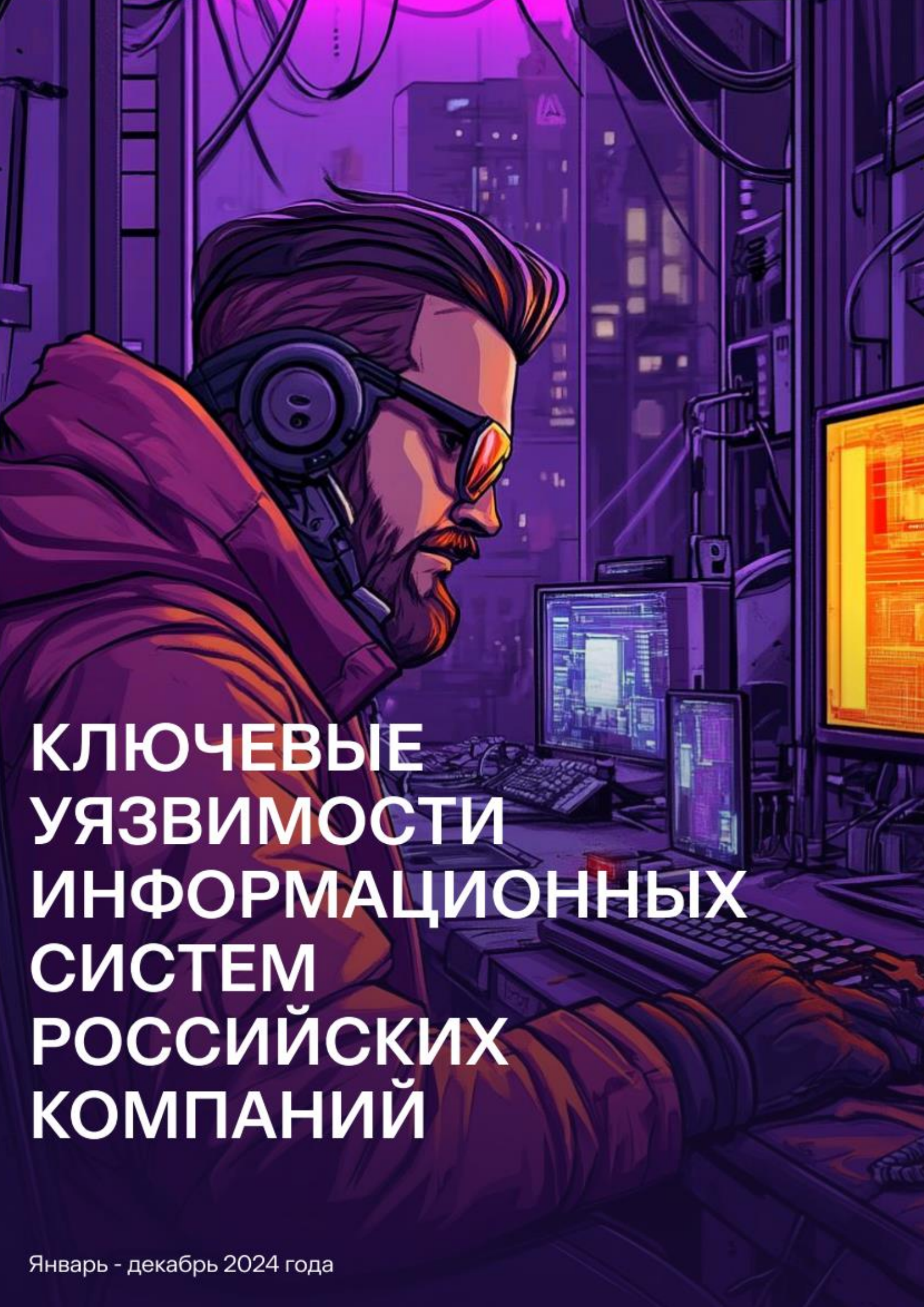


КЛЮЧЕВЫЕ УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ РОССИЙСКИХ КОМПАНИЙ

Январь - декабрь 2024 года

Об отчете

Настоящий отчет содержит статистические данные, полученные из результатов проектов по анализу защищенности и тестированию на проникновение, проведенных экспертами отдела анализа защищенности центра противодействия кибератакам Solar JSOC ГК «Солар» с января по декабрь 2024 года.

В отчете приведены сведения о распространенных уязвимостях, угрозах и векторах проникновения в корпоративные сети. Представленная аналитика базируется на результатах более 200 проектов. За услугами по анализу защищенности и тестированию на проникновение обращались компании из различных городов России. Отраслевая принадлежность исследованных компаний также разнообразна: государственный сектор, производство, информационные и телекоммуникационные технологии, финансы, медиа и т.д.

Методология

При исследовании обнаруженных уязвимостей использовались:

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

Тестирование на проникновение (англ. penetration test, сокр. пентест) – вид тестирования, при котором проводится моделирование атак злоумышленника на организацию, с целью получения той или иной выгоды. Тестирование может быть направлено на внешний или внутренний периметр организации.

