, так как используется для доступа в сеть Wi-Fi, развернутую на городском транспорте. Далее была подготовлена поддельная форма аутентификации, в которой использовались логотип и корпоративное оформление тестируемой компании. После подключения к поддельной точке доступа при попытке открыть любой веб-сайт все пользователи переадресовывались на страницу с поддельной формой аутентификации в корпоративной сети. В результате данной атаки удалось получить доменные учетные данные сотрудников компании и использовать их для дальнейшего развития атаки.



Атака с использованием поддельной точки доступа



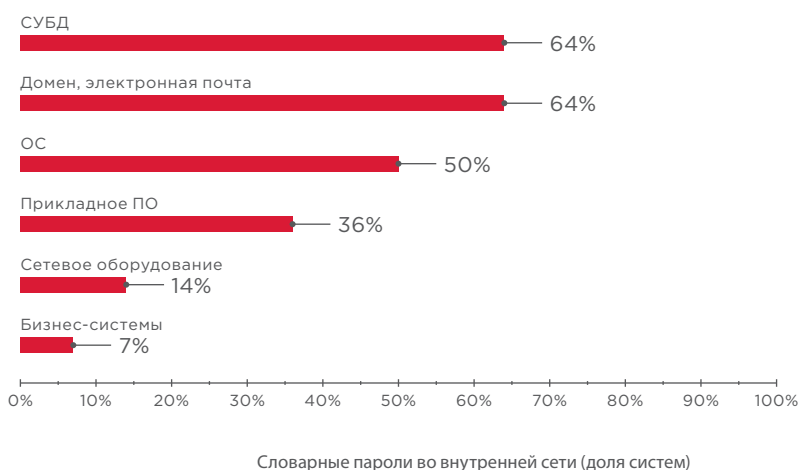
Только в 1 из 8 протестированных компаний сотрудники не стали вводить свои учетные данные в поддельную форму аутентификации

Во-вторых, злоумышленник с помощью поддельной точки доступа может перехватывать сохраненные на устройстве учетные данные пользователя. Для этого необходимо создать точку доступа с тем же ESSID и такими же параметрами, как и легитимная точка доступа. Если на устройстве пользователя настроено автоматическое подключение к сохраненной беспроводной сети, то оно осуществит попытку подключения к поддельной точке доступа автоматически, если у нее будет более мощный сигнал в месте расположения этого устройства. В результате таких атак злоумышленник может получить хеш-суммы паролей сотрудников компании и использовать их для дальнейшего развития атаки на корпоративную инфраструктуру.

Установлено, что в 75% случаев злоумышленник посредством атак на беспроводные сети может получить доступ к ресурсам внутренней сети, а также чувствительную информацию (например, доменные учетные записи пользователей). Данный способ проникновения во внутреннюю сеть является эффективной альтернативой классическим атакам на узлы сетевого периметра.

6. ИНТЕРЕСНЫЕ ФАКТЫ О СЛОВАРНЫХ ПАРОЛЯХ

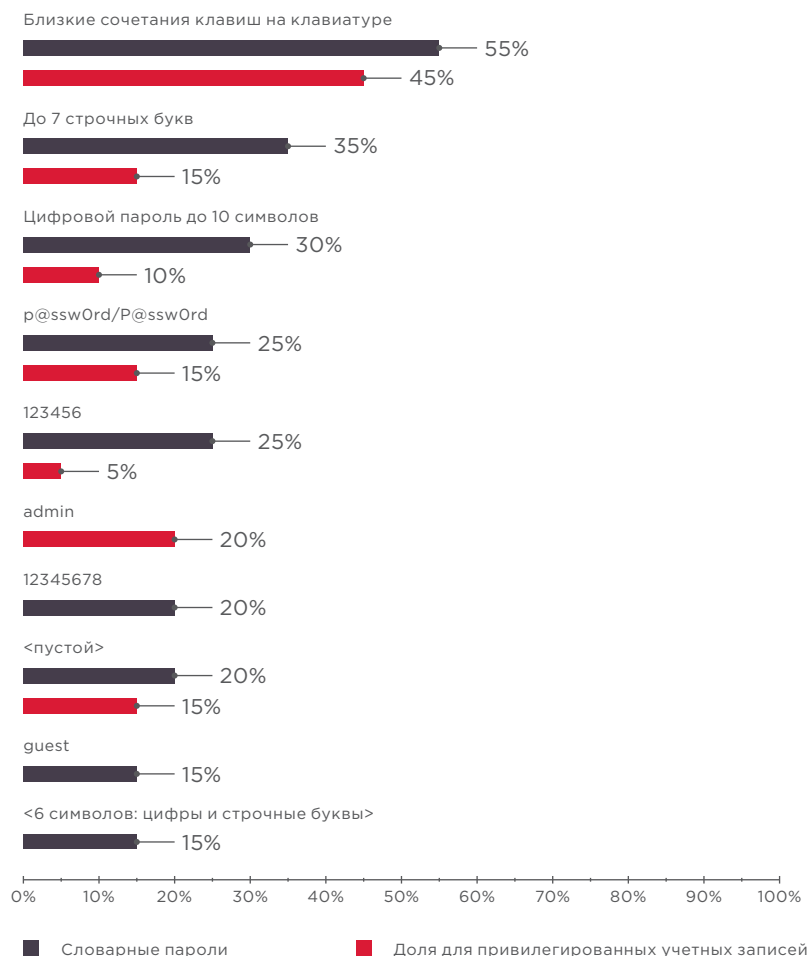
Каждый год по результатам тестов на проникновение мы определяем сервисы, для доступа к которым чаще всего использовались словарные пароли. Эта статистика предназначена в первую очередь для системных администраторов, чтобы напомнить им о необходимости использовать сложные пароли и своевременно заменять стандартные учетные записи после установки и ввода в эксплуатацию нового сервиса.



