SOLAR

ОТЧЕТ

КЛЮЧЕВЫЕ УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ РОССИЙСКИХ КОМПАНИЙ

W: RT-SOLAR.RU

МОСКВА 2024

СОДЕРЖАНИЕ

ОБ ОТЧЕТЕ

Настоящий отчет содержит результаты аналитических исследований, основанных на статистических данных, полученных в ходе проектов по анализу защищенности и тестированию на проникновение, проведенных экспертами отдела анализа защищенности центра противодействия кибератакам Solar JSOC в 2023 году.

В рамках отчета проанализированы результаты более 100 проектов. Приведены сведения о распространенных уязвимостях, угрозах и векторах проникновения в корпоративные сети. За услугами по анализу защищенности и тестированию на проникновение обращались компании из различных городов России. Отраслевая принадлежность исследованных компаний также разнообразна: телекоммуникации, информационные технологии, маркетинг, энергетика, торговля и т. д.

МЕТОДОЛОГИЯ

При исследовании обнаруженных уязвимостей использовались результаты:

- работ по внешнему и внутреннему тестированию на проникновение;
- проектов по анализу защищенности веб- и мобильных приложений.

В статистике распространенности уязвимостей внешних и внутренних периметров корпоративных сетей учитывались только уязвимости и недостатки, отмеченные высокой степенью критичности. При этом из нескольких выявленных в одном проекте уязвимостей одинакового типа в статистику попала только одна.

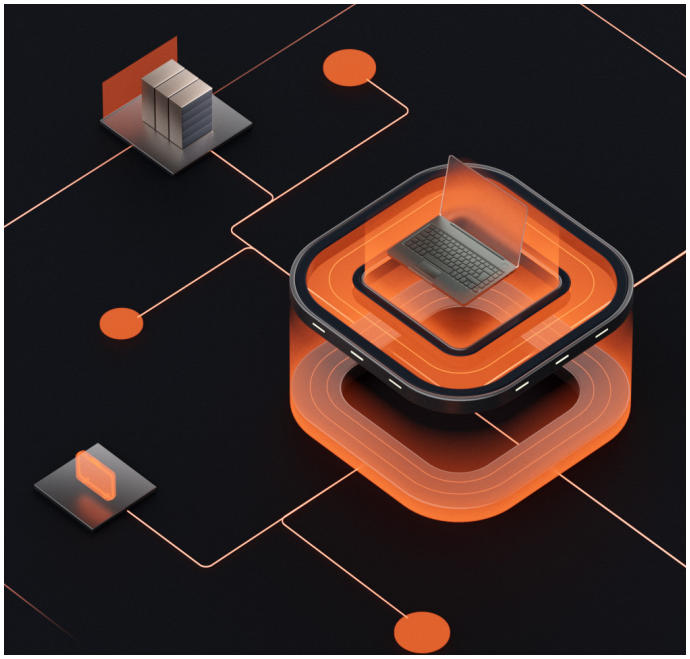
В проектах по анализу защищенности мобильных и веб-приложений каждый тип распространенной уязвимости учитывался только один раз. То есть из нескольких одинаковых уязвимостей в статистику попала только одна – с наибольшей критичностью и наименьшей сложностью эксплуатации. Здесь основными критериями оценки уязвимости были:

- возможность и последствия эксплуатации;
- ее местонахождение;
- роль уязвимой функциональности или системы;
- необходимость особых условий для эксплуатации.

Такой выбор критериев обусловлен тем, что разработчикам свойственно допускать однотипные ошибки в различных местах. При сборе статистики учитывалось количество проектов с определенным типом уязвимости, а не общее количество уязвимостей конкретного типа.

В свою очередь, при сравнительном анализе сложности и условий эксплуатации уязвимостей веб-приложений учитывались все обнаруженные уязвимости в каждом из реализованных проектов.

В проектах по тестированию на проникновение анализировались успешно реализованные векторы атак, которые позволили достигнуть поставленных целей (получить контроль над доменом, доступ во внутреннюю сеть извне и т. п.). Длина вектора отражает количество атак или действий, которые были совершены до достижения цели.



КЛЮЧЕВЫЕ ВЫВОДЫ

70%

В 70% проектов по внутреннему тестированию на проникновение были достигнуты поставленные цели. Использование слабых паролей и уязвимая конфигурация центра сертификации – наиболее распространенные проблемы внутренней инфраструктуры.

01

Самые распространенные недостатки веб-приложений связаны с некорректным контролем доступа (отмечалось в 75% приложений). Также не теряют актуальности риски, сопряженные с раскрытием отладочной и конфигурационной информации (73%), в содержимом которой встречаются такие чувствительные данные, как логины, пароли и cookie пользователей, JWT-секреты, настройки используемых СУБД и прочие сведения, позволяющие злоумышленнику повысить привилегии в приложении, получить доступ к критичным данным и реализовать прочие угрозы информационной безопасности.

02

Преодолеть внешний периметр удалось в 88% исследованных компаний. При этом в 41% случаев был получен доступ во внутреннюю сеть, в 18% случаев – скомпрометированы различные узлы внешнего периметра, а в 29% проектов – получен доступ к критичным данным, внешним системам и приложениям. В 50% проектов начальной точкой проникновения хотя бы в одном выявленном векторе послужила эксплуатация уязвимостей, связанных с использованием слабых паролей.

03

Самыми актуальными проблемами серверной части мобильных приложений оказались недостатки контроля доступа и раскрытие отладочной и конфигурационной информации. Каждый из этих недостатков обнаружился в 60% приложений. В клиентской части самыми распространенными оказались недостатки, связанные с небезопасным хранением данных на устройстве (в 47% приложений).

ВНЕШНЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Внешнее тестирование на проникновение направлено на поиск уязвимостей и недостатков с высоким уровнем критичности, эксплуатация которых может привести к получению доступа во внутреннюю сеть организации или к критичным внешним системам.

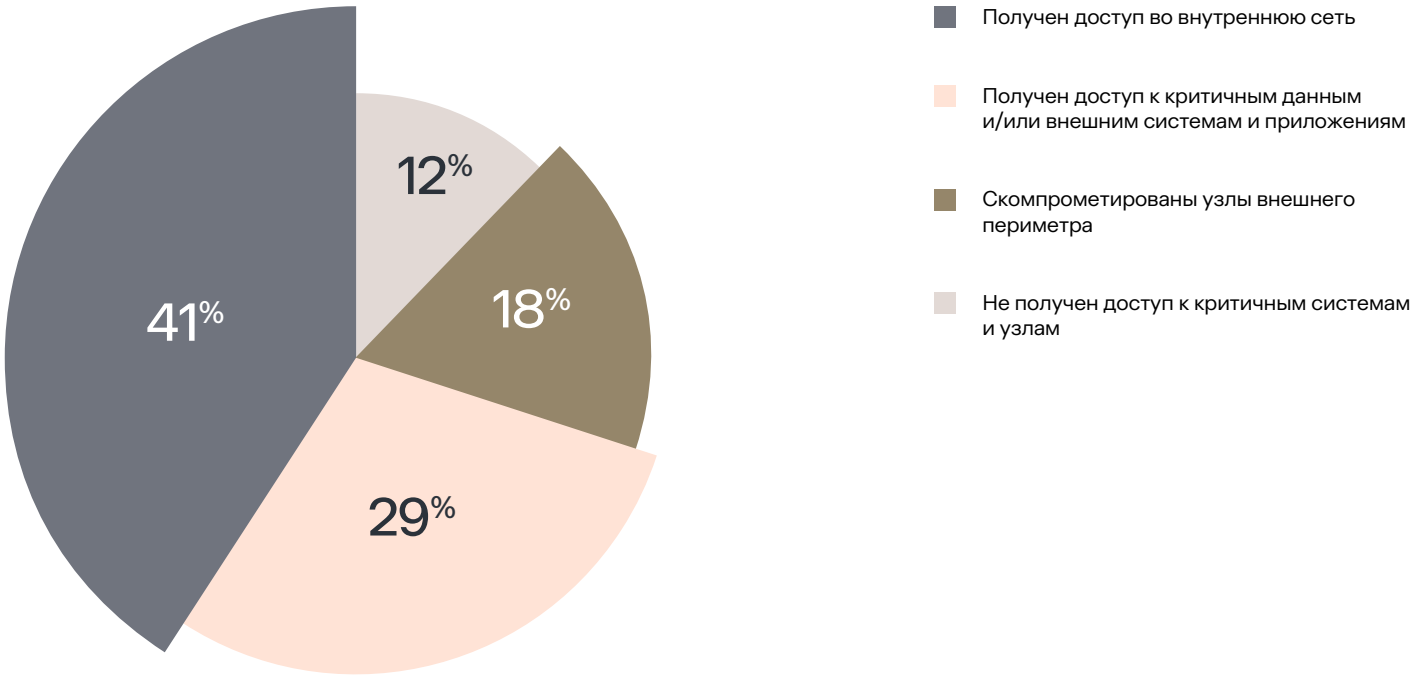
При проведении работ моделируются действия потенциального внешнего нарушителя, не обладающего сведениями об инфраструктуре. Подобный подход позволяет получить независимую оценку эффективности методов и средств защиты информации в компании.

