

Уязвимости периметра корпоративных сетей

**Результаты инструментального
анализа защищенности**

Содержание

Что такое инструментальный анализ защищенности	3
Об исследовании	3
Ключевые итоги	4
Сводная статистика: есть над чем задуматься	5
Как избавиться от лишнего: инвентаризация сервисов	6
Корень зла — устаревшие версии ПО и небезопасные протоколы	9
Типы уязвимостей	11
Выполнение произвольного кода	12
Отказ в обслуживании	12
Повышение привилегий	13
Разглашение информации	14
Выводы и рекомендации	15
Режимы сканирования MaxPatrol 8	16

Что такое инструментальный анализ защищенности

Грамотная оценка защищенности корпоративной инфраструктуры требует времени и высокой квалификации специалистов по ИБ. На помощь могут прийти средства анализа защищенности — специальные системы, которые в автоматизированном режиме выявляют открытые сетевые порты и доступные службы, уязвимости в ПО, а также недостатки конфигурации оборудования, серверов и средств защиты. Современные средства анализа защищенности позволяют проводить сканирование информационных систем в различных режимах в зависимости от конкретной задачи — сетевое сканирование, системные проверки, контроль соответствия стандартам безопасности.

Инструментальный анализ защищенности относится к превентивным мерам защиты, и его главная цель — своевременно обнаружить недостатки, чтобы специалисты по ИБ в организации могли устранить их и тем самым предотвратить возможные атаки. При этом сокращаются трудозатраты на анализ защищенности системы и минимизируется влияние человеческого фактора.

Об исследовании

В этом отчете мы поделимся результатами инструментального анализа защищенности сетевых периметров корпоративных информационных систем. Сканирование осуществлялось с помощью автоматизированной системы контроля защищенности и соответствия стандартам MaxPatrol 8 в режиме PenTest. Подробное описание режимов сканирования MaxPatrol 8 можно найти в конце отчета.

В исследование включены результаты 19 наиболее информативных проектов 2019 и первой половины 2020 года. Это те проекты, заказчики которых не накладывали существенных ограничений на список ресурсов, вошедших в границы проведения работ, и дали согласие на публикацию результатов их сканирования в обезличенном виде. Всего было просканировано 3514 узлов, включая сетевые устройства, серверы и рабочие станции.

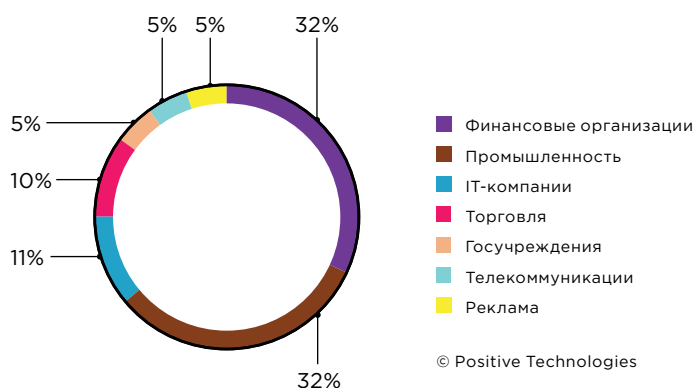


Рисунок 1. Распределение исследованных систем по отраслям экономики

Исследование представляет интерес для специалистов, занимающихся вопросами управления уязвимостями ИБ. Мы расскажем, какие сервисы чаще всего доступны на сетевом периметре и какие потенциальные бреши в его защите выявляются с помощью инструментального сканирования; приведем статистику выявленных уязвимостей по степени риска и наличию общедоступных эксплойтов. Степень риска определена на основе значения Common Vulnerability Scoring System (CVSS) версии 2. Верификация выявленных уязвимостей не проводилась.

Ключевые итоги

- На внешних сетевых ресурсах 84% организаций выявлены уязвимости высокого уровня риска.
- Каждой десятой уязвимостью может воспользоваться даже низкоквалифицированный злоумышленник, использовав для этого готовый публичный эксплойт.
- Каждая вторая уязвимость может быть устранена установкой актуальных обновлений ПО.
- Риску заражения шифровальщиком WannaCry все еще подвержены 26% организаций.
- В 74% организаций служба SSH напрямую доступна для подключения из интернета. В то же время каждая пятая уязвимость в ПО связана с ошибками в OpenSSH, которые могут привести к получению контроля над ресурсами сетевого периметра или к проникновению в локальную сеть.
- На периметре всех организаций выявлены узлы, уязвимые для атаки SWEET32, а для 84% из них до сих пор актуальна атака POODLE. Если злоумышленнику удастся реализовать эти атаки, он сможет извлечь конфиденциальные данные из зашифрованных соединений.

Сводная статистика: есть над чем задуматься

1. В ходе инструментального анализа обнаружены 9483 уязвимости на 599 узлах. Выявленные уязвимости связаны с отсутствием актуальных обновлений ПО, использованием устаревших алгоритмов и протоколов, недостатками конфигурации, ошибками в коде веб-приложений, учетными записями с простыми паролями и паролями по умолчанию.

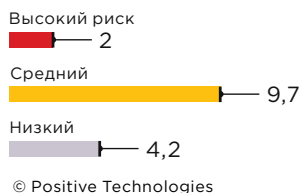


Рисунок 2. Среднее число уязвимостей на одном узле в зависимости от уровня риска

2. Для 10% выявленных уязвимостей существуют общедоступные эксплойты, а значит — каждую десятую уязвимость злоумышленник может проэксплуатировать даже не имея профессиональных навыков программирования или опыта обратной разработки.

