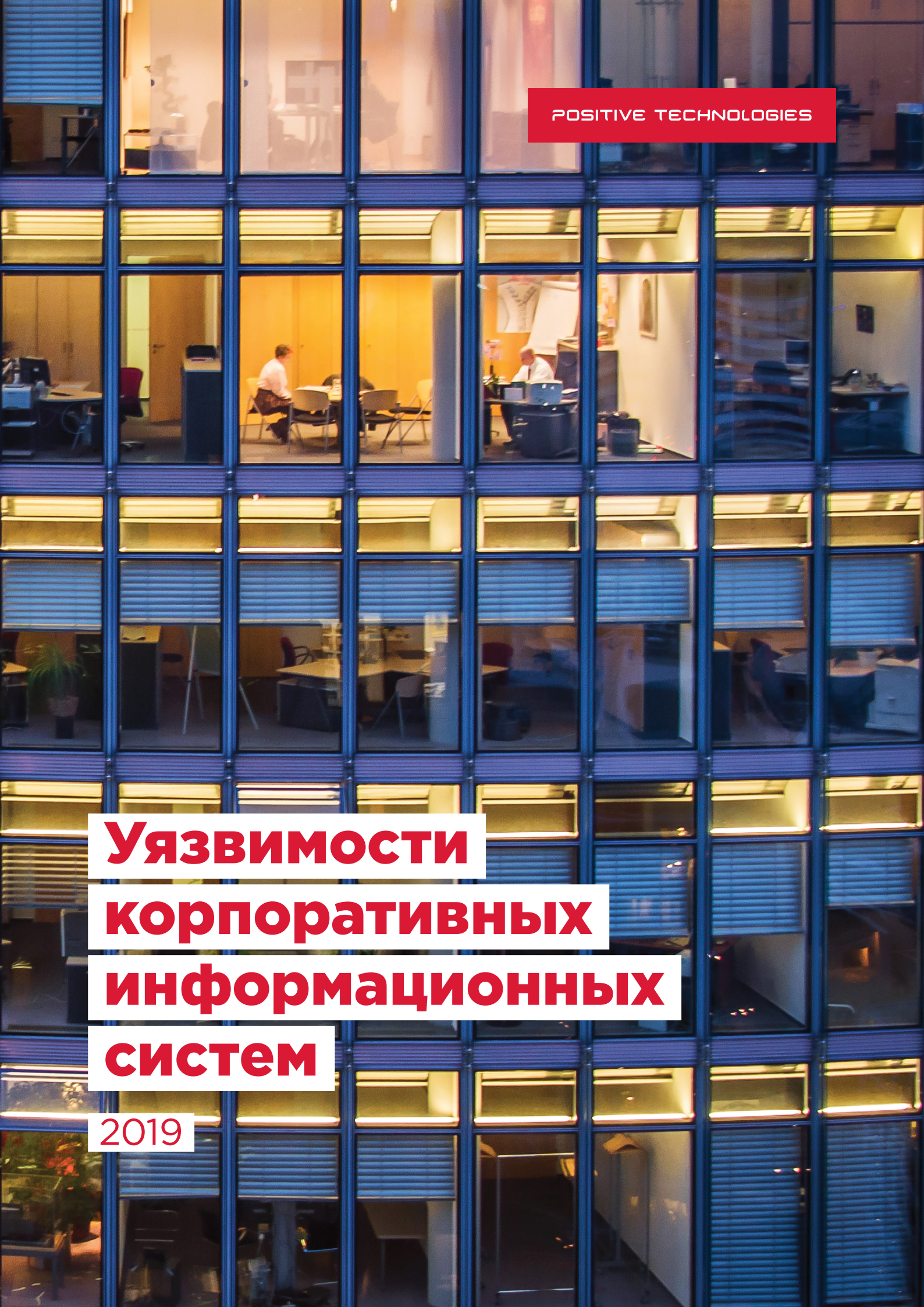

POSITIVE TECHNOLOGIES

Уязвимости корпоративных информационных систем

2019

Содержание

Введение

Корпоративная информационная система представляет собой сложную структуру, в которой объединены различные сервисы, необходимые для функционирования компании. Эта структура постоянно меняется — появляются новые элементы, изменяется конфигурация существующих. По мере роста системы обеспечение информационной безопасности и защита критически важных для бизнеса ресурсов становятся все более сложной задачей.

Для того чтобы выявить недостатки защиты различных компонентов и определить потенциальные векторы атак на информационные ресурсы, проводится анализ защищенности. Эффективный способ анализа — тестирование на проникновение, в ходе которого моделируется реальная атака злоумышленников. Такой подход позволяет объективно оценить уровень защищенности корпоративной инфраструктуры и понять, могут ли противостоять атакам применяемые в компании средства защиты.

В данном отчете представлены результаты проектов по анализу защищенности корпоративных информационных систем, выполненных в 2018 году специалистами Positive Technologies. Документ содержит обзор наиболее распространенных недостатков безопасности, практические примеры их эксплуатации и описание вероятных векторов атак, а также рекомендации по повышению уровня защищенности.

Сделанные выводы могут не отражать актуальное состояние защищенности информационных систем в других компаниях. Данное исследование проведено с целью обратить внимание специалистов по ИБ на наиболее актуальные проблемы и помочь им своевременно выявить и устранить уязвимости.

Резюме

Анализ защищенности сетевого периметра

- Преодолеть сетевой периметр и получить доступ к ресурсам ЛВС было возможно в 92% проектов по внешнему тестированию на проникновение.
- В половине компаний злоумышленник может преодолеть сетевой периметр за один шаг.
- Уязвимости в коде веб-приложений — главная проблема на сетевом периметре. Три четверти векторов проникновения связаны с недостатками защиты веб-ресурсов.

Анализ защищенности внутренних ресурсов

- Полный контроль над инфраструктурой удалось получить *во всех проектах* по внутреннему тестированию на проникновение.
- Использование словарных паролей и недостаточная защита от восстановления учетных данных из памяти ОС — основные недостатки во внутренней сети.
- Перехват учетных данных успешно эксплуатируется при внутреннем тестировании на проникновение. Ни одна из компаний, где проводился анализ сетевого трафика, не обеспечивает защиту от перехвата чувствительной информации.