РЕЗУЛЬТАТЫ РАБОТ

В 88% проектов специалисты отдела анализа защищенности Solar JSOC успешно преодолели внешний периметр, при этом в 41% случаев был получен доступ во внутреннюю сеть, а в 18% – скомпрометированы различные узлы внешнего периметра. Еще в 29% проектов удалось получить доступ к критичным данным и внешним системам и приложениям.

Стоит отметить, что существенный ущерб компании может нанести не только проникновение злоумышленника во внутреннюю сеть, но и компрометация узлов внешнего периметра, не имеющих прямой связанности с внутренней сетью организации (например, находящихся в сети DMZ – сегменте, где расположены сетевые устройства, взаимодействующие с внешними сетями).

Результаты внешнего пентеста



Это открывает возможности для проведения дальнейших атак и получения различных чувствительных данных. Например, в ходе одного из проектов успешная компрометация таких узлов позволила получить доступ к информации о пользователях, а именно к списку пользователей и хешам паролей.

Кроме того, даже при отсутствии уязвимостей и недостатков, позволяющих получить доступ во внутреннюю сеть или скомпрометировать узлы внешнего периметра, в системе могут присутствовать уязвимости высокой степени критичности, приводящие к раскрытию значимой информации.

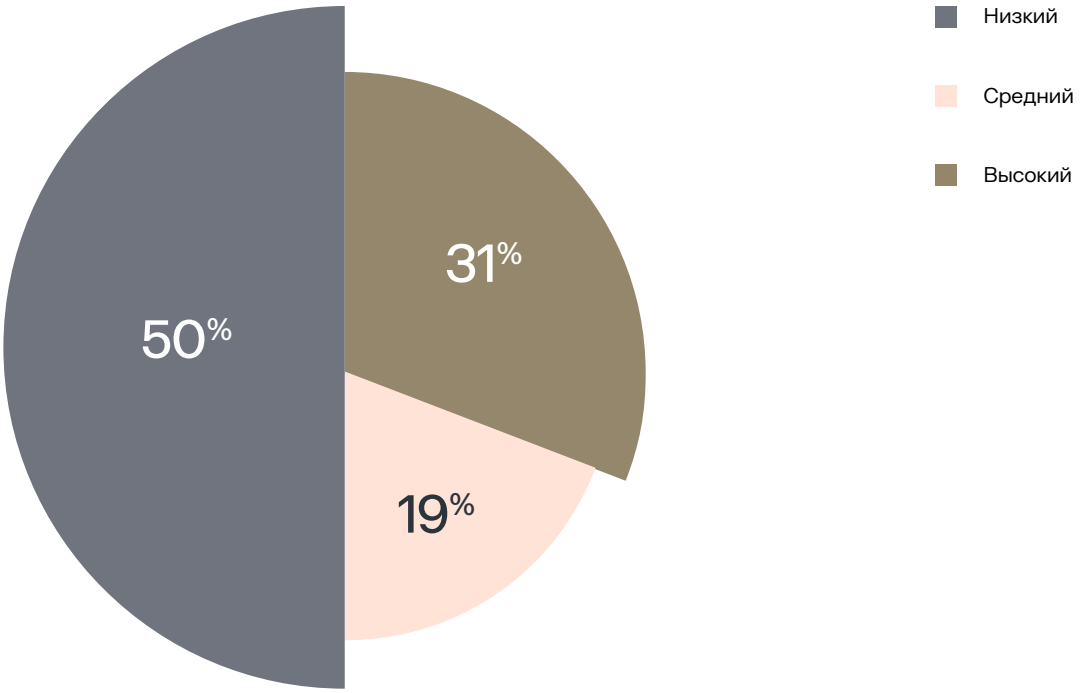
Приведем пример: в одном из проектов получить доступ во внутреннюю сеть или скомпрометировать узлы внешнего периметра не представилось возможным.

Тем не менее эксперты Solar JSOC обнаружили недостатки контроля доступа, позволившие получить персональные данные пользователей.

Уровень защищенности внешнего периметра был оценен как низкий в 50% исследованных компаний, то есть в каждой второй организации злоумышленник легко может проникнуть во внутреннюю сеть.

При этом в некоторых проектах, где удалось преодолеть внешний периметр, уровень защищенности мог быть оценен как средний или высокий в связи с высокой сложностью реализации вектора атаки (например, начальной точкой вектора являлась атака подбора пароля, которая продолжалась длительное время).

Уровень защищенности исследованных внешних периметров



Важную роль при оценке уровня защищенности играет наличие активных средств защиты информации (СЗИ). Так, в ходе одного из проектов исследование проводилось в двух форматах: при включенных и при отключенных средствах межсетевого экранирования. Сначала IP-адреса специалистов ГК «Солар» добавили в белые списки СЗИ заказчика, затем их исключили.

При добавлении IP-адресов в белые списки специалистам удалось успешно скомпрометировать несколько узлов внешнего периметра, а также осуществить эксплуатацию уязвимостей, позволяющих получить чувствительные данные, повысить привилегии в приложениях на внешнем периметре и реализовать прочие угрозы. В рассматриваемой ситуации уровень защищенности корпоративной сети был оценен как низкий.

В то же время при исключении IP-адресов из белых списков возможность эксплуатации имеющихся уязвимостей и компрометации узлов внешнего периметра была ограничена. Однако СЗИ не ограничивали доступ к части уязвимых систем и сервисов, в связи с чем уровень защищенности корпоративной сети в данной ситуации был оценен как средний.

Вот почему важно помнить, что включенные СЗИ не устраняют имеющиеся уязвимости и недостатки. При внесении заказчиком изменений в настройки средств защиты своих ресурсов потенциальный злоумышленник может получить доступ к уязвимым элементам и осуществить их эксплуатацию.

В нескольких проектах провести тестирование на проникновение не удалось, так как на внешнем периметре отсутствовало достаточное количество доступных для анализа сервисов. Такие проекты в исследовании не учитывались.

ВЕКТОРЫ ПРЕОДОЛЕНИЯ ВНЕШНЕГО ПЕРИМЕТРА

В исследовании учитывались все обнаруженные в каждом из проектов векторы, в результате которых был успешно получен доступ во внутреннюю сеть или скомпрометированы узлы внешнего периметра.

В среднем в проектах, в которых был успешно получен доступ во внутреннюю сеть или скомпрометированы узлы внешнего периметра, было продемонстрировано 2 вектора проникновения, что свидетельствует о наличии более одного способа преодоления внешнего периметра. Максимальное количество векторов в одном проекте за отчетный период доходило до 4.