При анализе распространенных критичных уязвимостей внешней и внутренней инфраструктуры учитывались только уязвимости и недостатки, отмеченные высокой степенью критичности. При этом из нескольких выявленных в одном проекте критичных уязвимостей одинакового типа в статистику попадала только одна.

В проектах по тестированию на проникновение анализировались успешно реализованные векторы атак, которые позволили достигнуть поставленные цели (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.

В проектах по анализу защищенности мобильных и веб-приложений при аналитическом исследовании распространенных уязвимостей каждый тип 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;
- местонахождение;
- роль уязвимой функциональности или системы;
- необходимость особых условий для эксплуатации.

Такой выбор критериев обусловлен тем, что разработчикам свойственно допускать однотипные ошибки. При составлении 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 приложений учитывались все обнаруженные уязвимости в каждом из реализованных проектов.

Стоит отметить, что при составлении выборок для проведения аналитического исследования по каждому из типов работ не учитывались проекты, в ходе которых действия специалистов значительно ограничивались, например, путем блокировки попыток использования автоматизированных инструментов исследования и эксплуатации уязвимостей. Также в выборки не были включены проекты, в которых

перечень предоставленных ресурсов был недостаточен для проведения работ, например, в случаях, когда на внешнем периметре отсутствовало достаточное количество сервисов, доступных для проведения анализа.

Подобные условия искажают результаты работ и не позволяют дать объективную оценку уровня защищенности внешнего периметра, внутренней сети, веб- или мобильного приложения.

Ключевые выводы

- Внешний периметр **91%** компаний оказался уязвим к атакам, успешная реализация которых может привести к проникновению во внутреннюю сеть, компрометации узлов внешнего периметра или получению доступа к чувствительным данным и/или критичным внешним системам и приложениям. Одними из самых распространенных проблем внешних периметров российских компаний остаются **слабые пароли** (**38%**) и **устаревшие версии программного обеспечения, подверженные различным уязвимостям** (**32%**).

- В **91%** проектов по внутреннему тестированию были достигнуты поставленные цели: получен контроль над доменом, получен доступ к критичным целевым системам и базам данных во внутренней сети. **Слабые пароли** (**57%**) **и использование программного обеспечения с известными уязвимостями** (**37%**) остаются самыми актуальными проблемами и для внутренних сетей.

- Более чем **в половине** веб-приложений имеются уязвимости и недостатки **высокой** и **средней** степени критичности, успешная эксплуатация которых может позволить злоумышленнику нанести существенный ущерб информационным активам и репутации компании.

- Самым распространенным недостатком веб-приложений оказалось **раскрытие отладочной и конфигурационной информации** (**70%**). В уязвимых веб-приложениях раскрываются учетные данные, ключи шифрования JWT токенов, фрагменты исходного кода, внутренние IP-адреса и прочие сведения, позволяющие злоумышленнику повысить привилегии, получить доступ к критичным данным и реализовать прочие угрозы информационной безопасности. В ряде проектов подобная информация предоставляла возможность эксплуатации других имеющихся в приложении уязвимостей. Распространенными остаются **недостатки контроля доступа** (**60%**), позволяющие скомпрометировать данные других пользователей и прочую чувствительную информацию, повысить привилегии и выполнить различные действия, недоступные из графического интерфейса.

- Самые распространенные недостатки серверной части мобильных приложений связаны с **раскрытием отладочной и конфигурационной информации** (**53%**) и **некорректной реализацией контроля доступа** (**40%**). А основной проблемой клиентской части в 2024 году стало отсутствие **обфускации исходного кода мобильного приложения** (**40%**).

Внешнее тестирование на проникновение

Внешнее тестирование на проникновение направлено на поиск уязвимостей и недостатков с высоким уровнем критичности, которые могут позволить определить и реализовать успешные векторы получения доступа во внутреннюю сеть или к критичным внешним системам компании. При проведении работ моделируются действия потенциального внешнего нарушителя, не обладающего данными об инфраструктуре. Подобный подход позволяет получить независимую оценку эффективности методов и средств защиты информации в компании.

Результаты работ

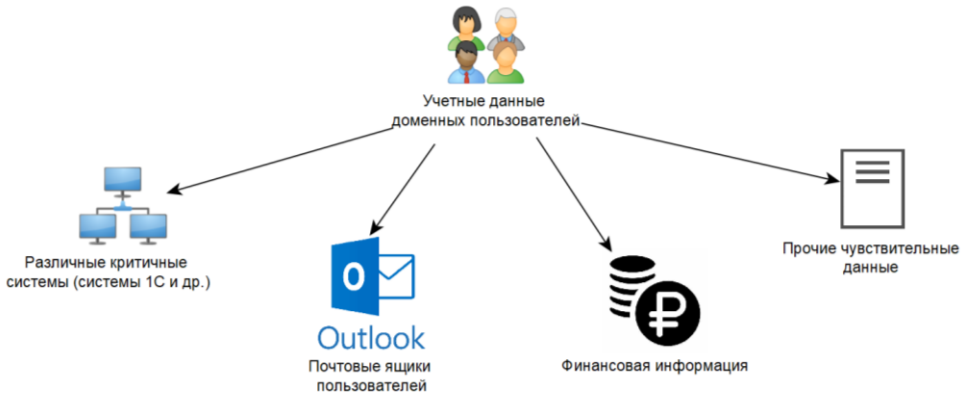
За минувший год нами было выполнено **около 50 проектов** по внешнему тестированию на проникновение.