Оценка осведомленности сотрудников

- Каждый третий сотрудник рискует запустить вредоносный код на своем рабочем компьютере.
- Каждый седьмой сотрудник может вступить в диалог со злоумышленником и выдать конфиденциальную информацию.
- Каждый десятый сотрудник вводит учетные данные в поддельную форму аутентификации.

Анализ защищенности беспроводных сетей

- Злоумышленник может подключиться к корпоративным беспроводным сетям *во всех протестированных компаниях*.
- В 63% систем из-за недостатков защиты беспроводных сетей был получен доступ к ресурсам ЛВС.

Исходные данные

Для подведения статистики за 2018 год были выбраны 33 работы по анализу защищенности корпоративных информационных систем из числа тех компаний, которые разрешили использовать обезличенные данные. Чтобы получить объективные результаты, мы отбирали наиболее информативные проекты. Так, в исследовании не учитываются работы, которые проводились на ограниченном числе узлов, поскольку они не отражают подлинного состояния защищенности системы. В итоговую выборку вошли российские и зарубежные компании из различных отраслей экономики, при этом большую часть составили промышленные, финансовые и транспортные компании.

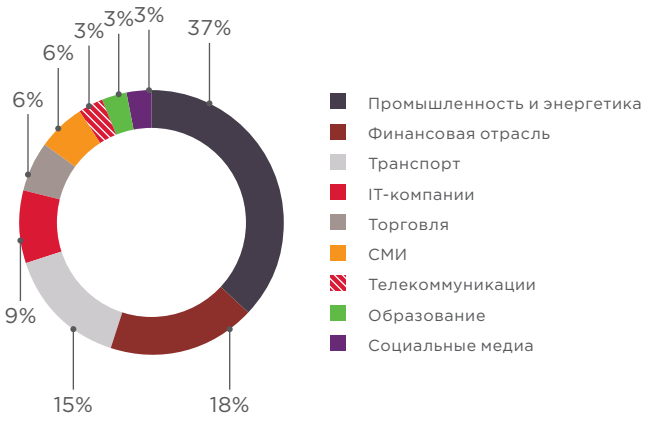

Рисунок 1. Распределение исследованных систем по отраслям экономики

Анализ защищенности информационной системы проводится путем внешнего и внутреннего тестирования на проникновение. Во время работ воссоздаются условия, максимально приближенные к условиям реальной атаки: это позволяет сформировать корректную оценку уровня защищенности. В ходе внешнего тестирования моделируются действия потенциального злоумышленника, который не обладает привилегиями в рассматриваемой системе и действует из интернета. В этом случае перед экспертами ставится задача преодолеть сетевой периметр и получить доступ к ресурсам локальной сети. Внутреннее тестирование подразумевает, что нарушитель действует из сегмента локальной сети, а его целью является контроль над инфраструктурой или над отдельными критически важными ресурсами, которые определяет заказчик. В четверти компаний проводились оба вида работ — так называемое комплексное тестирование на проникновение.

Для некоторых заказчиков выполнялись анализ защищенности беспроводных сетей и оценка осведомленности персонала в вопросах информационной безопасности.

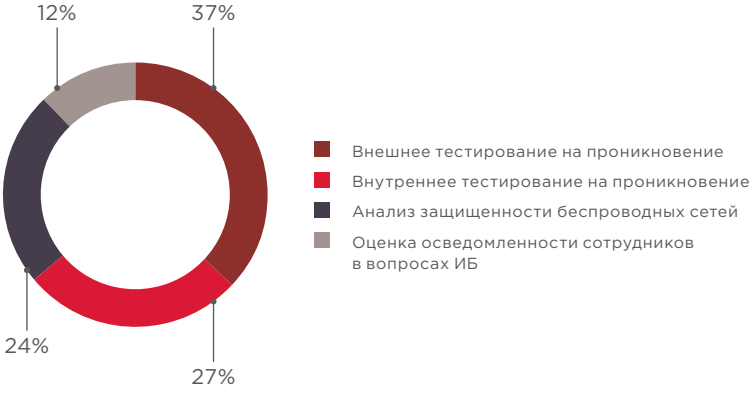

Рисунок 2. Виды проведенных работ

Общие результаты

При анализе защищенности наши эксперты выявляют различные уязвимости и недостатки механизмов защиты, которые можно разделить на четыре категории:

- недостатки конфигурации;
- отсутствие обновлений безопасности;
- уязвимости в коде веб-приложений;
- недостатки парольной политики.

Каждой уязвимости присваивается уровень риска (критический, высокий, средний или низкий), который рассчитывается в соответствии с системой классификации CVSS 3.0. Как и в прошлом году, практически во всех системах были обнаружены критически опасные уязвимости. В основном они связаны с недостатками парольной политики.

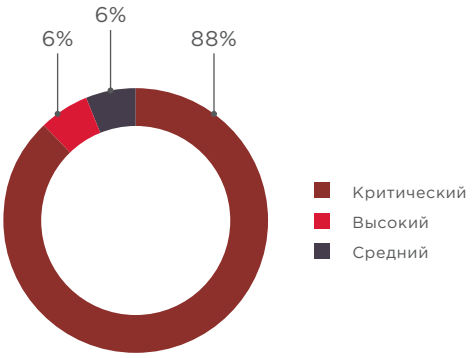

Рисунок 3. Максимальный уровень опасности уязвимостей (доля систем)