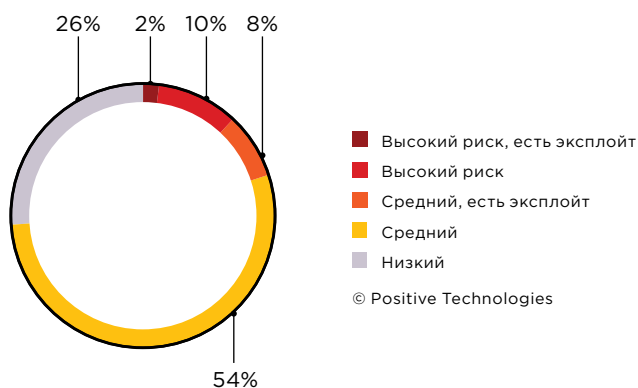


Рисунок 3. Распределение уязвимостей по уровню риска

3. В 84% организаций выявлены уязвимости высокого уровня риска. В 58% организаций обнаружены уязвимости высокого уровня риска, для которых существуют общедоступные эксплойты.

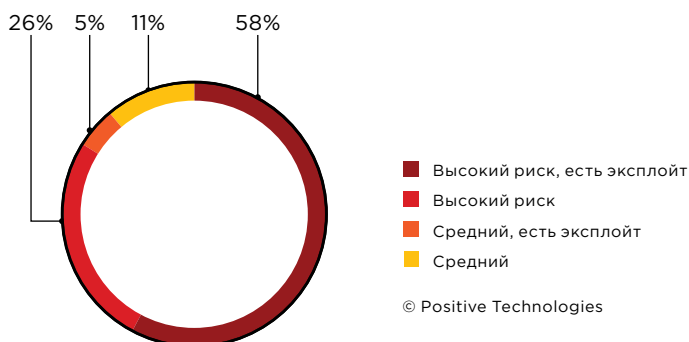


Рисунок 4. Максимальный уровень риска уязвимостей (доля организаций)

Как избавиться от лишнего: инвентаризация сервисов

На узлах, где в ходе инструментального сканирования не были выявлены уязвимости, оказались доступны лишь единичные сервисы, причем стоит отметить, что эти сервисы имели актуальные обновления ПО и безопасную конфигурацию. В связи с этим мы полагаем, что выстраивание защищенного периметра должно начинаться с инвентаризации ресурсов, то есть с поиска и отключения активных, но неиспользуемых служб. Далее мы расскажем, какие сервисы доступны на периметре большинства организаций и какие основные недостатки безопасности с ними связаны.

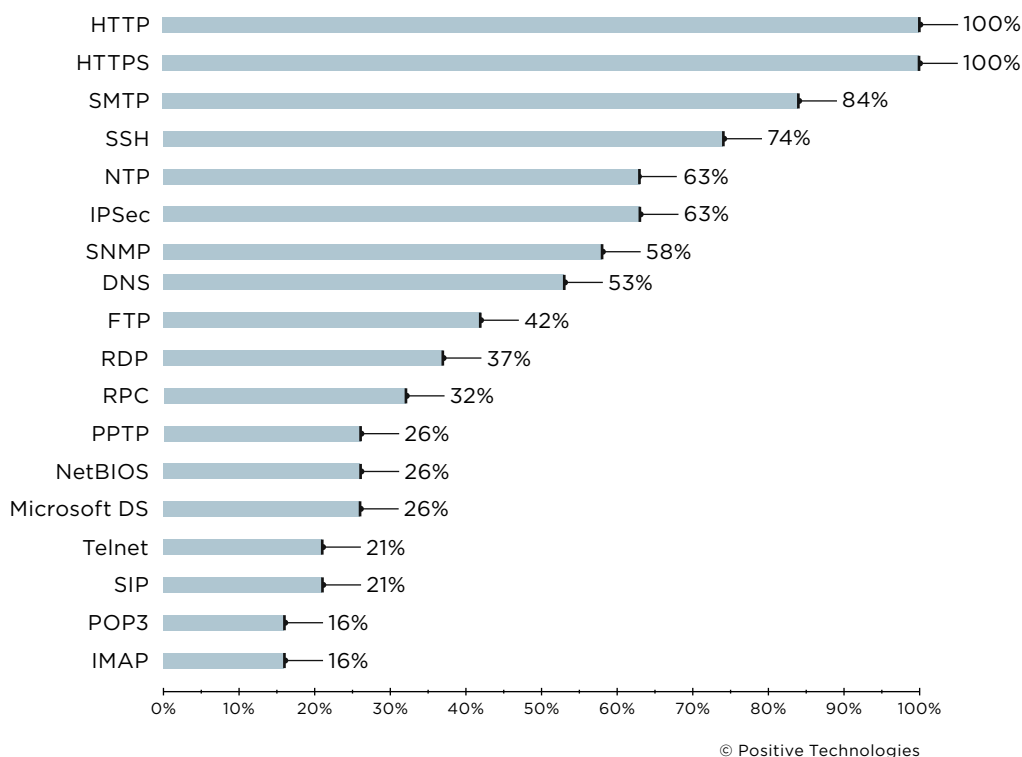


Рисунок 5. Службы, доступные на сетевом периметре (доля организаций)

В 26% организаций на узлах с внешними сетевыми интерфейсами открыт сетевой порт 445/TCP, что подвергает корпоративную инфраструктуру риску заражения шифровальщиком [WannaCry](#).