Минимальный вектор состоял из 1 шага, то есть реальному злоумышленнику достаточно было бы выполнить всего одно действие для компрометации узла сети. Среди всех успешно реализованных за отчетный период векторов внешний периметр был преодолен за 1 шаг в 30% случаев. Одним из примеров подобного вектора является эксплуатация известных уязвимостей в используемом ПО, в результате которой потенциальный злоумышленник может успешно загрузить веб-интерпретатор командной строки и выполнить произвольный код на сервере.

Кроме того, проведенные за отчетный период работы показали, что в 85% случаев злоумышленнику для преодоления внешнего периметра достаточно выполнить не более 4 шагов.

2

Среднее количество успешных векторов в одном проекте

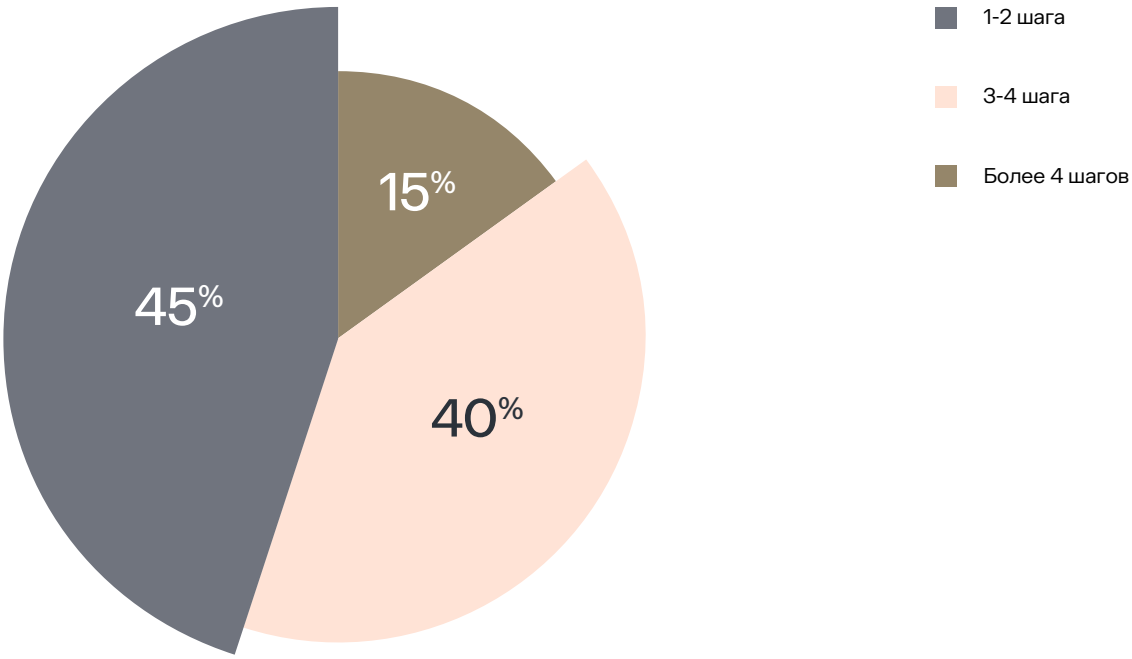
3

Среднее количество шагов в одном векторе

1

Минимальное количество шагов в векторе проникновения

Длина векторов, позволивших успешно преодолеть внешний периметр



РАСПРОСТРАНЕННЫЕ КРИТИЧЕСКИЕ УЯЗВИМОСТИ ВНЕШНИХ ПЕРИМЕТРОВ

Внешнее тестирование на проникновение направлено на поиск уязвимостей с высоким уровнем критичности, поскольку именно они чаще всего позволяют получить доступ к ресурсам компаний.

На протяжении нескольких лет первенство сохраняет использование слабых паролей, однако с каждым годом процент проектов с указанным недостатком сокращается. Слабые пароли были обнаружены в 78% компаний в 2021 году и в 59% – в 2022 году. Тем не менее именно эксплуатация этой уязвимости послужила начальной точкой проникновения хотя бы в одном векторе в половине реализованных проектов.

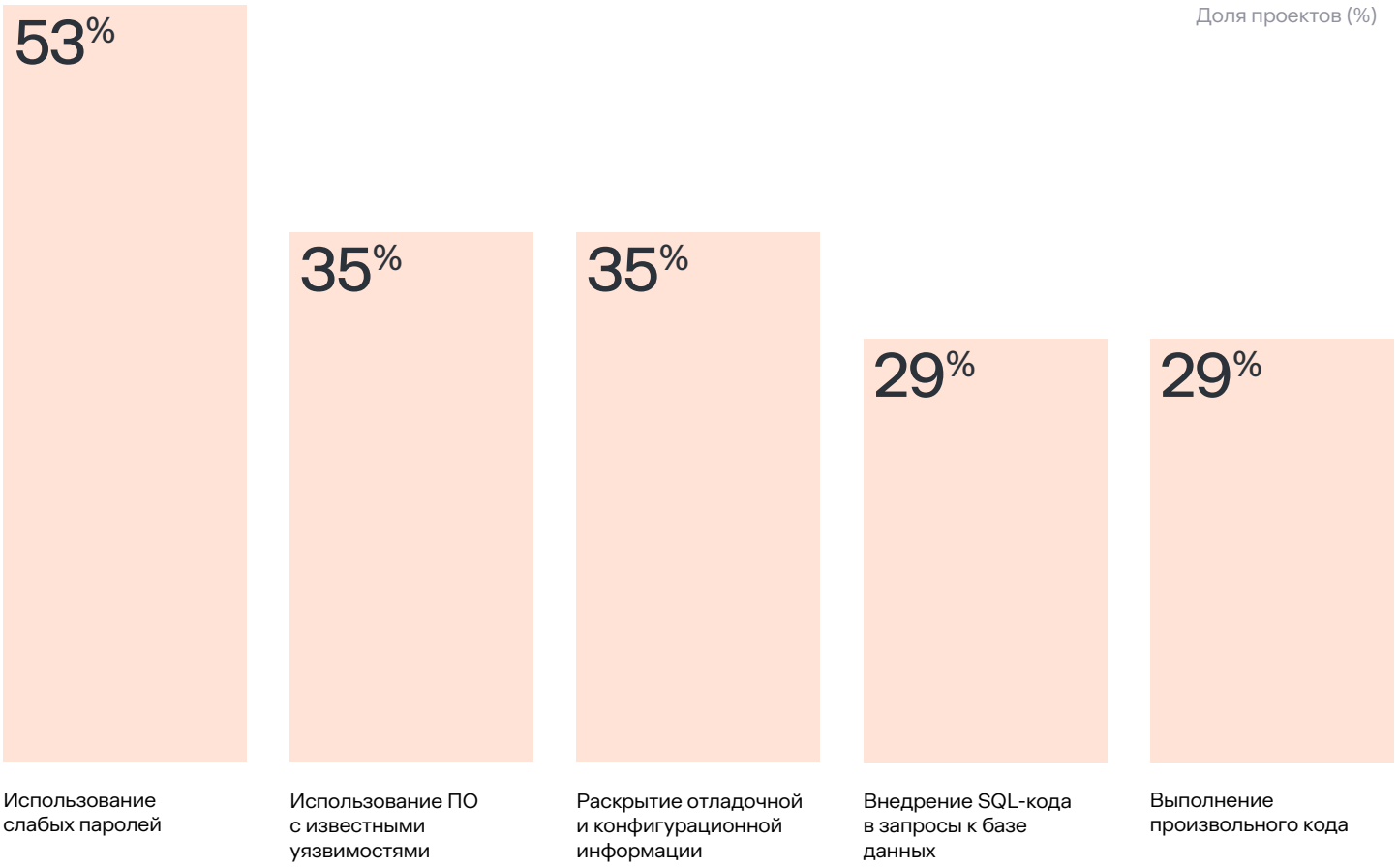
Таким образом, самым распространенным источником рисков информационной безопасности в последние несколько лет остается человеческий фактор. Поэтому не теряет актуальности обучение сотрудников компаний навыкам ИБ, а также необходимость внедрения строгой парольной политики.