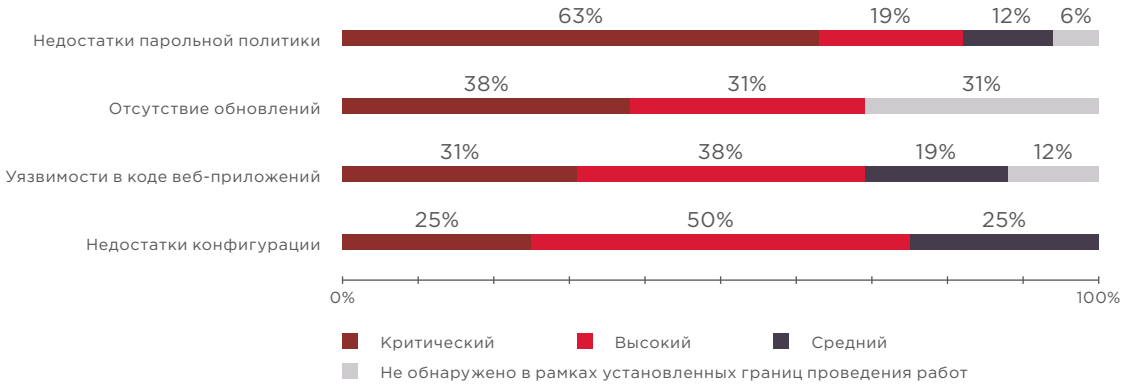

Рисунок 4. Максимальный уровень опасности уязвимостей (доля систем)

Важно учитывать, что работы по тестированию на проникновение проводятся методом черного ящика, поэтому невозможно выявить все уязвимости, существующие в системе. В инфраструктуре каждой компании могли присутствовать недостатки защиты, обусловленные отсутствием своевременного обновления ПО, уязвимостями в коде веб-приложений и использованием словарных паролей, которые не были обнаружены в ходе анализа. Целью тестирования является не поиск всех без исключения недостатков системы, а получение объективной оценки уровня ее защищенности от атак нарушителей.

Результаты внешних тестов на проникновение

В 92%
компаний удалось преодолеть сетевой периметр в рамках внешнего тестирования на проникновение

В 2018 году в рамках внешнего тестирования на проникновение удалось преодолеть сетевой периметр 92% компаний. В одном проекте доступ к ресурсам внутренней сети был возможен только с применением методов социальной инженерии.

В большинстве случаев проникнуть во внутреннюю сеть можно было несколькими способами. В среднем на одну систему приходилось два вектора, а максимальное число векторов проникновения, обнаруженных в одной системе, — пять. В половине компаний существовал способ преодолеть сетевой периметр всего за один шаг; как правило, он заключался в эксплуатации уязвимости в веб-приложении.

5 — максимальное число векторов проникновения, обнаруженных в одной системе

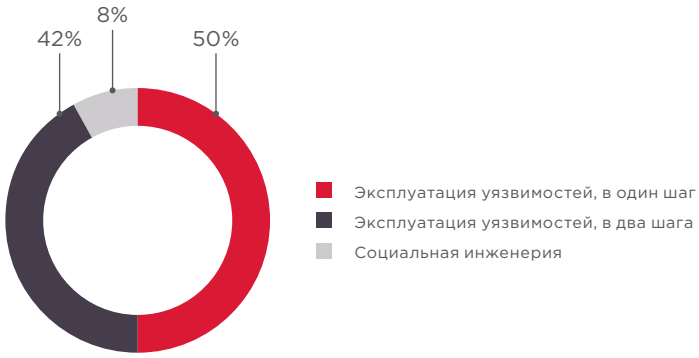

Рисунок 5. Кратчайший путь преодоления сетевого периметра (доля систем)

Три четверти векторов оказались связаны с недостаточной защитой веб-приложений: это основная проблема на сетевом периметре. При этом, если вектор состоял из нескольких шагов, на каждом шаге могли эксплуатироваться уязвимости разного типа. Типовой сценарий атаки — подбор словарной учетной записи пользователя веб-приложения и последующая эксплуатация уязвимости, возникшей из-за ошибок в коде веб-приложения, например возможности загрузки на сервер произвольных файлов.

Рисунок 6. Векторы проникновения во внутреннюю сеть

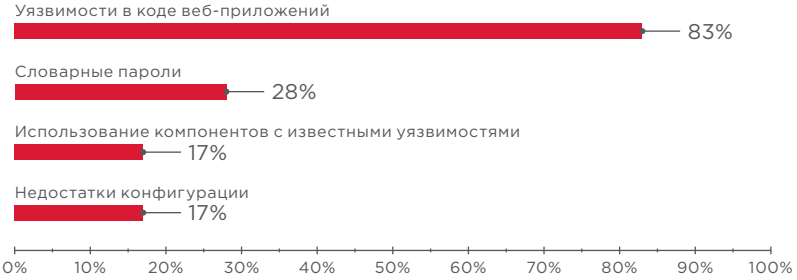

Рисунок 7. Уязвимости веб-приложений, позволившие преодолеть сетевой периметр (доли векторов)

Рекомендации

Регулярно проводить анализ защищенности веб-приложений. Чем сложнее веб-приложение и чем больше у него различных функций, тем выше вероятность того, что разработчики допустили в коде ошибку, которая позволит злоумышленнику провести атаку. Частично такие ошибки выявляются в рамках тестирования на проникновение, но наибольшее их число может быть выявлено только при проверке приложения методом белого ящика, подразумевающим анализ исходного кода. Для исправления уязвимостей обычно требуется внести изменения в код, на что может потребоваться значительное время. Чтобы сохранить непрерывность бизнес-процессов, рекомендуется применять межсетевой экран уровня приложений (web application firewall), который не позволит эксплуатировать уязвимость, пока ее не устранили, а также защитит от новых и еще не найденных уязвимостей.

Прочие векторы состояли преимущественно в подборе словарных паролей к различным системам — Outlook Web App (OWA), VPN-серверам и рабочим станциям, а также в использовании недостатков конфигурации сетевого оборудования. Преодоление периметра потенциально возможно и через устаревшие версии ПО, которые содержат уязвимости, позволяющие получить контроль над сервером. Для многих таких уязвимостей есть общедоступные эксплойты, но их эксплуатация может нарушить работу систем, поэтому заказчики, как правило, не соглашаются на проведение подобных проверок в рамках тестирования на проникновение.

Пример эксплуатации

+ Словарные пароли пользователей

В ходе тестирования на проникновение обнаружено, что для доступа к сервису OWA используется доменная учетная запись test:test1234. Подключившись к OWA, наши эксперты загрузили автономную адресную книгу (Offline Address Book), где содержатся идентификаторы пользователей домена. Подобрав словарный пароль к учетной записи одного из пользователей, эксперты подключились к шлюзу удаленных рабочих столов (RDG) и по протоколу RDP получили доступ к компьютеру сотрудника и внутренней сети.