Исследование результатов проведенных в 2024 году проектов по внешнему пентесту показало, что внешний периметр **91%** компаний уязвим к атакам, успешная реализация которых может привести к получению доступа во внутреннюю сеть, компрометации узлов внешнего периметра или получению доступа к чувствительным данным и/или критичным внешним системам и приложениям.

Существенный ущерб **информационным и финансовым активам**, а также **репутации компании** несет не только преодоление внешнего периметра, но и получение доступа к критичным внешним системам и приложениям и имеющимся в них чувствительным данным.

Например, в ходе одного из проектов в результате атаки Password Spraying (атака подбора пароля к учетным записям) были получены учетные данные доменного пользователя, позволившие выполнить выгрузку адресной книги и провести повторную атаку подбора пароля, которая привела к получению учетных данных более 80

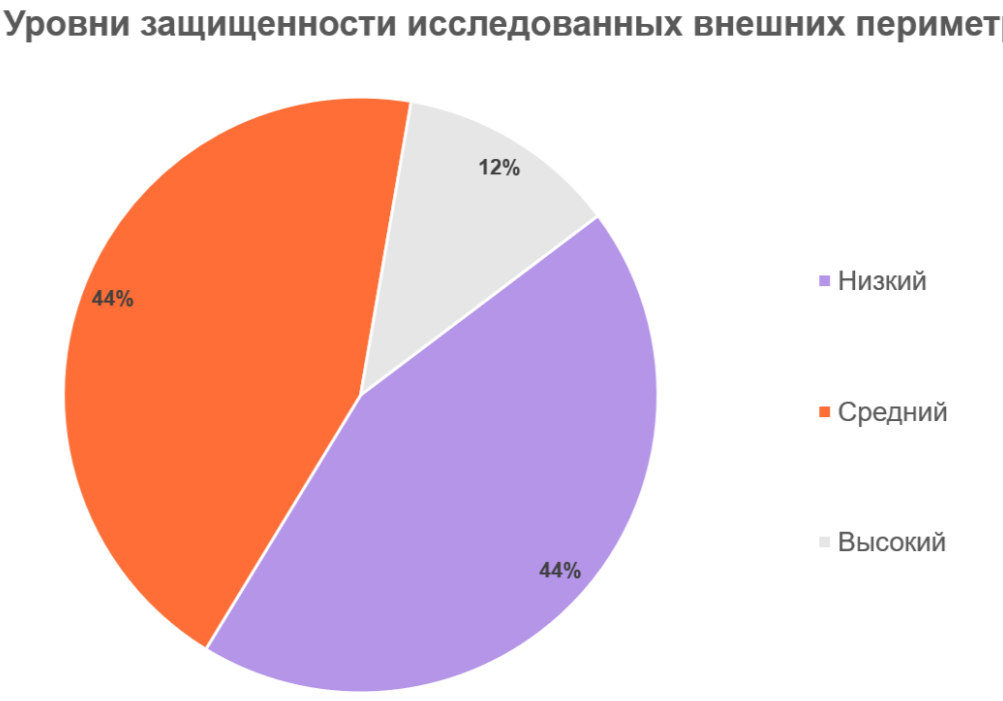
доменных пользователей. С их помощью в свою очередь удалось получить доступ к различным критичным системам (1С, внешняя система видеоконференцсвязи и др.) и чувствительным данным, например, к финансовой информации в содержимом почтовых ящиков сотрудников. **При этом преодоление внешнего периметра для получения указанных доступов не требовалось.**



Также не стоит забывать, что к **финансовым и репутационным потерям** для компании может привести не только получение доступа во внутреннюю сеть, но и эксплуатация имеющихся уязвимостей и недостатков, не требующих преодоления внешнего периметра. Например, в ходе одного из проектов было обнаружено приложение, с помощью которого пользователи могут записаться на получение предоставляемых компанией услуг. Подтверждение записи осуществлялось посредством проверки одноразового кода из SMS. При этом в приложении имелись недостатки бизнес-логики, позволяющие обойти проверку кода и записать на получение услуг пользователей без их ведома. Таким образом, компания получает неактуальные заявки на услуги и не может адекватно оценить загрузку специалистов, а также ограничивается возможность получения услуг реальными пользователями.