Значительная часть векторов успешного преодоления внешнего периметра также была связана с эксплуатацией известных уязвимостей, которым подвержено используемое на внешних узлах ПО. Например, актуальными остаются уязвимости в системе Bitrix, послужившие начальной точкой проникновения в 30% проектов.

Практика показывает, что компании все чаще обращаются за услугами анализа защищенности на долгосрочной основе (годовые контракты, периодические работы, регулярные автоматизированные сканирования и прочие услуги).

Отвечая на потребности рынка, в начале 2024 года «Солар» запустил сервис Solar CPT (Continuous Penetration Testing), который предоставляет услуги постоянного контроля защищенности внешнего ИТ-периметра.

Топ-5 критических уязвимостей внешних периметров



С одной стороны, такой подход к ИБ демонстрирует заинтересованность бизнеса в защите своих информационных активов. С другой – при проведении периодических работ эксперты часто обнаруживают уязвимости и недостатки, выявленные ранее. То есть компании не всегда следуют приведенным в отчетах рекомендациям и не устраняют обнаруженные уязвимости.

Например, в одном из проектов обнаруженные в ходе предыдущих работ учетные данные позволили успешно получить авторизованный доступ к одному из узлов внешнего периметра и реализовать атаку «Внедрение шаблонов в серверной части приложения (SSTI)», что привело к возможности выполнения произвольного кода на этом узле.

Наличие не устраненных длительное время уязвимостей значительно увеличивает риски информационной безопасности. В этой связи необходимо обратить внимание на важность следования рекомендациям по устранению уязвимостей, которые приводятся в отчете по результатам работ.

ВНУТРЕННЕЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Внутреннее тестирование на проникновение направлено на проверку возможности повышения привилегий во внутренней инфраструктуре, получения доступа к критичной информации или системам.

За отчетный период специалисты отдела анализа защищенности Solar JSOC проводили как отдельные работы по внутреннему тестированию на проникновение, так и работы в качестве продолжения внешнего пентеста. В первом случае доступ был предоставлен заказчиком, во втором – получен в результате преодоления внешнего периметра.

РЕЗУЛЬТАТЫ РАБОТ

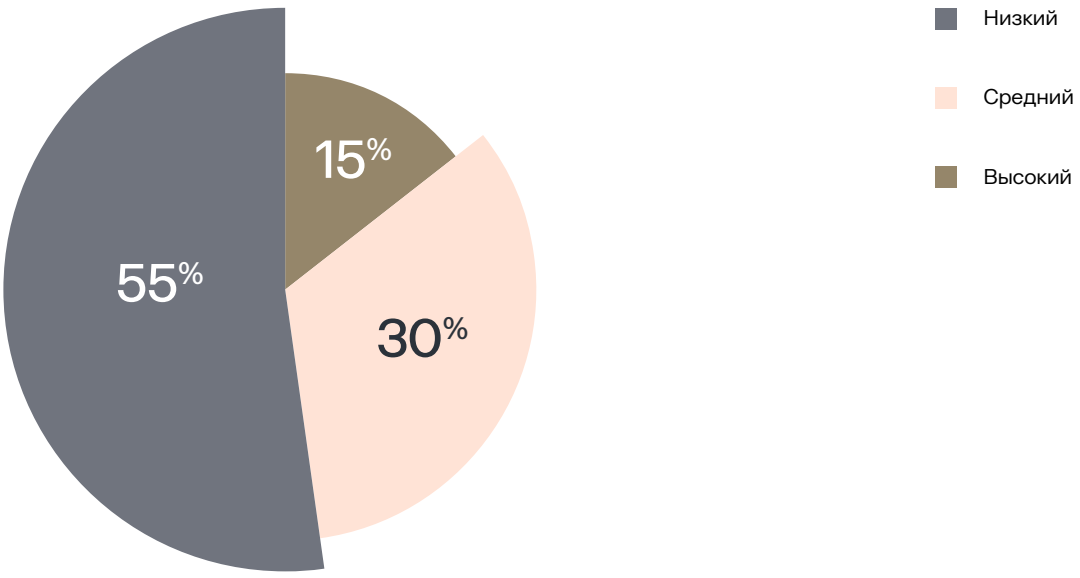
Основной целью работ в большинстве проектов являлось получение контроля над доменом. При этом нередки случаи, когда заказчиками ставились дополнительные цели – например, получение доступа к различным базам данных, к сегментам АСУ ТП и системам 1С. Подобный подход говорит о том, что компании уделяют все больше внимания защите своих информационных активов во внутренней сети.

Поставленные цели были успешно достигнуты в 70% выполненных проектов.

При этом 55% исследованных инфраструктур были отмечены низким уровнем защищенности. То есть более чем в половине компаний злоумышленник может легко повысить привилегии или получить доступ к различным критичным системам и данным во внутренней сети.

В некоторых проектах даже в случае успешного достижения цели уровень был оценен как средний в связи с высокой сложностью реализации вектора атаки.

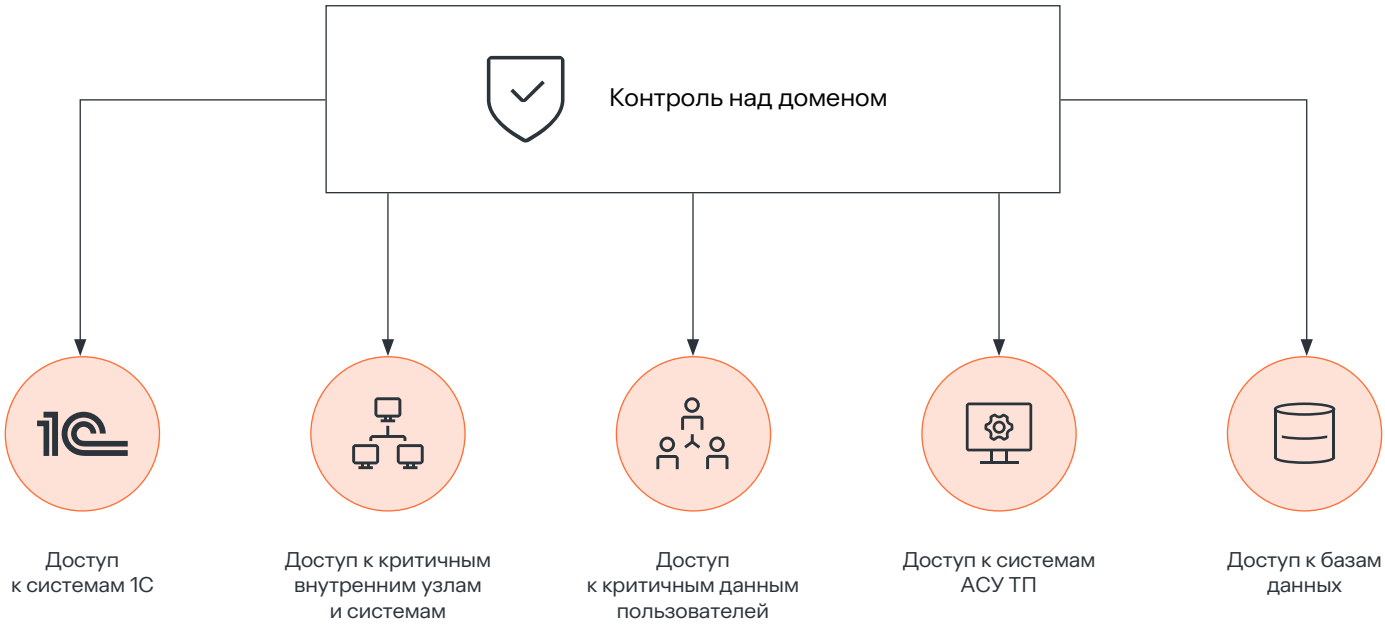
Уровень защищенности исследованных внутренних сетей



ВЕКТОРЫ ПОВЫШЕНИЯ ПРИВИЛЕГИЙ

В исследовании учитывались все обнаруженные векторы, в результате которых был успешно получен контроль над доменом, так как именно это являлось не только основной целью в 90% проектов, но и было необходимо для реализации дополнительных целей.