Рисунок 8. Вектор проникновения, основанный на подборе словарных учетных записей

Пример эксплуатации

+ Интерфейс управления оборудованием доступен из внешних сетей
+ Словарные пароли пользователей
+ Использование уязвимой версии ПО. Выполнение произвольного кода

Один из распространенных вариантов проведения успешных атак в рамках тестирования — обнаружение на сетевом периметре интерфейсов систем, которые должны быть доступны исключительно из внутренней сети. Несколько лет подряд мы сталкиваемся с некорректной настройкой и уязвимостями в системах видеонаблюдения, и 2018 год не стал исключением. Можно было не только просматривать видео с камер, но и выполнить произвольный код из-за устаревшей версии прошивки видеорегистратора, причем одна из уязвимостей (CVE-2013-0143) была опубликована пять лет назад. Этот пример показывает, как важно правильно определять границы сетевого периметра и следить за состоянием защищенности каждого компонента системы.

Рисунок 9. Эксплуатация уязвимостей в системе видеонаблюдения

Десятка наиболее распространенных уязвимостей на сетевом периметре мало изменяется из года в год. Ранее мы отмечали существенное снижение доли компаний, где были выявлены словарные пароли, но в этом году они вернулись на первые строки рейтинга. Все еще широко распространено использование открытых протоколов передачи данных, в том числе для доступа к интерфейсам администрирования. Злоумышленник может перехватить учетные данные, передаваемые по открытым протоколам без использования шифрования, и получить доступ к соответствующим ресурсам. Более чем в половине систем внешнему нарушителю доступны интерфейсы удаленного доступа, управления оборудованием и подключения к СУБД.

Рекомендации

Ограничить количество сервисов на сетевом периметре, убедиться в том, что открытые для подключения интерфейсы действительно должны быть доступны всем интернет-пользователям. Регулярно проводить инвентаризацию ресурсов, доступных для подключения из интернета. Уязвимости могут появиться в любой момент, поскольку конфигурация инфраструктуры постоянно меняется, в ней появляются новые узлы, новые системы, и не исключены ошибки администрирования.

Отказаться от использования простых и словарных паролей, разработать строгие правила для корпоративной парольной политики и контролировать их выполнение.

19 лет назад
была опубликована самая старая из обнаруженных уязвимостей (CVE-1999-0024)

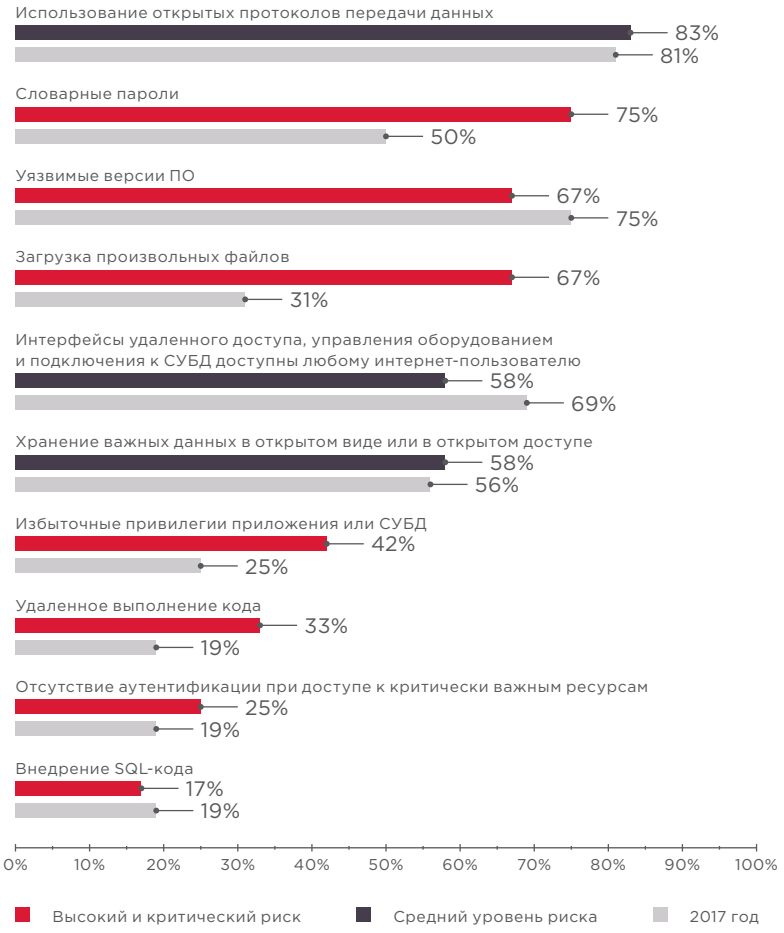

Рисунок 10. Наиболее распространенные уязвимости на сетевом периметре (доля систем)

На ресурсах сетевого периметра часто хранятся в открытом виде важные данные, которые помогают злоумышленнику развить атаку. Это могут быть резервные копии веб-приложений, конфигурационная информация о системе, учетные данные для доступа к критически важным ресурсам или идентификаторы пользователей, к которым злоумышленник может подобрать пароль.

Рекомендации

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. Если у компании не хватает ресурсов, чтобы выполнить такие проверки собственными силами, то мы рекомендуем привлекать сторонних экспертов для тестирования на проникновение.

Актуальной остается и проблема несвоевременного обновления ПО. Чаще всего мы выявляем уязвимые версии прикладного ПО, веб-серверов и веб-приложений, поставляемых вендорами.

Пример эксплуатации

+ Использование уязвимой версии ПО. Обход аутентификации
+ Использование уязвимой версии ПО. Выполнение произвольного кода

В ходе внешнего тестирования на проникновение на сетевом периметре компании была обнаружена устаревшая версия Cisco TelePresence Video Communication Server. Эта версия уязвима для атаки, направленной на обход аутентификации (CVE-2015-0653). В результате эксплуатации этой уязвимости был получен доступ к веб-интерфейсу администрирования.

Веб-интерфейс администрирования содержит встроенную функцию загрузки обновлений, которую можно использовать для выполнения команд на сервере. Для этого создается архив, содержащий набор команд на языке командного интерпретатора shell. Архив загружается на сервер в качестве файла с обновлениями, и в результате злоумышленник получает возможность выполнять произвольные команды.