На множестве ресурсов были выявлены интерфейсы удаленного доступа и администрирования, например SSH, RDP, Telnet. Это позволяет любому внешнему злоумышленнику проводить атаки на подбор учетных данных для подключения к соответствующим сервисам. Так, в одной из организаций были выявлены открытый сетевой порт для подключения по протоколу Telnet и учетная запись Cisco:123456. Подобные простые пароли злоумышленники подбирают за считанные минуты, а получив доступ к сетевому оборудованию с правами соответствующей учетной записи — могут развить вектор нападения. Кроме того, есть риск, что узел попадет под брутфорс-атаку со стороны ботнета и сам станет его частью в случае успеха этой атаки. Например, ботнет [Dark Nexus](#) компрометирует устройства посредством эксплуатации известных уязвимостей в ПО и подбора учетных данных для подключения по Telnet, после чего эти устройства используются для DDoS-атак.

Как защитить удаленное администрирование серверов

Ограничьте доступ к интерфейсам управления списком разрешенных IP-адресов вашей внутренней сети. Откажитесь от использования протокола Telnet, так как учетные данные передаются по нему в открытом виде. Для администрирования серверов используйте SSH. Чтобы сделать SSH-соединения более защищенными:

- настройте аутентификацию по открытому ключу;
- используйте нестандартный порт для защиты от массовой автоматизированной атаки;
- запретите доступ по SSH для учетной записи root.

На периметре 84% организаций открыт сетевой порт 25/TCP, на котором доступна служба отправки электронной почты SMTP. Данные по протоколу SMTP передаются в открытом виде, а значит, как и в случае с HTTP, злоумышленник может перехватывать трафик и читать корпоративную переписку. Кроме того, небезопасная конфигурация почтовых серверов может приводить к утечке почтовых адресов организации. Нередко IT-администраторы не отключают возможность выполнять команды VRFY, EXPN и RCPT TO. В результате у злоумышленника появляется возможность по ответам SMTP-сервера подбирать адреса электронной почты, причем взломщик может легко автоматизировать этот процесс: для этого существует готовая общедоступная утилита. В дальнейшем собранные таким образом адреса сотрудников могут использоваться при подборе учетных данных для подключения к ресурсам сетевого периметра или внутренней сети через службы удаленного доступа — либо для фишинговых рассылок.

```
root@kali:~/smtp-user-enum# perl smtp-user-enum.pl -M RCPT -U /root/ /4test.txt -D 
-t @ptsecurity.com
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
| Scan Information |
-----

Mode ..... RCPT
Worker Processes ..... 5
Usernames file ..... /root/ /4test.txt
Target count ..... 1
Username count ..... 78
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....

##### Scan started at Mon Nov 18 06:14:40 2019 #####
: exists
: exists
: exists
##### Scan completed at Mon Nov 18 06:15:29 2019 #####
3 results.

78 queries in 49 seconds (1.6 queries / sec)
```

Рисунок 6. Подбор адресов электронной почты методом RCPT

На периметре 42% организаций доступны для подключения FTP-серверы. Если FTP-сервер защищен ненадежным паролем, то подобрав учетные данные, злоумышленник не только получит доступ к файлам, но и попытается развить атаку. В ходе одного из проектов по тестированию на проникновение инструментальное сканирование выявило на узле периметра открытый сетевой порт, на котором работал FTP-сервер vsFTPd. Имея некоторую ранее собранную информацию об анализируемой системе, наши специалисты смогли подобрать логин и пароль для подключения по протоколу FTP. Подключившись, они обнаружили файлы веб-приложения и, загрузив веб-интерпретатор командной строки, получили возможность выполнять на узле команды ОС.

В двух организациях был разрешен анонимный вход на FTP-серверы, из-за чего возникал риск по ошибке предоставить доступ к файлам, которые не должны быть общедоступными. Более серьезная угроза возникает, когда без аутентификации на FTP-сервер разрешено загружать файлы: в этом случае у злоумышленника появляется больше возможностей. Например, он может использовать FTP-сервер как площадку для размещения вредоносного ПО.

Однако даже используя надежную парольную защиту, не стоит забывать, что старые версии программных реализаций FTP содержат множество известных уязвимостей. Кроме того, учетные данные по протоколу FTP передаются в открытом виде, поэтому мы рекомендуем использовать его защищенные версии — FTPS или SFTP.

На периметре каждой организации открыты сетевые порты 80/TCP и 443/TCP. Как правило, на этих сетевых портах работают приложения под управлением веб-серверов Apache HTTP Server, Apache Tomcat, nginx и других. Идентифицировав веб-сервер и его версию, злоумышленник сможет подобрать необходимые эксплойты. Согласно результатам нашего исследования, для 16% уязвимостей веб-серверов готовые эксплойты есть в открытом доступе.