Контроль над доменом открывает возможность дальнейшего продвижения во внутренней сети, результатом которого может стать получение доступа к различным критичным данным и системам:



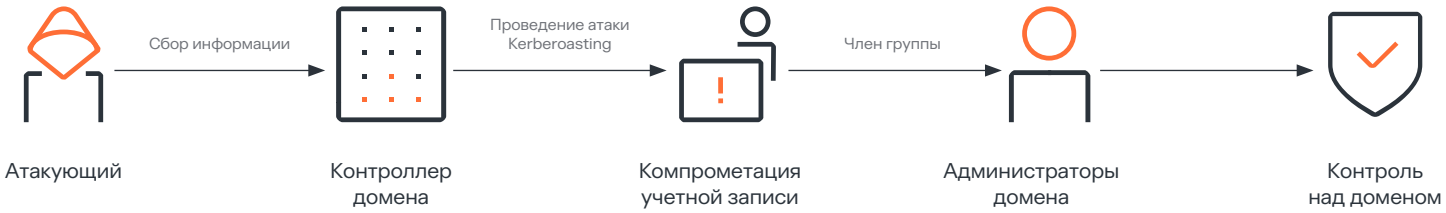
Однако важно понимать, что контроль над доменом не является обязательным для выполнения поставленных целей и задач, так как в системе могут присутствовать критичные уязвимости и недостатки, сами по себе представляющие угрозу для компании.

Например, в одном из проектов обнаруженные уязвимости и недостатки позволили получить доступ к ряду внутренних узлов с правами локального администратора, а также к различным чувствительным данным из внутренних систем. При этом права доменного администратора для реализации указанных угроз не понадобились. Полученная информация, в свою очередь, может быть использована злоумышленником для проведения дальнейших атак на внутреннюю инфраструктуру.

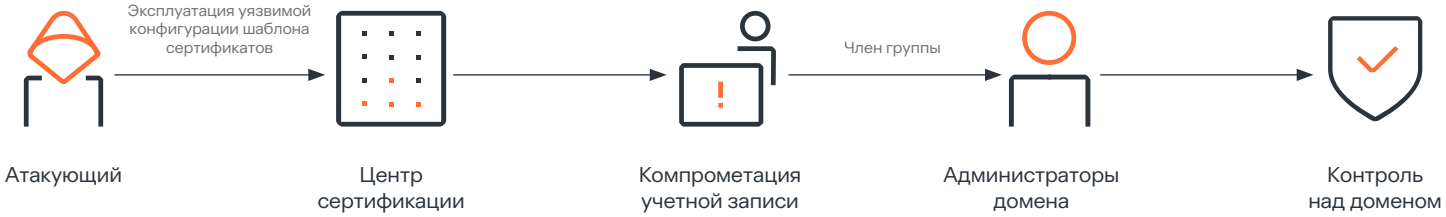
Аналитическое исследование показало, что в 68% случаев для получения привилегий администратора домена необходимо выполнить не более 4 шагов. В среднем именно 4 шага отделяют злоумышленника от получения полного контроля над доменом.

Наибольшее количество обнаруженных векторов было связано с использованием слабых и повторяющихся паролей, а также с эксплуатацией уязвимой конфигурации шаблонов сертификатов. Так, использование слабых и повторяющихся паролей послужило начальной точкой в 21% векторов. Аналогичное количество успешных векторов было начато с эксплуатации уязвимой конфигурации шаблонов сертификатов.

Пример вектора атаки с использованием слабых паролей:



Пример вектора атаки с использованием уязвимой конфигурации шаблона сертификатов:



РАСПРОСТРАНЕННЫЕ КРИТИЧЕСКИЕ УЯЗВИМОСТИ ВНУТРЕННИХ СЕТЕЙ

Начальной точкой любого вектора повышения привилегий и получения доступа к различным системам и данным во внутренней сети выступают критичные уязвимости и недостатки.

Из года в год не сдает своих позиций использование слабых и повторяющихся паролей, то есть человеческий фактор остается самым уязвимым не только для внешнего периметра, но при атаках во внутренних сетях. Пользователи по-прежнему устанавливают пароли по умолчанию, простые и словарные пароли. В частности, в проектах встречались пароли, совпадающие с названием организации и с именем учетной записи.

Также во внутренней сети часто отмечались недостатки, связанные с уязвимой конфигурацией центра сертификации. Подобный недостаток может позволить злоумышленнику успешно повысить привилегии в домене и получить доступ к критичным данным.

Например, обнаруженная в одном из проектов некорректная настройка центра сертификации предоставляла возможность указывать произвольное альтернативное имя субъекта для всех сертификатов, несмотря на конфигурацию шаблона сертификата. Указанный недостаток позволил выпустить сертификат для администратора домена, а затем использовать его для получения TGT-билета привилегированной учетной записи и компрометации домена.

Топ-5 критических уязвимостей внутренних сетей

Кроме того, в каждом пятом проекте было обнаружено использование программного обеспечения с известными уязвимостями. Примеры таких уязвимостей:

- MS17-010
- CVE-2021-21972
- CVE-2021-21974
- CVE-2022-35914
- CVE-2019-0708

Наличие подобных уязвимостей позволяет злоумышленнику выполнять произвольный код на узлах внутренней сети, в том числе с повышенными привилегиями, что, в свою очередь, может быть использовано для проведения дальнейших атак и реализации различных киберугроз.

Среди всех обнаруженных уязвимостей во всех выполненных за отчетный период проектах доля уязвимостей высокой степени критичности составила 60%. При этом хотя бы одна подобная уязвимость была обнаружена в 95% проектов.

Вместе с тем 83% критических уязвимостей было отмечено низкой сложностью. То есть для их эксплуатации хакеру не нужны какие-либо дополнительные условия. Это значительно упрощает реализацию векторов повышения привилегий и получения доступа к различным системам и данным во внутренней сети.

АНАЛИЗ ЗАЩИЩЕННОСТИ ВЕБ-ПРИЛОЖЕНИЙ

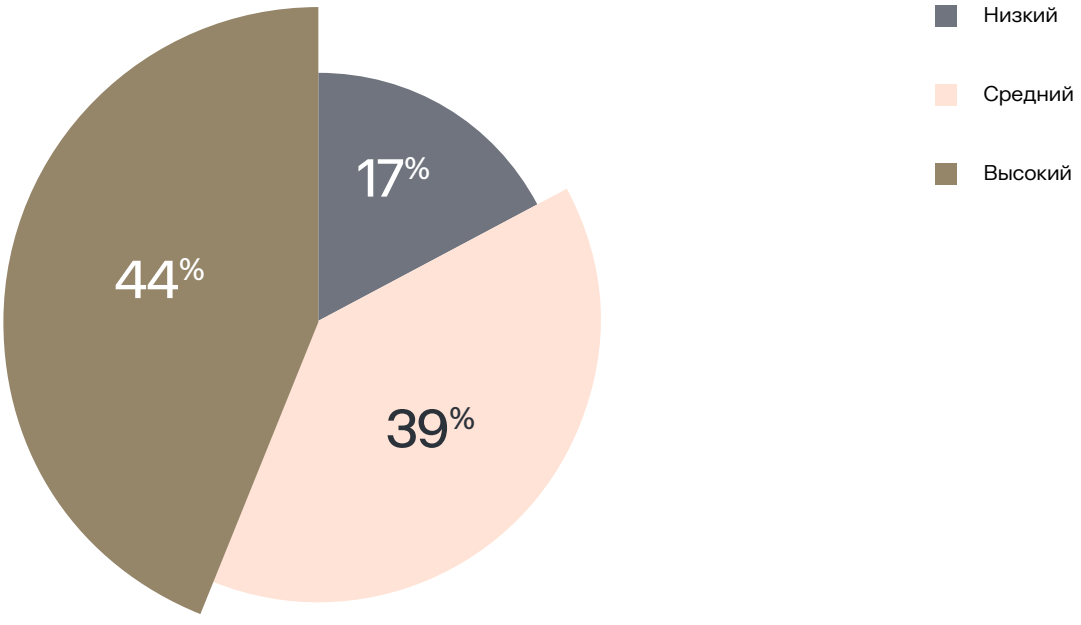
Работы по анализу защищенности веб-приложений направлены на поиск максимального количества уязвимостей и недостатков, демонстрацию возможностей их эксплуатации, а также оценку уровня защищенности и последствий успешной эксплуатации обнаруженных уязвимостей.