На сервере был выявлен интерфейс внутренней сети, следовательно, дальше злоумышленник может развивать атаку на ресурсы ЛВС.

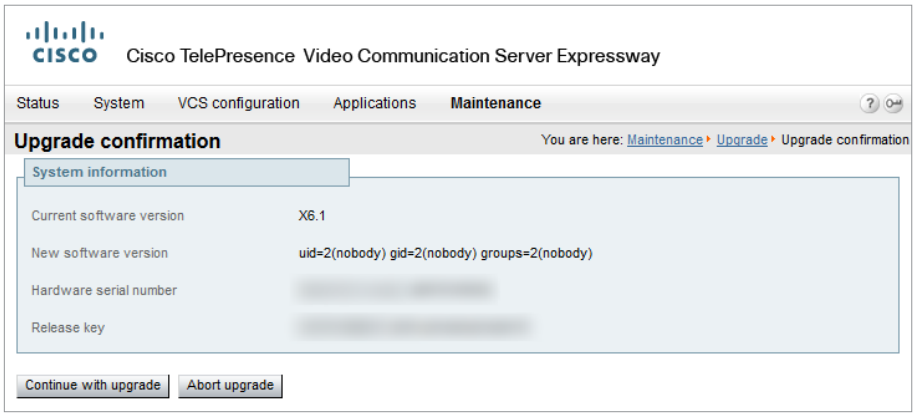

Рисунок 11. Выполнение команды id с информацией о текущем пользователе на сервере

Рекомендации

Своевременно устанавливать обновления безопасности для ОС и последние версии прикладного ПО. Обеспечить регулярный контроль появления ПО с известными уязвимостями на периметре корпоративной сети.

Результаты внутренних тестов на проникновение

Во всех исследуемых системах был получен полный контроль над внутренней инфраструктурой. В среднем для этого требовалось четыре шага. Типовой вектор атаки строится на подборе словарных паролей и восстановлении учетных записей из памяти ОС с помощью специальных утилит. Повторяя эти шаги, злоумышленник перемещается внутри сети от одного узла к другому вплоть до обнаружения учетной записи администратора домена.

Рекомендации

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 (на серверах — Windows Server 2012 R2 или выше) и включить привилегированных пользователей домена в группу Protected Users. Кроме того, можно использовать современные версии Windows 10 на рабочих станциях и Windows Server 2016 на серверах, в которых реализована система Remote Credential Guard, позволяющая изолировать и защитить системный процесс lsass.exe от несанкционированного доступа.

Обеспечить дополнительную защиту привилегированных учетных записей (в частности администраторов домена). Хорошей практикой является использование двухфакторной аутентификации.

Во всех исследуемых системах получен полный контроль над внутренней инфраструктурой

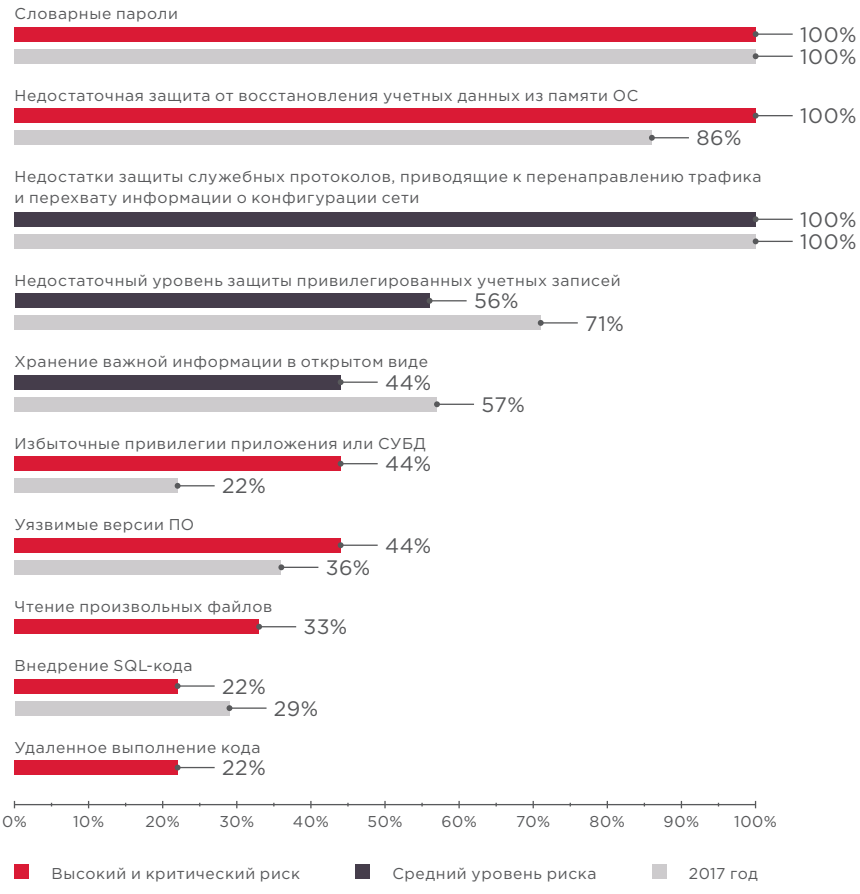

Рисунок 12. Наиболее распространенные уязвимости внутренней сети (доля систем)

Анализ сетевого трафика проводился в 78% компаний. В каждой из них присутствовали те или иные недостатки, которые позволяли перехватывать информацию, передаваемую по сети. Например, в 86% проанализированных систем отсутствовала защита протоколов NBNS и LLMNR. Злоумышленник может перехватить идентификаторы и хеш-суммы паролей пользователей с помощью атак NBNS Poisoning и LLMNR Poisoning, а затем подобрать пароли по полученным хеш-суммам.