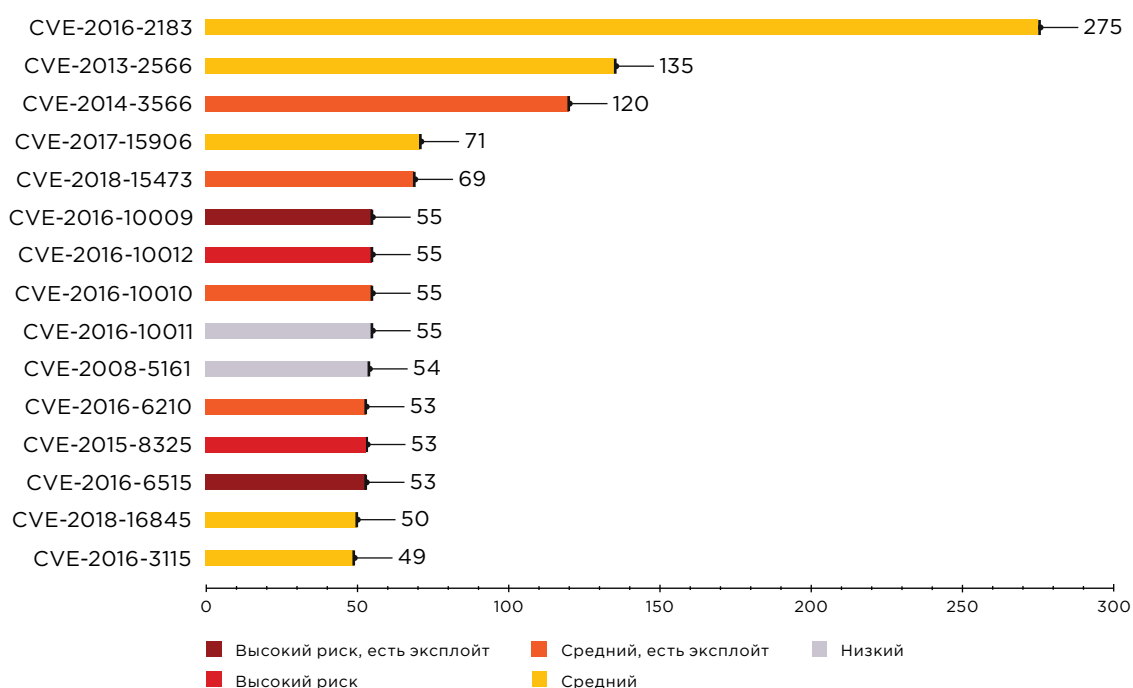
Доступность сетевого порта 80/TCP означает, что возможен обмен данными по протоколу HTTP. Как известно, HTTP-трафик передается в незашифрованном виде, а значит, злоумышленник может перехватить его, например вынудив жертву подключиться к поддельной точке доступа. Если при этом учетные данные передаются методом Basic (в кодировке Base64), то злоумышленник сможет легко декодировать их и получить пароль для доступа к веб-приложению.

Распределение уязвимостей по сервисам и уровням риска

Сервис	Высокий риск, эксплойт	Высокий риск	Средний риск, эксплойт	Средний риск	Низкий риск
Веб-сервисы	24	609	344	3659	1507
Удаленный доступ	110	192	234	452	441
Служба доменных имен	36	183	21	227	15
Электронная почта	—	10	102	598	437
VPN-сервисы	—	—	12	30	24
Файловые службы	—	—	4	49	19
Другие	—	7	14	72	51

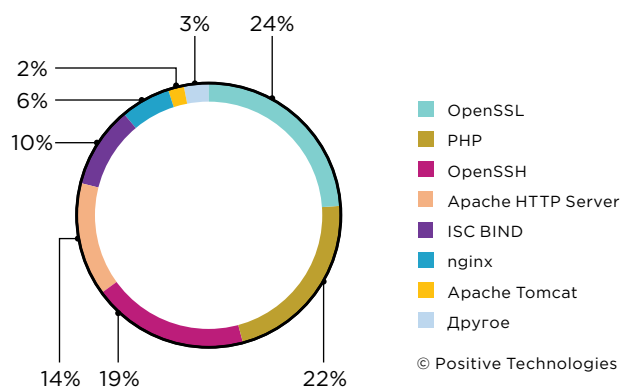
Корень зла — устаревшие версии ПО и небезопасные протоколы

Как показывают результаты инструментального анализа защищенности сетевых периметров, почти половина (47%) выявленных уязвимостей могут быть устранены установкой актуальных версий ПО. Проблемы с наличием обновлений были выявлены во всех организациях, а в 42% организаций используются программные продукты, производители которых официально прекратили поддержку и больше не выпускают обновления безопасности. Например, в 32% организаций есть приложения, написанные на языке программирования PHP версии 5, который не поддерживается с января 2019 года. К слову, возраст самой старой уязвимости, обнаруженной в ходе инструментального анализа, составляет 16 лет.



© Positive Technologies

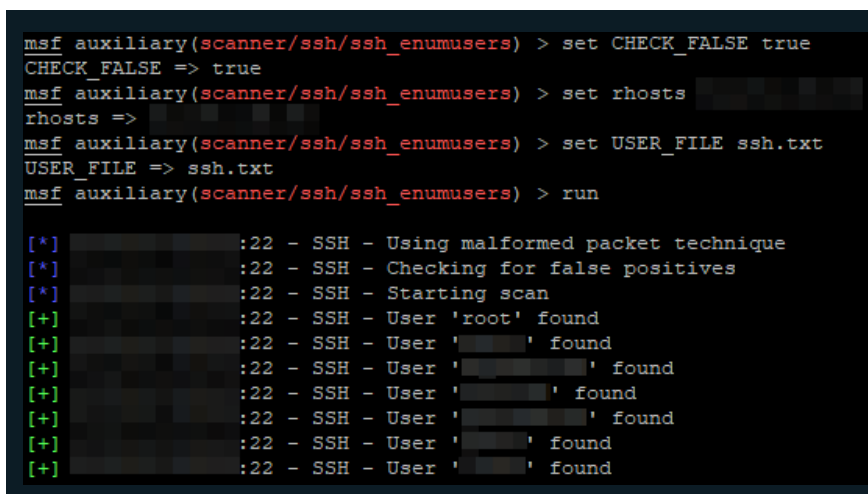
Рисунок 7. Самые распространенные уязвимости на сетевом периметре (количество узлов)



© Positive Technologies

Рисунок 8. Уязвимое ПО (доля уязвимостей, связанных с использованием устаревших версий)