РЕЗУЛЬТАТЫ РАБОТ

Низкий уровень защищенности исследователи отметили в 17% приложений, средний – в 39%. То есть больше половины приложений имеют уязвимости высокой или средней степени критичности, успешная эксплуатация которых позволяет злоумышленнику нанести существенный ущерб информационным активам компании.

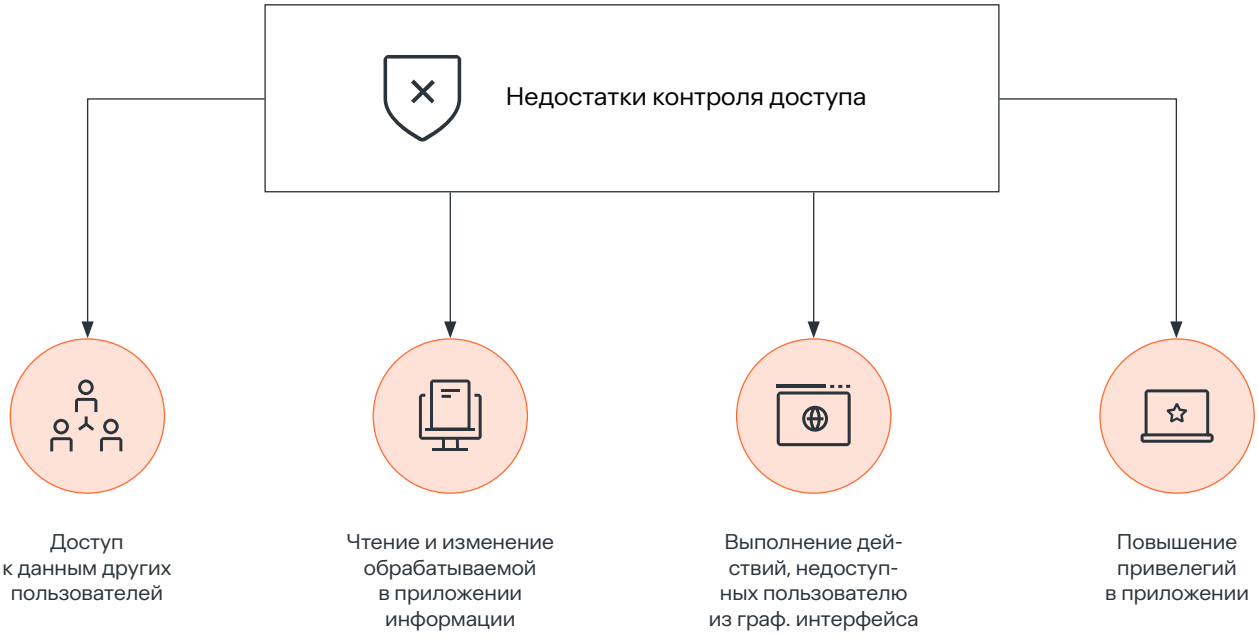
При этом в 54% исследованных приложений была обнаружена хотя бы одна критичная уязвимость.

Уровень защищенности веб-приложений



УЯЗВИМОСТИ

Самой распространенной проблемой веб-приложений на протяжении последних нескольких лет остаются недостатки контроля доступа, которые были обнаружены в 70% проектов, выполненных в 2021 году, и в 86% проектов 2022-го года. За минувший год указанные недостатки были выявлены в 75% исследованных приложений, при этом в 29% проектов они были отмечены высокой степенью критичности. Успешная эксплуатация недостатков контроля доступа может позволить злоумышленнику получить доступ к данным пользователей, повысить привилегии в приложении и реализовать прочие угрозы информационной безопасности:



Еще одной проблемой веб-приложений, не теряющей актуальности последние несколько лет, остается раскрытие отладочной и конфигурационной информации. Так, в 73% исследованных приложений были обнаружены уязвимости и недостатки, позволяющие получить различные данные о структуре, компонентах и работе приложения. В 10% случаев они имели высокую степень критичности.

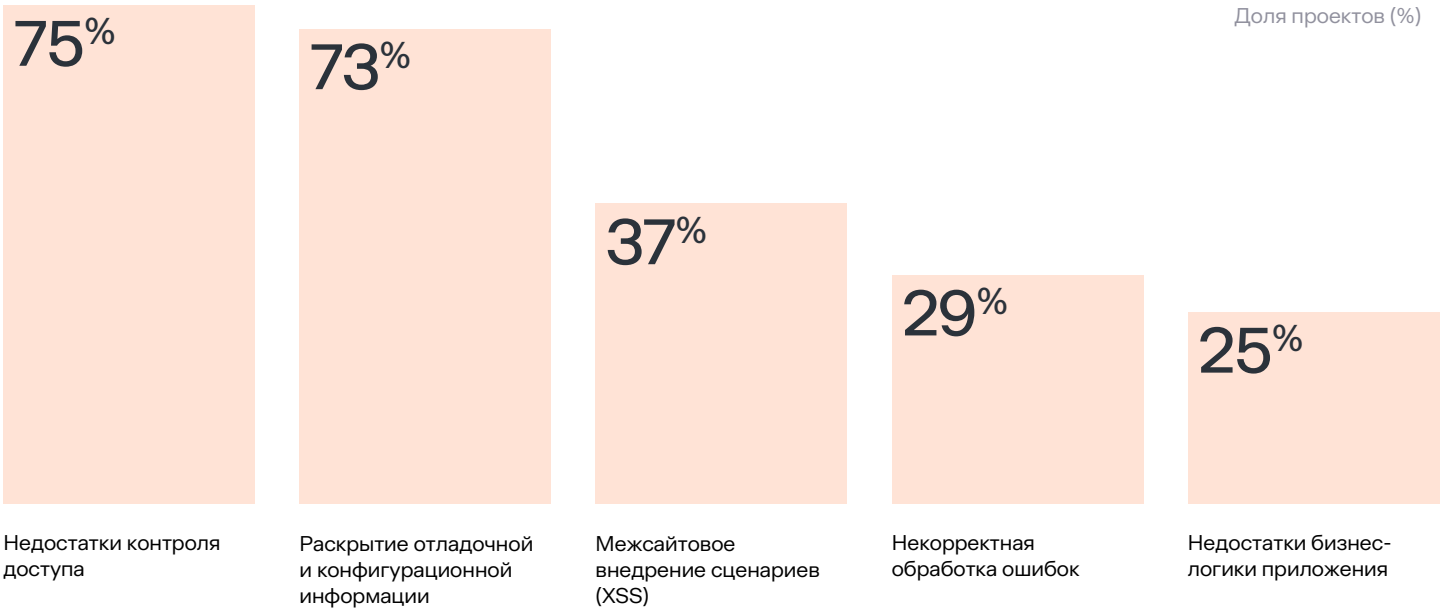
Среди доступных сведений оказались логины, пароли и cookie пользователей, настройки используемых СУБД, внутренние IP-адреса и прочие чувствительные данные. Владение подобной информацией позволяет злоумышленнику упростить поиск известных уязвимостей и подготовиться к последующим атакам.

Например, в ходе одного из проектов в конфигурационном файле был обнаружен валидный JWT-секрет, с помощью которого был сгенерирован JWT-токен, позволивший получить доступ к различным чувствительным данным от имени привилегированного пользователя admin.