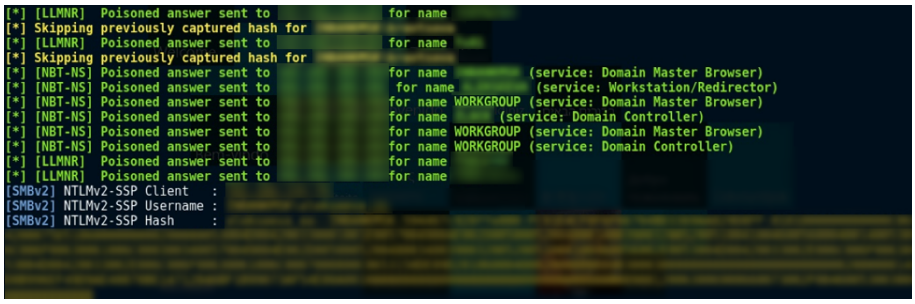

Рисунок 13. Перехват учетных данных пользователей путем атак NBNS Poisoning и LLMNR Poisoning

Рекомендации

Отключить не используемые в ЛВС протоколы канального и сетевого уровня. Если эти протоколы требуются для работы каких-либо систем, следует выделить для них отдельный сегмент сети, к которому нет доступа из пользовательского сегмента.

Во внутренней инфраструктуре компаний чаще всего встречались уязвимые версии ОС: они были выявлены в 44% протестированных систем. Отсутствие обновлений, особенно связанных с устранением критически опасных уязвимостей, помогает злоумышленнику развивать атаку внутри сети. Например, в каждой третьей системе была обнаружена уязвимость, описанная в бюллетене безопасности MS17-010, для эксплуатации которой еще в 2017 году был опубликован эксплойт EternalBlue. На отдельных узлах удавалось повысить привилегии с помощью уязвимостей, описанных в MS17-018, и CVE-2016-5195 (DirtyCow).

Пример эксплуатации

+ Недостаточная защита от восстановления учетных данных из памяти ОС
+ Уязвимые версии ПО. Удаленное выполнение произвольного кода (MS17-010)

Во время внутреннего тестирования на проникновение в результате эксплуатации уязвимости MS17-010 был получен доступ к серверу под управлением Windows Server 2012 R2. Эта версия ОС позволяет обеспечить защиту от восстановления учетных данных, но для этого привилегированные пользователи домена должны быть включены в группу Protected Users; это условие не было выполнено. На узле была запущена утилита mimikatz, и были получены из памяти ОС идентификаторы и пароли пользователей в открытом виде.

Среди извлеченных данных находился пароль учетной записи, которая обладает привилегиями локального администратора на серверах Microsoft Hyper-V. Одна из основных особенностей среды виртуализации на базе Hyper-V — это возможность скопировать жесткий диск виртуальной машины без ее выключения. Наши эксперты скопировали диск виртуальной машины, на которой был запущен контроллер домена. С этого диска были выгружены файлы ntds.dit и SYSTEM, а затем с помощью ПО secretsdump.py (из общедоступного набора Impacket) извлечены NTLM-хеш-суммы пользователей домена, в том числе NTLM-хеш-сумма пароля пользователя krbtgt.

```
(.env) > $ ./secretsdump.py Administrator@          -just-dc-user krbtgt
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:
[*] Cleaning up...
```

Рисунок 14. Получение хеш-суммы пароля пользователя krbtgt

Наличие NTLM-хеш-суммы пароля пользователя krbtgt позволяет провести атаку «Золотой билет Kerberos». Протокол Kerberos базируется на предоставлении билетов доступа к ресурсам доменной инфраструктуры. Привилегии служебной учетной записи krbtgt позволяют предоставить билеты Kerberos с любым уровнем доступа и обращаться к ресурсам с максимальными привилегиями. С помощью утилиты ticketer.py из набора Impacket был сгенерирован golden ticket и получена возможность выполнять команды ОС на контроллере домена с максимальными привилегиями.

Чтобы ликвидировать последствия атаки «Золотой билет Kerberos» потребуется не только дважды сбросить пароль служебной учетной записи krbtgt, но и переустановить все системы доменной инфраструктуры.

Результаты оценки осведомленности сотрудников в вопросах ИБ

Социальная инженерия — один из самых популярных и успешных способов проникновения во внутреннюю сеть компании. Поэтому в дополнение к работам по тестированию на проникновение важно проводить проверки осведомленности сотрудников в вопросах информационной безопасности. Работы выполняются по заранее согласованным сценариям, которые имитируют реальную атаку злоумышленника.

2639
электронных писем отправлено в 2018 году в рамках работ по оценке осведомленности пользователей

Проверки осуществляются путем телефонного взаимодействия и рассылки электронных писем. В телефонном разговоре предпринимаются попытки узнать у пользователей ту или иную ценную информацию. Электронные письма содержат вложенные файлы или ссылку на веб-ресурс, где требуется ввести учетные данные. В ходе проверки фиксируется реакция сотрудников: факты перехода по ссылке, ввода учетных данных или запуска вложения.

Почти треть пользователей перешла по ссылке или запустила приложенный файл, а каждый десятый сотрудник ввел свои учетные данные в фальшивую форму аутентификации. Заметная доля пользователей (14%) раскрыли конфиденциальную информацию в разговоре по телефону или вступили в переписку с условным злоумышленником, сообщив при этом дополнительные сведения о компании: имена и должности сотрудников, номера внутренних и мобильных телефонов.

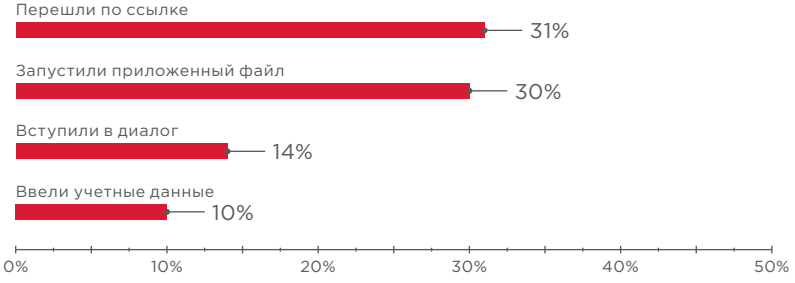

Рисунок 15. Результаты оценки осведомленности сотрудников

Рекомендации

С целью выявления и предотвращения атак методами социальной инженерии рекомендуется использовать специализированное антивирусное ПО со встроенной изолированной средой («песочницей») для динамической проверки файлов, способное выявлять и блокировать вредоносные файлы в корпоративной электронной почте до момента их открытия сотрудниками. Наиболее эффективным будет использование антивирусного ПО, построенного на решениях одновременно нескольких вендоров, способного обнаруживать скрытое присутствие вредоносных программ и позволяющего выявлять и блокировать вредоносную активность в различных потоках данных — в почтовом, сетевом и веб-трафике, в файловых хранилищах, на веб-порталах. Важно, чтобы выбранное решение позволяло проверять файлы не только в реальном времени, но и автоматически анализировало уже проверенные, это позволит выявить не обнаруженные ранее угрозы при обновлении баз сигнатур.