В ходе инструментального анализа было выявлено более тысячи уязвимостей, связанных с устаревшими версиями OpenSSH, для 27% из них в свободном доступе есть эксплойты. Так, например, в 58% организаций в ходе инструментального анализа была найдена уязвимость [CVE-2018-15473](#) в пакете OpenSSH версий ниже 7.7. Она позволяет определить идентификаторы существующих в системе пользователей. Для этого злоумышленнику требуется отправить специально сформированный запрос на аутентификацию. Если включенный в запрос идентификатор не существует в системе, то сервер ответит сообщением об ошибке, а если существует — соединение будет прервано без ответа. Для автоматизации процесса есть общедоступный инструмент. Эту уязвимость наши специалисты неоднократно использовали в ходе тестов на проникновение.



```
msf auxiliary(scanner/ssh/ssh_enumusers) > set CHECK_FALSE true
CHECK_FALSE => true
msf auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 192.168.1.10
rhosts => 192.168.1.10
msf auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE ssh.txt
USER_FILE => ssh.txt
msf auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.1.10:22 - SSH - Using malformed packet technique
[*] 192.168.1.10:22 - SSH - Checking for false positives
[*] 192.168.1.10:22 - SSH - Starting scan
[+] 192.168.1.10:22 - SSH - User 'root' found
[+] 192.168.1.10:22 - SSH - User 'user' found
[+] 192.168.1.10:22 - SSH - User 'admin' found
[+] 192.168.1.10:22 - SSH - User 'guest' found
[+] 192.168.1.10:22 - SSH - User 'nobody' found
[+] 192.168.1.10:22 - SSH - User 'daemon' found
```

Рисунок 9. Эксплуатация уязвимости CVE-2018-15473

С использованием небезопасных версий протокола SSL/TLS и устаревших версий криптографической библиотеки OpenSSL связаны 16% всех выявленных уязвимостей. В каждой организации выявлены узлы, уязвимые для атаки [SWEET32](#) ([CVE-2016-2183](#)), в 84% организаций — для атаки [POODLE](#) ([CVE-2014-3566](#)). Отметим, что для реализации этих атак у злоумышленника должна быть возможность перехватывать информацию между клиентом и сервером и модифицировать ее. В случае успешной эксплуатации злоумышленник может восстановить зашифрованные данные, например значения HTTP-cookies. Предотвратить атаку SWEET32 возможно отказавшись от использования блочных алгоритмов шифрования с длиной блока 64 бита (Blowfish, DES, 3DES). Для защиты от атаки POODLE откажитесь от использования SSL версии 3. Если по каким-то причинам это невозможно, активируйте механизм [TLS_FALLBACK_SCSV](#).

В 53% организаций обнаружены узлы, уязвимые для атаки [DROWN](#). Атака возможна из-за уязвимости [CVE-2016-0800](#) в реализации протокола SSL версии 2. В результате атаки при определенных условиях злоумышленник может завладеть сеансовыми ключами, которые передаются в SSL-сессиях, а значит — получить доступ ко всей информации, передаваемой по зашифрованному каналу.

В двух организациях были выявлены серверы, подверженные нашеству в 2014 году уязвимости Heartbleed ([CVE-2014-0160](#)) в OpenSSL 1.0.1. Она позволяет извлечь из оперативной памяти сервера закрытые ключи шифрования и пароли пользователей. Для уязвимости существует готовый эксплойт.

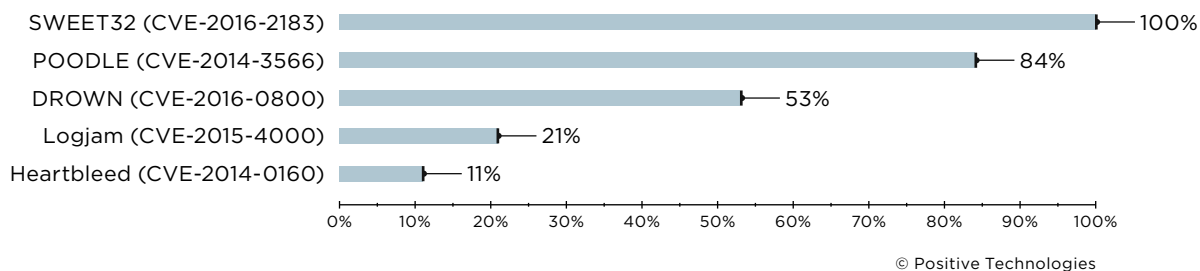


Рисунок 10. Известные уязвимости в SSL/TLS и OpenSSL (доля организаций)

Уязвимости, из-за которых разработчики ПО вынуждены периодически выпускать обновления безопасности, а компании — тщательно следить за выходом этих обновлений, связаны с ошибками, допущенными в программном коде. Каждую такую уязвимость мы соотнесли с недостатками ПО из списка [Common Weakness Enumeration \(CWE\)](#). В результате мы выяснили, что 30% уязвимостей, выявленных в устаревших версиях ПО и коде веб-приложений, связаны с наиболее опасными программными ошибками по версии MITRE (рейтинг [2019 CWE Top 25 Most Dangerous Software Errors](#)). В рейтинг MITRE вошли наиболее распространенные критические ошибки, которые злоумышленники легко находят и эксплуатируют, что позволяет им похитить информацию, вызвать отказ в обслуживании или получить полный контроль над уязвимым приложением.

Типы уязвимостей

Для удобства мы сгруппировали все выявленные в ходе инструментального сканирования уязвимости по категориям. Ниже представлены наиболее распространенные категории — те, которые встретились как минимум в половине организаций.