Для **трети** организаций, на внешнем периметре которых не было обнаружено уязвимостей и недостатков, позволяющих получить доступ во внутреннюю сеть или к критичным данным и внешним системам, ранее неоднократно проводились работы по внешнему и внутреннему пентесту. Регулярное проведение таких работ позволило своевременно выявить и устранить критичные уязвимости и недостатки и таким образом повысить уровень защищенности как внешнего периметра, так и внутренней сети.

В отчетном периоде всего у **12%** компаний уровень защищенности внешнего периметра были оценен как **высокий**. То есть почти в каждой **девятой** компании на внешнем периметре имелись уязвимости и недостатки высокой и средней степени критичности, позволяющие легко получить доступ во внутреннюю сеть или к критичным внешним системам и данным.



И даже у компаний, уровень защищенности которых был оценен как **высокий**, на внешнем периметре обнаруживались уязвимости и недостатки, позволяющие получить доступ к различным чувствительным данным, внешним системам и приложениям. Уровень защищенности в таком случае был оценен как высокий в связи с тем, что эксплуатация уязвимостей затруднительна и/или требует значительного количества времени.

Важно заметить, что отсутствие на внешнем периметре критичных уязвимостей и недостатков на момент проведения работ не гарантирует, что уровень защищенности не может снизиться в дальнейшем. Это связано с тем, что периметр организации не является статичным: появляются новые приложения и сервисы, которые могут быть подвержены уязвимостям и недостаткам. Причиной снижения уровня защищенности может стать, например, обнаружение уязвимостей нулевого дня в используемых приложениях, изменение конфигурации внешних систем и др.

Кроме того, результаты работ по проверке корректности устранения уязвимостей показывают, что зачастую обнаруженные в ходе тестирования уязвимости не устраняются. Поэтому для обеспечения безопасности информационных активов также немаловажно своевременное устранение выявленных уязвимостей и недостатков в соответствии с рекомендациями, приведенными в отчете по итогам работ.

Векторы преодоления внешнего периметра

В выборку для исследования вошли все обнаруженные в каждом из проектов векторы, результатом которых стало получение доступа во внутреннюю сеть или компрометация узлов внешнего периметра.

2

Среднее количество успешных векторов в одном проекте

8

Максимальное количество успешных векторов в одном проекте

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 проекте – **8**. При этом стоит отметить, что начальной точкой векторов в одном проекте могут служить разные уязвимости и недостатки, что в свою очередь открывает больше возможностей для подготовки и реализации атак, а также повышает вероятность успешного преодоления внешнего периметра.

Например, в одном из проектов начальной точкой 3-х векторов стала эксплуатация известных уязвимостей в устаревших версиях ПО, в 3-х – проблемы, связанные с использованием слабых паролей, и еще в 2-х – возможность проведения атак «Внедрение SQL-кода в запросы к базе данных».

1

Минимальное количество шагов в векторе проникновения

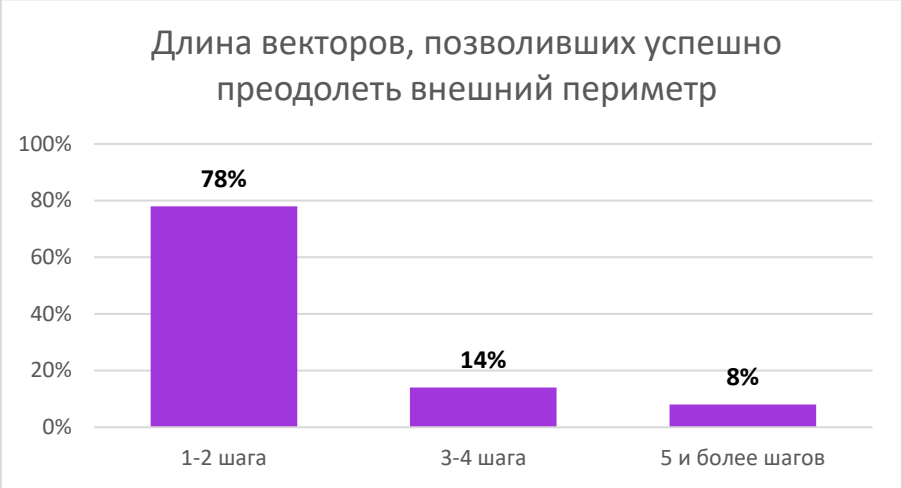
Минимальная длина успешного вектора составила **1 шаг**, т.е. для получения доступа во внутреннюю сеть или компрометации узла внешнего периметра злоумышленнику достаточно выполнить всего **одно действие**. При этом такие векторы составили **треть** от общего количества всех обнаруженных векторов.

2

Среднее количество шагов в векторе проникновения

В среднем для реализации успешного вектора получения доступа во внутреннюю сеть или компрометации узла внешнего периметра требуется **2 шага**. В **92%** случаев для реализации вектора требуется не более **4-х шагов**.

Шаг атаки – действие злоумышленника, являющееся частью вектора атаки и позволяющее получить необходимые для дальнейшего развития доступы, данные или привилегии. Пример шага атаки – проведение атаки подбора пароля, в результате которой были получены учетные данные, предоставившие привилегированный доступ к системе, функциональность которой позволяет реализовать загрузку исполняемого файла и выполнение произвольного кода.