Регулярно проводить обучение сотрудников, направленное на повышение их компетенции в вопросах информационной безопасности, с контролем результатов.

Результаты анализа защищенности беспроводных сетей

Беспроводные сети являются потенциальным вектором проникновения во внутреннюю инфраструктуру компании. Злоумышленнику достаточно установить на ноутбук общедоступное ПО для атак на беспроводные сети и приобрести недорогой модем, который может работать в режиме мониторинга трафика. В семи из восьми протестированных систем беспроводные сети были доступны за пределами контролируемой зоны, а значит, злоумышленник мог бы проводить атаки, просто находясь на близлежащей территории, например на парковке рядом с офисом или в кафе на цокольном этаже здания.

Почти во всех сетях использовался протокол WPA2 с методами аутентификации PSK или EAP.

В 5 из 8
систем получен доступ к ЛВС через беспроводные сети

В 4 из 8
систем атаку удалось развить до получения максимальных привилегий в доменной инфраструктуре

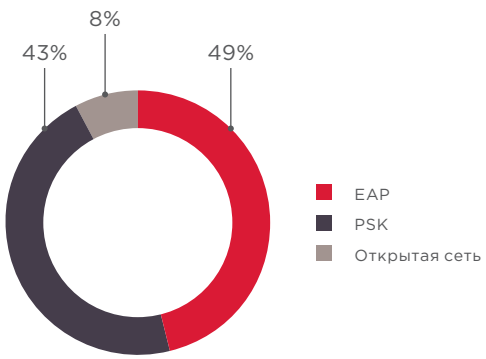

Рисунок 16. Методы аутентификации в беспроводных сетях

В одной промышленной компании через беспроводную сеть получен доступ **к ресурсам АСУ ТП**

В зависимости от используемого метода аутентификации проверяется возможность реализации разных типов атак. Для WPA2/PSK проводится перехват рукопожатия между точкой доступа и легитимным клиентом точки доступа с последующим подбором паролей методом перебора. Успех этой атаки обусловлен сложностью пароля. В ходе проверок было установлено, что словарные ключи для подключения к беспроводной сети используются в половине систем.

Другой способ атаки — создание поддельной точки доступа — применяется для любого метода аутентификации. Если при подключении к беспроводной сети не производится проверка подлинности сертификатов, то злоумышленник может создать поддельную точку доступа с идентичным названием сети (ESSID) и более мощным сигналом, чем у оригинальной. В случае подключения клиента к этой точке доступа злоумышленник получает его идентификатор в открытом виде и значение NetNTLM v1 challenge-response, с помощью которого может подобрать пароль методом перебора.

Проверка сертификатов отсутствовала в трех системах. Если она все же осуществляется, то злоумышленник может взять название известной публичной точки доступа. Например, среди жителей Москвы популярна сеть MT_FREE, которая развернута в городском общественном транспорте. Даже если оригинальная точка доступа использует механизмы защиты, поддельная сеть может быть открытой и подключение к ней пройдет незаметно для пользователя. В более общем случае возможно проведение так называемой KARMA-атаки. Многие устройства пользователей отправляют запросы с целью найти ранее сохраненные беспроводные сети. Злоумышленник может создавать поддельные открытые точки доступа, представляясь той сетью, название которой содержится в запросе. Такие атаки применяются в совокупности с использованием ложной формы аутентификации, оформленной в корпоративном стиле. При подключении к сети пользователь перенаправляется на страницу с формой аутентификации, где ему предлагается ввести корпоративную учетную запись. Результат атаки зависит от того, насколько сотрудники компании осведомлены в вопросах информационной безопасности.

Рисунок 17. Проведение KARMA-атаки с использованием фишинговой формы аутентификации

В 7 из 8 систем не обеспечивается изоляция пользователей

Для гостевой сети важно, чтобы обеспечивалась изоляция пользователей, а сотрудники компании не пользовались ею с тех устройств, с которых подключаются к корпоративным беспроводным сетям. Злоумышленник, получивший доступ к гостевой сети, где нет изоляции, сможет атаковать пользователей и получить в открытом виде пароли от других точек доступа Wi-Fi, если сотрудник сохраняет их для автоматического подключения. В результате злоумышленник получит пароль от корпоративной сети без атаки на нее.

Рекомендации

Для повышения безопасности гостевой сети необходимо использовать надежные механизмы шифрования (WPA2). Важно обеспечить изоляцию пользователей точки доступа, а также запретить ее использование сотрудниками компании. Гостевую сеть необходимо отделять от ресурсов ЛВС.

Корпоративная сеть должна быть защищена стойким паролем. Нужно ограничивать зону ее действия так, чтобы она не была доступна за пределами контролируемой зоны. На устройствах сотрудников следует настроить проверку подлинности сертификатов при подключении к корпоративным сетям, чтобы исключить возможность успешного проведения атак с использованием поддельной точки доступа.

Необходимо повышать осведомленность сотрудников в вопросах информационной безопасности при пользовании беспроводными сетями. Для этого следует проводить периодические тренинги с контролем результатов.

Рекомендуется регулярно проводить анализ защищенности беспроводных сетей, чтобы выявлять ошибки конфигурации и потенциальные векторы проникновения во внутреннюю сеть.

Факты о словарных паролях

Словарные пароли чаще всего встречались у доменных учетных записей и при доступе к веб-приложениям — как на сетевом периметре, так и во внутренней инфраструктуре компаний.