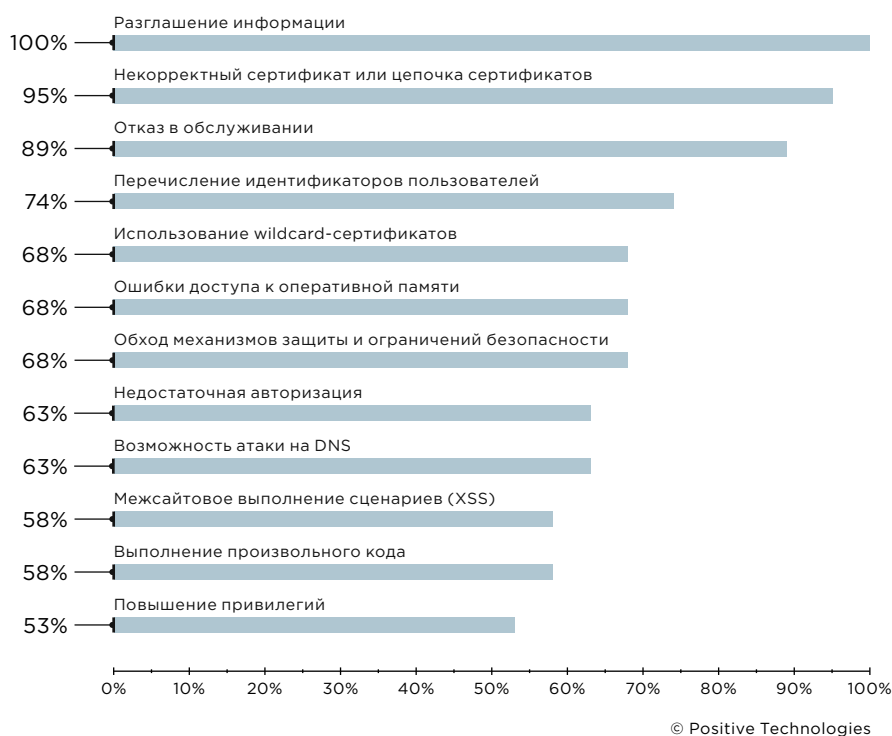


Рисунок 11. Наиболее распространенные категории уязвимостей (доля организаций)

В 95% организаций на ряде узлов обнаружены недостатки конфигурации, связанные с SSL-сертификатами. К ним относятся сертификаты с некорректной подписью, самоподписанные сертификаты, сертификаты с истекшим сроком действия, цепочки сертификатов, базирующиеся на недоверенном сертификате. В 68% организаций используются wildcard-сертификаты. Такой сертификат отличается от обычного тем, что выдается не только на доменное имя, но и на все поддомены следующего уровня. Использование wildcard-сертификатов экономит деньги организации и упрощает поддержку сертификатов в актуальном состоянии. Однако если такой сертификат будет скомпрометирован, под угрозой окажется не одно приложение, а множество.

К категории «Ошибки доступа к оперативной памяти» мы отнесли уязвимости, связанные с выделением и освобождением памяти, которые в зависимости от условий и сценариев эксплуатации могут приводить к различным последствиям: повреждению данных, утечке памяти, аварийному завершению работы ПО или выполнению произвольного кода.

Выполнение произвольного кода

Почти две трети (64%) выявленных уязвимостей, связанных с возможностью выполнения произвольного кода, имеют высокий уровень риска. Наиболее распространенная уязвимость (выявлена в 37% организаций) — [CVE-2017-12617](#) в Apache Tomcat. С помощью нее злоумышленник может загрузить на уязвимый сервер JSP-файл и выполнить код, содержащийся в этом файле.

Для 16% выявленных уязвимостей, связанных с выполнением произвольного кода, существуют общедоступные эксплойты. К таким уязвимостям, например, относится [CVE-2015-1635 \(MS15-034\)](#) в серверных версиях Windows. Она позволяет удаленно, через специально сформированные HTTP-запросы, выполнять код с максимальными привилегиями в системе. К счастью, эта опасная уязвимость сегодня встречается редко: она была выявлена на серверах только двух организаций.

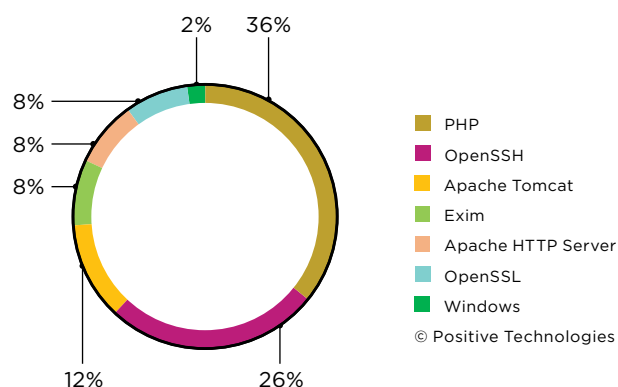


Рисунок 12. Уязвимое ПО (доля выявленных уязвимостей, связанных с выполнением произвольного кода)

Отказ в обслуживании

Уязвимости, приводящие к отказу в обслуживании, в основном вызваны ошибками в проверках входных данных, некорректной работой с памятью (ошибки при работе с переменными в стеке или куче, неверная работа с указателями), бесконтрольным выделением ресурсов. Например, уязвимость [CVE-2016-6515](#) в OpenSSH связана с отсутствием ограничений на количество символов при

вводе пароля. Существует публичный эксплойт, с помощью которого злоумышленник может отправить пароль длиной несколько десятков тысяч символов, что вызовет высокую загрузку процессора устройства. Эксплуатация подобных уязвимостей приводит к недоступности сервисов на сетевом периметре и, как следствие, к репутационным и финансовым потерям организации.