Минимальное время определения и реализации вектора преодоления внешнего периметра составило **1 час**. В среднем на определение и реализацию успешного вектора требовалось от **1** до **8 дней**. При этом в **31%** случаев успешный вектор был определен и реализован за **1 день**, еще **22%** векторов – за **2-4 дня**. То есть более чем в половине случаев для успешного преодоления внешнего периметра требуется не более **4-х дней**.

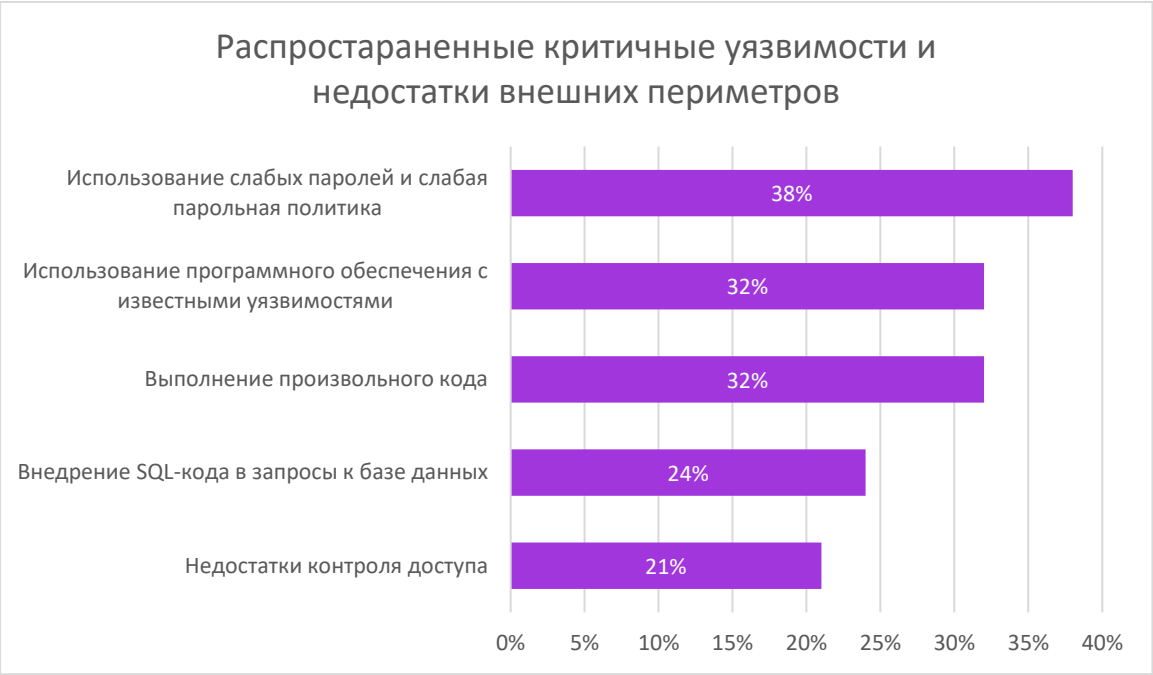
1 час

Минимальное время определения и реализации вектора проникновения

Распространенные критичные уязвимости внешних периметров

При проведении работ по внешнему тестированию на проникновение в первую очередь интерес представляют уязвимости и недостатки высокой степени критичности, так как именно они могут позволить определить и реализовать успешные векторы преодоления внешнего периметра. За минувший год на внешних периметрах компаний нам наиболее часто встречались следующие уязвимости и недостатки высокой степени критичности:

- использование слабых паролей и слабая парольная политика;
- выполнение произвольного кода;
- использование программного обеспечения с известными уязвимостями;
- внедрение SQL-кода в запросы к базе данных;
- недостатки контроля доступа.



Наиболее распространенными проблемами внешних периметров российских компаний остаются **слабые пароли** и **устаревшие версии программного обеспечения**, подверженные различным уязвимостям. По результатам наших исследований именно эти две категории возглавляют «Топ-5» критичных уязвимостей уже более трех лет.

При исследовании внешних периметров все также наблюдается использование **слабых паролей** и **паролей по умолчанию**, например, *password*, *user1*, *demo*, простых последовательностей чисел, пустых паролей в системе 1С и др.

Напомним, что использование простых паролей упрощает злоумышленникам подбор учетных данных, которые в дальнейшем могут позволить получить доступ к различным критичным системам. Доступ к подобным системам в свою очередь может позволить выполнить произвольный код на узлах внешнего периметра и получить доступ **во внутреннюю сеть**. Именно использование слабых паролей послужило начальной точкой успешного вектора в **19%** случаев.

Во многих компаниях по-прежнему **используется программное обеспечение с известными уязвимостями**. Среди встречавшегося на внешнем периметре уязвимого ПО, позволившего развить успешный вектор или получить доступ к чувствительным данным, было ПО *Liferay*, *1С-Битрикс*, *Pentaho*, *Cisco ExpressWay*, *CMS Битрикс*, *Microsoft Exchange*, *Avaya Aura*, *Jira* и др.