Распространенными также остаются уязвимости, предоставляющие возможность проведения атаки «Межсайтовое внедрение сценариев (XSS)» (обнаружены в 37% приложений). При ее успешной эксплуатации злоумышленник сможет, например, менять содержимое отображаемой страницы и выполнять действия от имени пользователей приложения.

Важно понимать, что эксплуатация уязвимостей веб-приложений может также стать начальной точкой вектора преодоления внешнего периметра и получения доступа во внутреннюю сеть. В этой связи особенно актуальным становится проведение периодических работ по анализу защищенности веб-приложений компании, а также следование рекомендациям по устранению уязвимостей, которые приводятся в отчете по итогам работ.

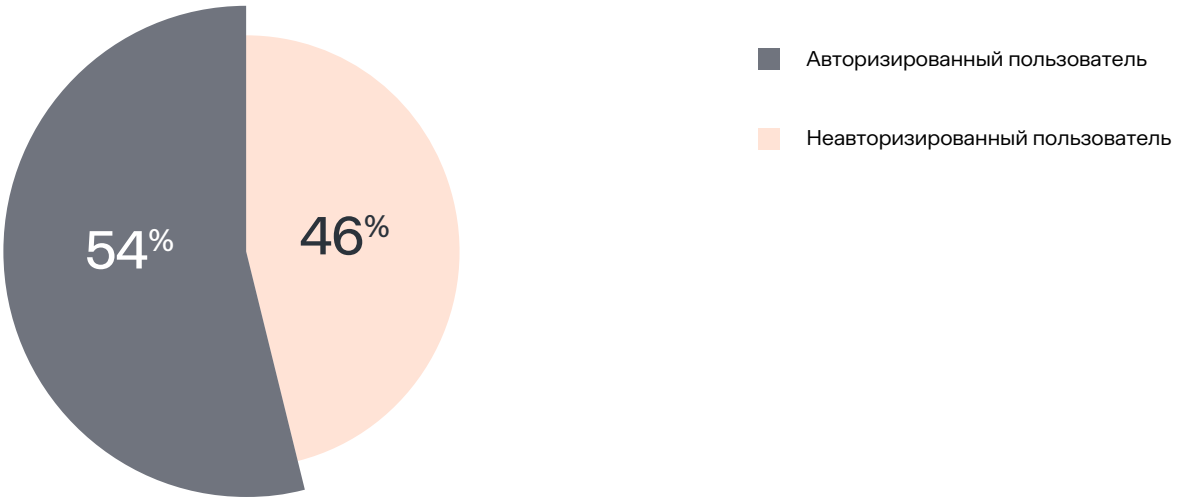
Топ-5 критических уязвимостей веб-приложений



При проведении работ по анализу защищенности веб-приложений оценивается не только критичность обнаруженных уязвимостей, но и сложность их эксплуатации. Сложность считается высокой, если для успешной эксплуатации уязвимости необходимы дополнительные условия, которые не зависят от злоумышленника (например, действия пользователя, определенное состояние или конфигурация системы и т. п.).

Только 13% уязвимостей веб-приложений, найденных исследователями, обладали высокой сложностью. Остальные 87% – низкой. То есть для их успешной эксплуатации не требуется выполнение никаких дополнительных условий. Кроме того, исследование показало, что для успешной эксплуатации 46% выявленных уязвимостей не требуется даже авторизованный доступ к приложению. Иными словами, успешная эксплуатации таких уязвимостей возможна без каких-либо привилегий.

Условия эксплуатации уязвимостей веб-приложений



АНАЛИЗ ЗАЩИЩЕННОСТИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

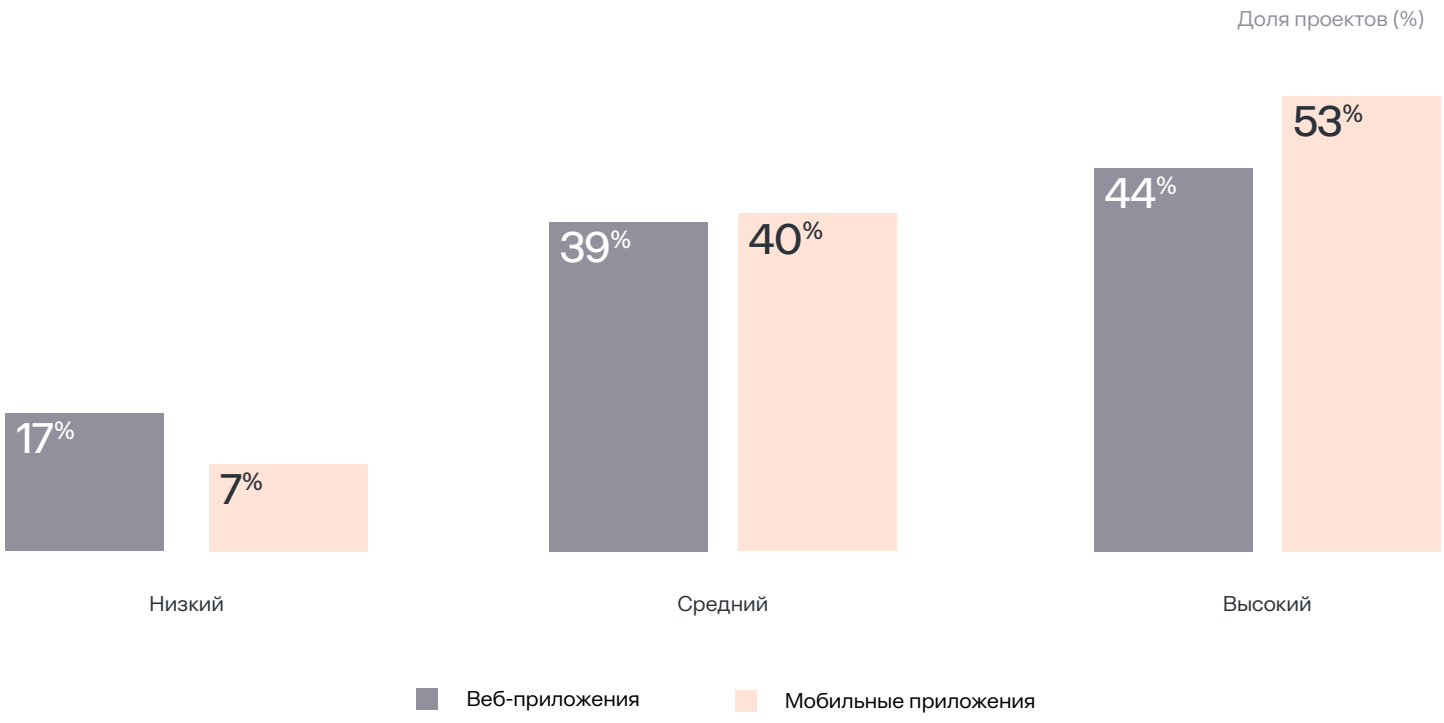
Анализ защищенности мобильных приложений направлен на поиск максимального числа уязвимостей, демонстрацию возможностей их эксплуатации и оценку общего уровня защищенности. В ходе каждого проекта проводится проверка приложений для двух операционных систем: iOS и Android.

РЕЗУЛЬТАТЫ РАБОТ

В минувшем году только 7% исследованных мобильных приложений было отмечено низким уровнем защищенности, что более чем в два раза меньше отмеченных аналогичным уровнем защищенности веб-приложений. Это позволяет сделать вывод о том, что мобильные приложения защищены лучше и менее подвержены критичным уязвимостям.

Но несмотря на положительную динамику, в мобильных приложениях по-прежнему присутствуют уязвимости и недостатки высокой и средней степени критичности, снижающие уровень защищенности и грозящие нанести ущерб компании.