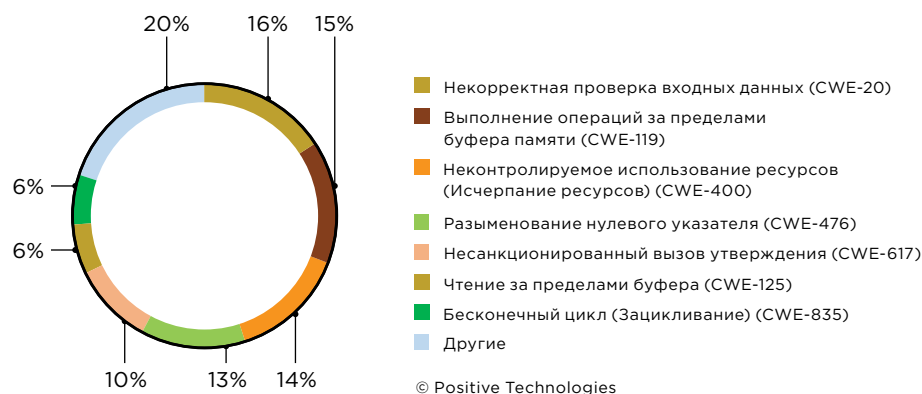


Рисунок 13. Выявленные ошибки в ПО, способные вызвать отказ в обслуживании

Повышение привилегий

На сетевом периметре 53% организаций выявлены уязвимости в ПО, позволяющие злоумышленнику, получившему доступ к узлу с правами обычного пользователя, повысить свои привилегии. Более чем для трети из них существуют общедоступные эксплойты. Например, если на узле используется OpenSSH версии ниже 7.4, злоумышленник, подобравший учетные данные, сможет с помощью готового эксплойта для уязвимости [CVE-2016-10010](#) повысить привилегии до максимальных. Максимальные привилегии позволяют редактировать и удалять любую информацию на узле, следовательно, возникает риск отказа в обслуживании, а для веб-серверов — еще и возможность дефейса, несанкционированного доступа к базе данных, проведения атак на клиентов. Кроме того, у злоумышленника появляется возможность развивать атаку на другие узлы. К примеру, привилегии пользователя root позволяют просматривать хеш-суммы паролей других пользователей из файла `/etc/shadow`. Если пароли удастся восстановить, взломщик может использовать их для попыток подключения к другим сервисам.

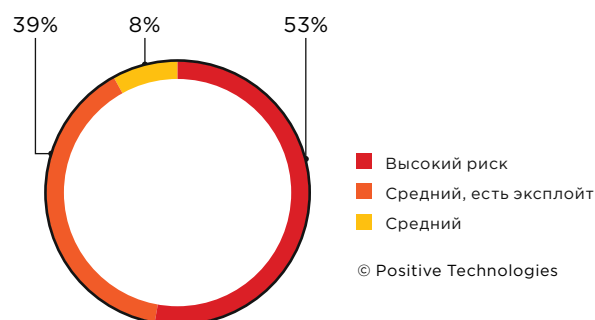


Рисунок 14. Распределение уязвимостей, связанных с повышением привилегий, по уровню риска

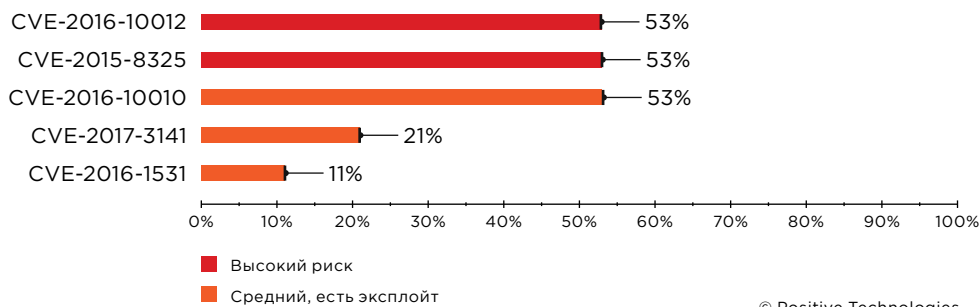


Рисунок 15. Топ-5 наиболее опасных уязвимостей, связанных с повышением привилегий (доля организаций)

Разглашение информации

Во всех организациях выявлены узлы, на которых раскрывается та или иная техническая информация: содержимое конфигурационных файлов, маршруты к сканируемому узлу, версии ОС или поддерживаемые версии протоколов. Чем больше подобной информации об атакуемой системе удастся собрать злоумышленнику, тем выше его шанс на успех. Причина кроется в небезопасной конфигурации служб. Так, в 92% организаций, где на сетевом периметре доступна служба NTP, не настроено игнорирование информационных пакетов, в результате чего путем запроса переменных NTP можно выяснить версию операционной системы, версию программного обеспечения NTP, тип процессора и параметры времени. В 58% организаций возможно подключение к узлам по протоколу SNMP. Обычно SNMP используют для мониторинга параметров сетевых устройств, но, на наш взгляд, этот интерфейс может представлять угрозу для безопасности периметра. В двух организациях для SNMP Community String выявлено значение public с правами только на чтение. Это означает, что злоумышленник, используя утилиту snmpwalk, сможет получить расширенную информацию о системе и в дальнейшем использовать ее для развития атаки.

Наиболее популярные уязвимости, которые могут привести к разглашению конфиденциальной информации ([CVE-2016-2183](#), [CVE-2014-3566](#), [CVE-2013-2566](#)), связаны с поддержкой устаревших версий протокола SSL/TLS. Ряд уязвимостей связаны с использованием недостаточно стойких криптографических алгоритмов и слабых ключей. В SSL-сертификатах 68% организаций выявлено использование хеш-функций SHA-1 и MD5. В настоящее время хорошо известны атаки, направленные на поиск коллизий в этих алгоритмах, что позволяет злоумышленнику скомпрометировать сертификат. В 53% организаций в сертификатах используются RSA-ключи длиной 1024 бита или меньше. В SSL/TLS использование слабого секретного ключа RSA означает для злоумышленника возможность перехватить сессию, выдав свой сервер за легитимный. Рекомендуемая NIST длина RSA-ключа должна составлять не менее 2048 бит.