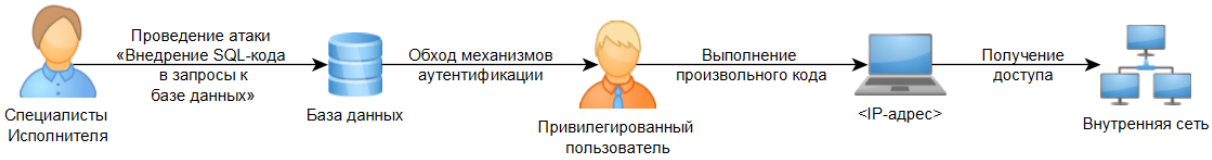
25%

векторов начинается с эксплуатации уязвимостей в устаревших версиях ПО

В обнаруженных устаревших версиях программного обеспечения встречались такие уязвимости, как *CVE-2020-7961*, *CVE-2022-27228*, *CVE-2019-5420*, *CVE-2022-43938* и др. Уязвимости в устаревших версиях программного обеспечения стали началом успешного вектора преодоления внешнего периметра в **25%** случаев.

Помимо прочего, почти **четверть** успешных векторов (**22%**) была начата с проведения атак «**Внедрение SQL-кода в запросы к базе данных**». Так, например, в ходе одного из проектов успешное проведение такой атаки позволило обойти механизмы аутентификации и получить доступ к уязвимому узлу от имени привилегированного пользователя. Полученный доступ позволил загрузить на сервер веб-интерпретатор командной строки и выполнить системные команды на узле, в результате чего был получен доступ во внутреннюю сеть.

Пример вектора с использованием атак внедрения SQL-кода:



Внутреннее тестирование на проникновение

Внутреннее тестирование на проникновение направлено на проверку возможности повышения привилегий во внутренней сети, получения доступа к критичной информации или внутренним системам. При проведении работ моделируются действия потенциального нарушителя, получившего тем или иным способом доступ во внутреннюю сеть организации. Подобный подход позволяет получить независимую оценку эффективности методов и средств защиты информации в компании.

Результаты работ

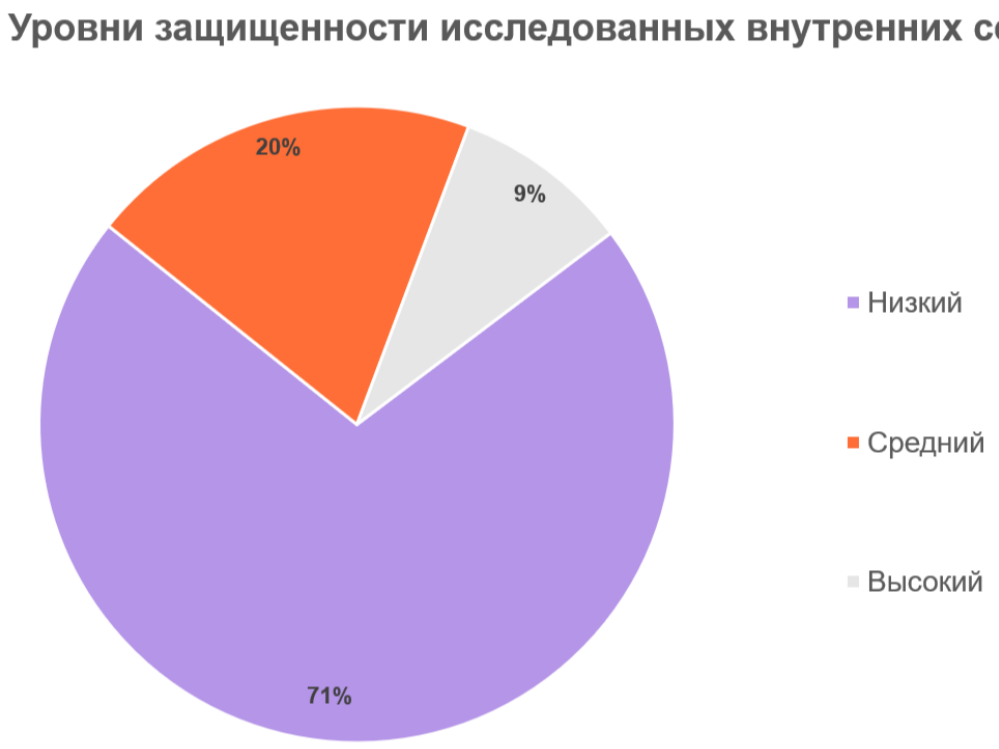
За минувший год нами было выполнено более 30 проектов по внутреннему тестированию на проникновения. В большинстве случаев основой целью работ являлось получение контроля над доменом. Однако заказчиками также ставились иные цели, например, получение доступа к различным информационным системам и базам данных во внутренней сети, к инфраструктурам резервного копирования, виртуализации, VPN и SIEM, а также к прочим критичным системам. Подобный подход говорит о том, что компании уделяют все больше внимания защите своих информационных активов во внутренней сети.