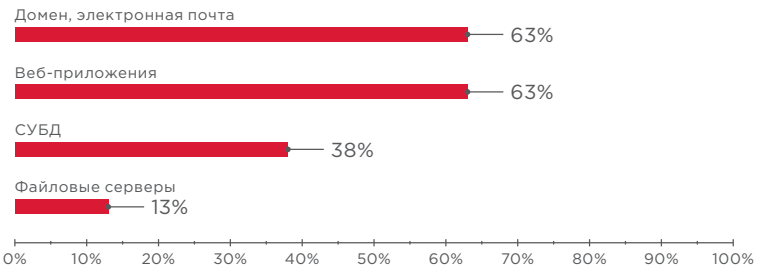

Рисунок 18. Словарные пароли (доля систем)

Qwerty123
и другие сочетания близких клавиш остаются самыми популярными паролями

admin
самый распространенный пароль среди привилегированных пользователей

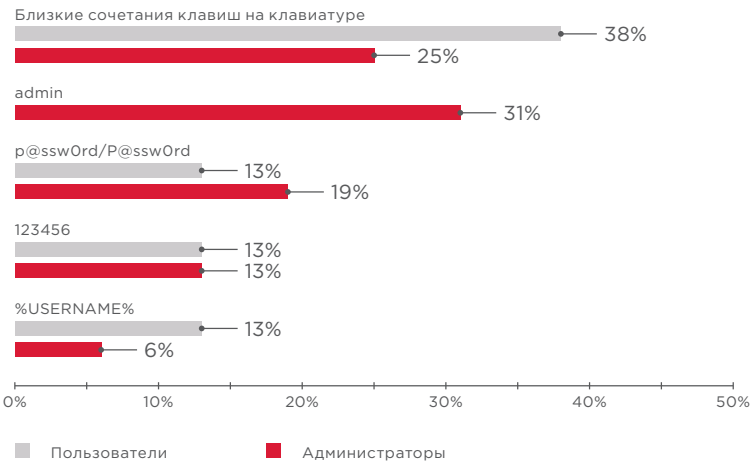

Рисунок 19. Самые распространенные пароли (доля систем)

В некоторых компаниях мы выявляли пароли вида [месяц в английской раскладке + год], например Yjz,hm2018 (Ноябрь2018). В основном такие пароли устанавливаются по умолчанию, например для первого входа в систему, с тем, чтобы сотрудник впоследствии сменил пароль на более сложный. Однако зачастую пользователи забывают сменить пароль, а иногда выбирают подобные легко запоминаемые сочетания сознательно, полагая, что они обеспечивают достаточный уровень безопасности.

Заключение

Корпоративные информационные системы остаются уязвимыми для атак злоумышленников. С каждым годом увеличивается доля компаний, где удается получить доступ к ресурсам внутренней сети от лица внешнего злоумышленника. Использование методов социальной инженерии и эксплуатация недостатков защиты беспроводных сетей дополнительно повышают шансы на успешное преодоление сетевого периметра. Дальнейшее развитие атаки из сегмента внутренней сети уже второй год подряд приводит к получению полного контроля над инфраструктурой во всех протестированных системах.

Как правило, векторы атак основываются на эксплуатации известных недостатков безопасности и в большинстве своем не требуют от злоумышленника глубоких технических знаний. Для поддержания высокого уровня защищенности системы необходимо соблюдать общие принципы обеспечения информационной безопасности. Рекомендации по устранению наиболее распространенных уязвимостей приведены в данном отчете.

На сетевом периметре компаний основная проблема безопасности заключается в недостаточной защите веб-приложений. Следует регулярно проводить анализ защищенности веб-приложений, при этом наиболее эффективным методом проверки является метод белого ящика, подразумевающий анализ исходного кода. В качестве превентивной меры рекомендуется использовать межсетевой экран уровня приложений (web application firewall) для предотвращения эксплуатации уязвимостей, которые могут появляться при внесении изменений в код или добавлении новых функций.

Только своевременное выявление попыток атаки позволит предотвратить ее до того, как злоумышленник нанесет существенный ущерб компании, поэтому следует применять технические решения, направленные на обнаружение подозрительной активности. Для эффективного реагирования на инциденты информационной безопасности рекомендуется использовать системы управления, анализа и мониторинга событий безопасности (SIEM-системы), которые позволяют выявлять злонамеренную активность в сети, попытки взлома инфраструктуры, присутствие злоумышленника и помогают принимать оперативные меры по нейтрализации угроз.

В рамках тестирования на проникновение действия экспертов редко обнаруживаются службой безопасности компаний, следовательно, и реальные злоумышленники могут долгое время находиться в инфраструктуре и оставаться незамеченными. Поэтому важно не только защищать сетевой периметр, но и проводить регулярный ретроспективный анализ сети с целью выявить уже случившееся проникновение. Для поиска следов компрометации рекомендуется использовать специализированные средства глубокого анализа сетевого трафика, способные обнаруживать сложные целевые атаки как в реальном времени, так и в сохраненных копиях трафика. Такое решение даст возможность не только увидеть факты взлома, но и отслеживать сетевые атаки, в том числе запуск вредоносных утилит, эксплуатацию уязвимостей ПО и атаки на контроллер домена. Это позволит уменьшить время скрытного присутствия нарушителя в инфраструктуре и тем самым минимизировать риски утечки важных данных и нарушения работы бизнес-систем, снизить возможные финансовые потери.

Наши исследования свидетельствуют о низком уровне осведомленности пользователей в вопросах информационной безопасности, поэтому необходимо организовывать тренинги для сотрудников, с периодическим контролем результатов. Дополнительно рекомендуется использовать специальное антивирусное ПО, которое проверяет файлы в изолированной среде, выявляет присутствие вредоносных программ и помогает блокировать вредоносную активность.

Важно следовать всем рекомендациям в комплексе, так как даже отдельные пробелы в механизмах защиты могут послужить причиной взлома инфраструктуры и компрометации критически важных ресурсов. Рекомендуется регулярно проводить тестирование на проникновение, чтобы выявлять векторы атак на корпоративную систему и на практике оценивать эффективность принятых мер защиты.

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

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.

Corp-Vulnerabilities-2019_A4.RUS.0006.05.JUN.07.2019