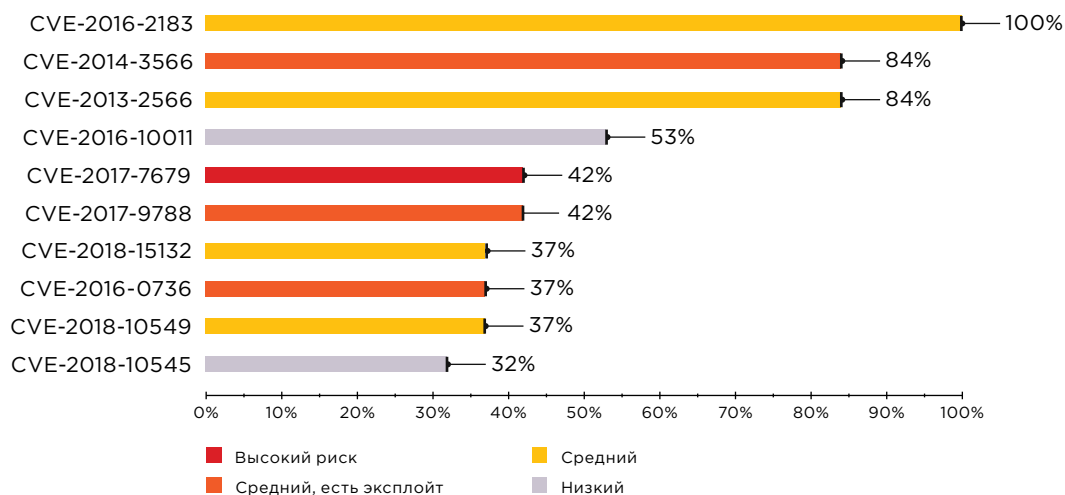


Рисунок 16. Распространенные уязвимости в ПО, связанные с разглашением информации (доля организаций)

Выводы и рекомендации

Сетевые периметры большинства корпоративных информационных систем остаются крайне уязвимыми для атак со стороны внешнего злоумышленника. Результаты инструментального анализа защищенности свидетельствуют, что на периметре всех организаций доступны для подключения разнообразные сетевые сервисы; это дает возможность любому интернет-пользователю проводить подбор учетных данных к этим сервисам и эксплуатировать уязвимости в ПО. Как показали итоги внешних тестов на проникновение, выполненных нашими специалистами в 2019 году, вектор атаки для успешного преодоления периметра включал в себя подбор паролей в 61% случаев.

По состоянию на 2020 год до сих пор остаются организации, уязвимые для Heartbleed и WannaCry. Наиболее часто встречающиеся в ходе инструментального анализа уязвимости датируются 2013–2017 годами, что говорит об отсутствии актуальных обновлений ПО. Мы рекомендуем ограничить количество сервисов на сетевом периметре и убедиться в том, что открытые для подключения интерфейсы действительно должны быть доступны из интернета. Если это так, необходимо обеспечить безопасную их конфигурацию и наличие установленных обновлений, закрывающих известные уязвимости.

Порой это сделать непросто. Ежегодно в базах данных уязвимостей появляется информация о тысячах новых брешей, а в IT-инфраструктуре организаций неминуемо происходят изменения, каждое из которых сопряжено с потенциальным риском для безопасности. Это делает управление уязвимостями ИБ довольно сложной задачей, при решении которой специалистам невозможно обойтись без инструментальных средств. Современные средства анализа защищенности позволяют не только автоматизировать инвентаризацию ресурсов и поиск уязвимостей, но и оценить соответствие инфраструктуры политикам безопасности.

Однако каждую найденную в ходе инструментального сканирования уязвимость необходимо верифицировать, и любая подтвержденная брешь представляет угрозу, поскольку невозможно предугадать, какой именно вектор атаки из множества возможных выберет злоумышленник. С этой точки зрения сканирование дает лишь общее представление о состоянии защищенности

организации. Для получения более полной картины необходимо сочетание инструментального анализа и тестов на проникновение.

Таким образом, инструментальное сканирование сетевых ресурсов — только первый шаг на пути к приемлемому уровню защищенности организации, за которым обязательно должны следовать верификация, приоритизация, устранение рисков и причин их возникновения. Этот процесс должен быть цикличным, а его регулярность позволяет минимизировать риск успешных атак на корпоративную инфраструктуру.

Режимы сканирования MaxPatrol 8

В системе контроля защищенности и соответствия стандартам MaxPatrol 8 предусмотрено три режима сканирования — PenTest, Audit и Compliance.

В режиме **PenTest** проводятся проверки, типичные для сканера сетевого уровня: инвентаризационные, «баннерные» проверки (анализ сообщений, которые передают приложения), фаззинг, подбор учетных записей. Также в MaxPatrol 8 есть специализированные проверки для анализа защищенности веб-приложений и СУБД. Данный режим предполагает минимальные знания об исследуемой системе (метод черного ящика).

В режиме **Audit** возможны инвентаризация аппаратного и программного обеспечения, сбор конфигурационных параметров ОС, служб, СУБД, прикладных систем и средств защиты информации, выявление уязвимостей, ошибок конфигурации и контроль обновлений. В этом режиме используются возможности, доступные внутреннему нарушителю, который имеет доступ к сканируемым узлам.

Режим **Compliance** позволяет проверять выполнение требований российских регулирующих органов, международных и отраслевых стандартов, корпоративных регламентов. В этом режиме проводятся как проверки, реализованные в режиме Audit, включающие идентификацию программного обеспечения узла, так и дополнительные проверки, необходимые для принятия решения о соответствии сканируемого объекта тем или иным требованиям.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](#).