Сравнительный анализ уровней защищенности мобильных и веб-приложений



Наиболее уязвимой оказалась серверная часть приложений, в которой было обнаружено 77% всех уязвимостей. Именно в серверной части приложений было выявлено 94% критичных уязвимостей. При этом три четверти всех обнаруженных в этой части уязвимостей были отмечены низкой сложностью эксплуатации.

Остальные 23% уязвимостей пришлись на клиентскую часть. Такое распределение обусловлено тем, что эксплуатация недостатков фронтенда затруднительна, так как в большинстве случаев требует физического или удаленного доступа к устройству. Таким образом, компаниям следует обратить особое внимание на защиту серверной части своих приложений.

УЯЗВИМОСТИ

Аналитическое исследование наиболее распространенных уязвимостей мобильных приложений продемонстрировало схожие с предыдущим годом результаты.

Подобная тенденция говорит о том, что при разработке мобильных приложений из года в год допускаются похожие ошибки.

Самые распространенные уязвимости серверной части мобильных приложений

Недостатки контроля доступа (60%)

Некорректная реализация прав доступа остается одной из самых актуальных проблем как для веб-приложений, так и для серверной части мобильных приложений. Недобросовестный контроль прав доступа позволяет пользователю совершать действия вне установленных для него привилегий, что может быть использовано злоумышленником для компрометации чувствительных данных или получения дополнительных возможностей для атаки.

Например, в одном из проектов подобные недостатки позволили получить доступ к отчетам, содержащим персональные данные пользователей, сведения о финансовых показателях компании и прочую чувствительную информацию.

Раскрытие отладочной и конфигурационной информации (60%)

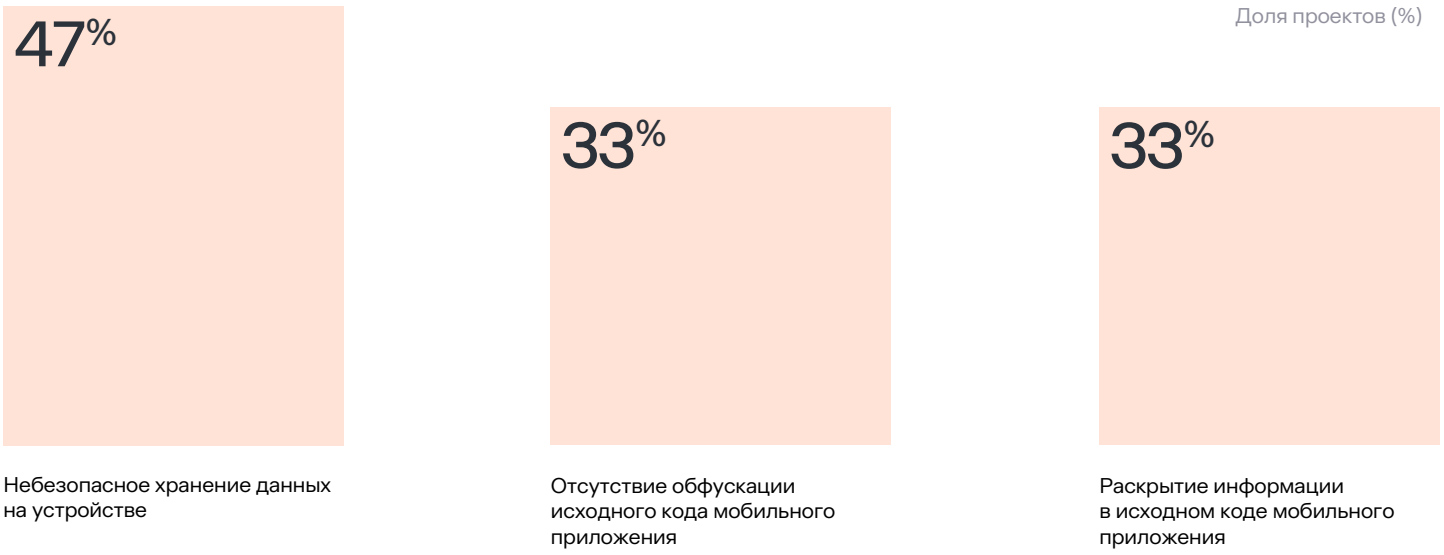
Отладочная и конфигурационная информация содержит сведения о текущих настройках, окружении и отдельных компонентах приложения, например данные о внутренних и тестовых адресах. Ее раскрытие упрощает хакерам процесс исследования приложения и подготовки дальнейших атак.

Недостатки бизнес-логики приложения (53%)

Недостатки бизнес-логики позволяют пользователю взаимодействовать с приложением по непредусмотренному разработчиками сценарию. Таким образом, злоумышленник может повысить привилегии в приложении, обойти установленные требования, получить доступ к чувствительной информации.

Эта уязвимость может даже привести к прямым финансовым потерям. Так, в мобильном приложении одного интернет-магазина специалисты «Солара» обнаружили недостатки бизнес-логики, позволяющие заблокировать доступ к заказу определенных товаров, что, в свою очередь, могло нанести финансовый ущерб продавцу.

Самые распространенные уязвимости в клиентской части мобильных приложений



Небезопасное хранение данных на устройстве (47%)

Почти в половине мобильных приложений чувствительные данные пользователей сохраняются в журналах, незашифрованных базах данных или других файлах непосредственно на устройствах. Например, при проведении работ были обнаружены токены доступа, информация об учетных записях и прочие значимые данные. При этом после выхода пользователя из приложения и аккаунта данные с устройств не удалялись.

Отсутствие обфускации исходного кода мобильного приложения (33%)

Если при сборке приложения не применяется обфускация, то после декомпиляции полученный код будет близок к оригинальному исходному коду. А наличие корректного исходного кода приложения позволяет злоумышленнику получить дополнительные сведения о его структуре и взаимодействии с серверной частью, а также упростить поиск уязвимостей и внедрение различных закладок.

Раскрытие информации в исходном коде мобильного приложения (33%)

В исходных кодах клиентской части приложений были обнаружены сведения о тестовых доменах, токены, позволяющие получить информацию о доступной в мобильном приложении функциональности, и прочие данные, которые не были удалены перед выводом приложения в продуктивное использование. Несмотря на то что исходный код не направляется пользователям в открытом виде, содержащаяся в нем информация становится доступна после распаковки и декомпиляции приложения.

РЕКОМЕНДАЦИИ

В очередной раз считаем необходимым подчеркнуть, что своевременное обнаружение и закрытие уязвимостей позволяет не только обезопасить инфраструктуру компании, но и защитить клиентов и пользователей от действий потенциальных злоумышленников.

Для повышения общего уровня кибербезопасности рекомендуется проводить:

Анализ защищенности веб- и мобильных приложений перед их выводом в продуктивное использование. Это позволит избежать появления критичных уязвимостей на внешнем или внутреннем периметре в связи с внедрением новых решений. А компаниям-разработчикам проверка приложений по окончании разработки позволит заранее устранять уязвимости и предоставлять своим клиентам только безопасные продукты.

Регулярные внешние и внутренние тестирования на проникновение – при этом внутреннее тестирование на проникновение не менее важно, чем внешнее. Стоит помнить, что цель внешнего пентеста – это выявление способов преодоления внешнего периметра, а внутреннего – возможностей развития атаки внутри сети. Только комплексный подход способен обеспечить высокий уровень защищенности от внешних и внутренних злоумышленников.

Постоянный контроль защищенности меняющегося внешнего ИТ-периметра инфраструктуры (Continuous Penetration Testing, CPT), благодаря чему компания может регулярно актуализировать картину своих ИТ-активов и лучше защищать инфраструктуру от ключевых угроз.

Регулярное автоматизированное сканирование, которое позволяет с минимальными затратами выявлять известные уязвимости и недостатки систем (в том числе из базы CVE), отслеживать безопасность используемых компонентов и появление в них новых уязвимостей. Эти задачи решает сервис контроля уязвимостей (Vulnerability Management, VM).

SOLAR

W: RT-SOLAR.RU
W: RT.RU

T +7 (499) 755-07-70
E solar@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1