Поставленные цели были достигнуты в **91%** проектов. Только в **9%** случаев уровень защищенности внутренней сети был оценен как **высокий**. То есть в каждой **девятой** компании злоумышленник может повысить привилегии и/или получить доступ к различным критичным системам и данным во внутренней сети.

Стоит отметить, что в некоторых проектах уровень был оценен как средний даже в случае успешного достижения цели в связи с **высокой сложностью реализации вектора атаки**. Это говорит о том, что в подобных случаях реализовать вектор атаки может только злоумышленник, обладающий достаточно высокой квалификацией и/или значительным количеством времени на его реализацию.

Злоумышленник низкой квалификации не обладает специализированными знаниями, специализированным ПО, использует публично доступные эксплойты.

Злоумышленник высокой квалификации обладает специализированными знаниями и навыками для создания собственного и модификации публично доступного ПО, способен составлять сложные цепочки атак.



Векторы повышения привилегий

В выборку для исследования были включены все векторы, позволившие получить контроль над доменом. Именно получение контроля над доменом являлось основной целью в большинстве проектов, а также требовалось для реализации дополнительных задач. Например, в результате успешного получения контроля над доменом в одном из проектов был получен доступ к нескольким внутренним БД, инфраструктурам VPN, SIEM и резервного копирования, кластерам Kubernetes продуктивного контура и прочим критичным системам.

При этом получение контроля над доменом не всегда было необходимо для реализации поставленных задач. Так, в ряде случаев для получения доступа к целевым системам привилегии администратора домена не понадобились. Например, в ходе одного из проектов удалось скомпрометировать два домена и 9 целевых информационных систем. При этом для компрометации 6 из этих систем получение контроля над доменом не требовалось.

6

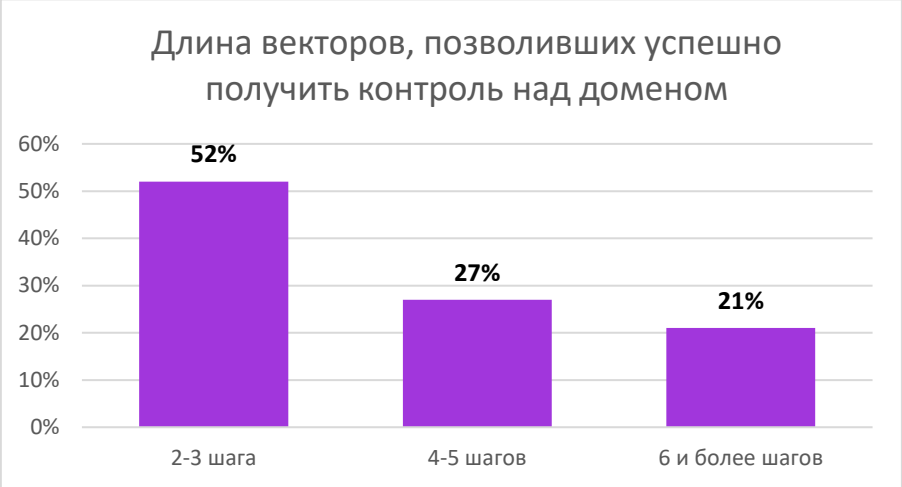
Максимальное количество успешных векторов в одном проекте

2

Минимальное количество шагов в векторе получения контроля над доменом

Максимальное количество векторов получения контроля над доменом, продемонстрированных в рамках одного проекта, было равно **6**. При этом, как и в случае с внешним пентестом, началом векторов послужила эксплуатация разных уязвимостей и недостатков, что также открывает больше возможностей для подготовки и реализации атак и увеличивает вероятность успешного повышения привилегий во внутренней сети.

Минимальная длина вектора получения контроля над доменом составила **2 шага**, то есть злоумышленнику достаточно совершить всего два действия для получения контроля над доменом. Более чем в половине случаев (**52%**) для захвата домена потребовалось не более **3-х шагов**, а почти каждый **восьмой** вектор был реализован не более чем за **5 шагов**.



2 часа

Минимальное количество времени на получение контроля над доменом

Минимальное количество времени, потребовавшееся для получения максимальных привилегий в домене, составило всего **2 часа**. В среднем для достижения указанной цели требовалось от **1** до **5** дней. При этом для определения и реализации **33%** таких векторов требовалось от **нескольких часов** до **1 дня**, еще для **46%** векторов – **2-3,5 дня**. То есть в **79%** случаев злоумышленнику нужно не более **3,5 дней** для получения повышенных привилегий в домене, которые позволят получить доступ к различным критичным информационным системам, базам данных и прочим значимым объектам во внутренней сети.