По итогам 2017 года установлено, что простые пользователи и администраторы в качестве своих паролей часто используют сочетания близких клавиш на клавиатуре, полагая, что длинный, ничего не значащий пароль (например, zaq12wsxcde3 или роiuytrewq) сможет защитить их от несанкционированного доступа. Однако это ошибочное мнение: несмотря на кажущуюся сложность пароля, все такие сочетания клавиш уже давно внесены в специальные словари, и атака методом подбора занимает у злоумышленника считанные минуты.

Qwerty, Zaq1xsw2

и другие сочетания близких клавиш на клавиатуре — самые популярные пароли, в том числе и среди привилегированных пользователей



Самые распространенные словарные пароли (доля систем)

ЗАКЛЮЧЕНИЕ

Корпоративные информационные системы по-прежнему уязвимы к атакам со стороны внешних и внутренних злоумышленников. Если при проведении внешнего тестирования на проникновение все чаще встречаются компании, которые обеспокоены вопросом защищенности своего сетевого периметра, то при тестировании защищенности корпоративной системы от лица внутреннего злоумышленника ситуация значительно хуже. В 2017 году от лица внешнего злоумышленника, использующего, в числе прочего, методы социальной инженерии и атаки на беспроводные сети, преодолеть сетевой периметр удалось в 68% работ. При этом от лица внутреннего нарушителя полный контроль над ресурсами ЛВС был получен во всех без исключения проектах — несмотря на используемые в компаниях технические средства и организационные меры для защиты информации.

Наши базовые рекомендации по обеспечению приемлемого уровня защищенности корпоративных информационных систем из года в год остаются неизменными:

- + Отказаться от использования простых и словарных паролей, разработать строгие правила для корпоративной парольной политики и контролировать их выполнение.
- + Обеспечить дополнительную защиту привилегированных учетных записей (например, администраторов домена). Хорошей практикой является использование двухфакторной аутентификации.
- + Обеспечить защиту инфраструктуры от атак, направленных на восстановление учетных записей из памяти ОС. Для этого на всех рабочих станциях привилегированных пользователей, а также на всех узлах, к которым осуществляется

подключение с использованием привилегированных учетных записей, установить Windows версии выше 8.1 и включить привилегированных пользователей домена в группу Protected Users. Кроме того, можно использовать современные версии Windows 10, в которых реализована система Remote Credential Guard, позволяющая изолировать и защитить системный процесс lsass.exe от несанкционированного доступа.

- + Убедиться, что в открытом виде (например, на страницах веб-приложения) не хранится чувствительная информация, представляющая интерес для злоумышленника. К такой информации могут относиться учетные данные для доступа к различным ресурсам, адресная книга компании, содержащая электронные адреса и доменные идентификаторы сотрудников, и т. п.
- + Ограничить количество сервисов на сетевом периметре, убедиться в том, что открытые для подключения интерфейсы действительно должны быть доступны всем интернет-пользователям.
- + Своевременно устанавливать обновления безопасности для ОС и последние версии прикладного ПО.
- + Провести анализ защищенности беспроводных сетей. Особое внимание стоит обратить на надежность используемых методов аутентификации, а также настроить изоляцию пользователей точки доступа.
- + На регулярной основе проводить обучение сотрудников, направленное на повышение их компетенции в вопросах информационной безопасности, с контролем результатов.
- + Для своевременного обнаружения атак использовать SIEM-систему. Только своевременное выявление попытки атаки позволит ее предотвратить до того, как злоумышленник нанесет существенный ущерб компании.
- + Для защиты веб-приложений — установить межсетевой экран уровня веб-приложения (web application firewall).
- + Регулярно проводить тестирование на проникновение, чтобы своевременно выявлять векторы атак на корпоративную систему и на практике оценивать эффективность принятых мер защиты.

Данный перечень не является исчерпывающим, но несоблюдение даже одного пункта может привести к полной компрометации корпоративной системы, и все затраты на различные дорогостоящие средства и системы защиты окажутся неоправданными. Комплексный подход к информационной безопасности — лучшая защита корпоративной информационной системы от любого нарушителя.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.