Распространенные критичные уязвимости внутренних сетей

Определение и реализация успешных векторов повышения привилегий и получения доступа к различным системам и данным во внутренней сети начинается с эксплуатации критичных уязвимостей и недостатков, поэтому именно они представляют наибольший интерес при проведении внутреннего пентеста.

В минувшем году наиболее часто нам встречались следующие критичные уязвимости и недостатки внутренних сетей:

- использование слабых паролей;
- использование программного обеспечения с известными уязвимостями;
- некорректная настройка ACL (Access Control List);
- некорректная настройка шаблонов сертификатов;
- повторное использование паролей.

На протяжении нескольких лет прослеживается тенденция использования **слабых** и **повторяющихся паролей**. Не стал исключением и 2024 год: в ходе проектов по внутреннему тестированию на проникновение все также встречалось большое количество недостатков, связанных с использованием слабых паролей (**57%**) и повторным использованием паролей (**20%**).

На использование слабых паролей пришлось **19%** от общего числа всех обнаруженных за отчетный период уязвимостей и недостатков во всех проектах по внутреннему пентесту. Именно эти недостатки послужили началом успешного вектора получения контроля над доменом в **30%** случаев.

Не менее существенным недостатком является **повторное использование паролей**. Например, в некоторых проектах этот недостаток позволил получить контроль сразу над **несколькими доменами** с помощью одного вектора атаки. Так, в ходе работ специалисты скомпрометировали учетную запись пользователя, входившего в группу администраторов домена, и получили контроль над доменом. Оказалось, что эти же учетные данные действительны для нескольких других доменов, что позволило также их скомпрометировать.

Во внутренних сетях по-прежнему наблюдается **использование ПО с известными уязвимостями** (**37%**). Например:

- MS17-010
- MS08-067
- CVE-2018-0171
- CVE-2020-24032

- CVE-2024-23897
- CVE-2019-0708 (BlueKeep)
- CVE-2021-1675 (PrintNightmare)
- CVE-2021-36942 (PetitPotam)
- CVE-2023-28130
- PrinterBug
- DFSCoerce
- MSEven

Указанные уязвимости открывают для злоумышленника возможности выполнения произвольного кода на узлах внутренней сети, в том числе с повышенными привилегиями, проведения атак «принуждение к аутентификации», а также чтения произвольных файлов на уязвимом узле без прохождения аутентификации.

Кроме того, актуальной проблемой внутренних сетей в 2024 году стала **некорректная настройка ACL** (Access control lists). Эксплуатация указанного недостатка может привести к компрометации различных систем и сервисов во внутренней сети, а также к получению контроля над доменом.

Также распространенными остаются недостатки, связанные с **некорректной конфигурацией шаблонов сертификатов**. Указанные недостатки послужили началом **19%** успешных векторов.

Интересные особенности проектов по внутреннему пентесту

В минувшем году помимо типовых задач, заключающихся в получении контроля над доменом и/или доступа к различным критичным системам, в рамках проектов по внутреннему пентесту мы также решали дополнительные задачи, связанные с анализом физического периметра и Wi-Fi сетей.

Анализ защищенности физического периметра

В ходе ряда проектов проводилась проверка возможности получения доступа на территорию заказчика путем клонирования пропусков сотрудников. В результате проверок было выявлено, что компании, для которых проводились такие работы, используют устаревшие технологии, уязвимые к атакам дистанционного клонирования пропусков.

Например, в ходе одного из проектов специалистам «Солара» удалось клонировать пропуск сотрудника ИТ-департамента и получить **доступ к критичному объекту в офисе** заказчика. При этом факт клонирования пропуска и проникновения постороннего человека на критичный объект не был замечен службой безопасности, а пропуск не был заблокирован.

Кроме того, данные для клонирования пропусков для несанкционированного доступа на территорию компании могут быть получены в ходе ранних этапов тестирования. Например, в ряде случаев в ходе внутреннего тестирования развитие в сети позволило нам получить доступ к серверам СКУД, находящимся в одной подсети с офисными ресурсами. Доступ к подобным системам в свою очередь позволил получить сведения о сотрудниках и их пропусках, что позволило сделать дубликат пропуска и получить доступ на территорию заказчика.

Таким образом, не стоит забывать об уязвимостях физического периметра, используя которые, злоумышленник может проникнуть на территорию организации и получить

доступ к различным критичным объектам, например, к серверным помещениям. Поэтому важно отметить, что компаниям не стоит исключать подобные векторы из своих рисков ИБ.

Анализ защищенности беспроводных сетей

В ходе ряда проектов также проверялась возможность получения первичного доступа во внутреннюю сеть через беспроводные сети. Например, в одном из проектов удалось успешно подключиться к беспроводной сети, дальнейший анализ которой показал, что она **никак не изолирована от внутренней сети** заказчика. Это позволило развить дальнейший вектор атаки и получить **контроль над доменом**.

Таким образом, использование уязвимых технологии беспроводных сетей и отсутствие корректных разграничений между сетями может позволить злоумышленнику получить доступ во внутреннюю сеть и развить вектор повышения привилегий.

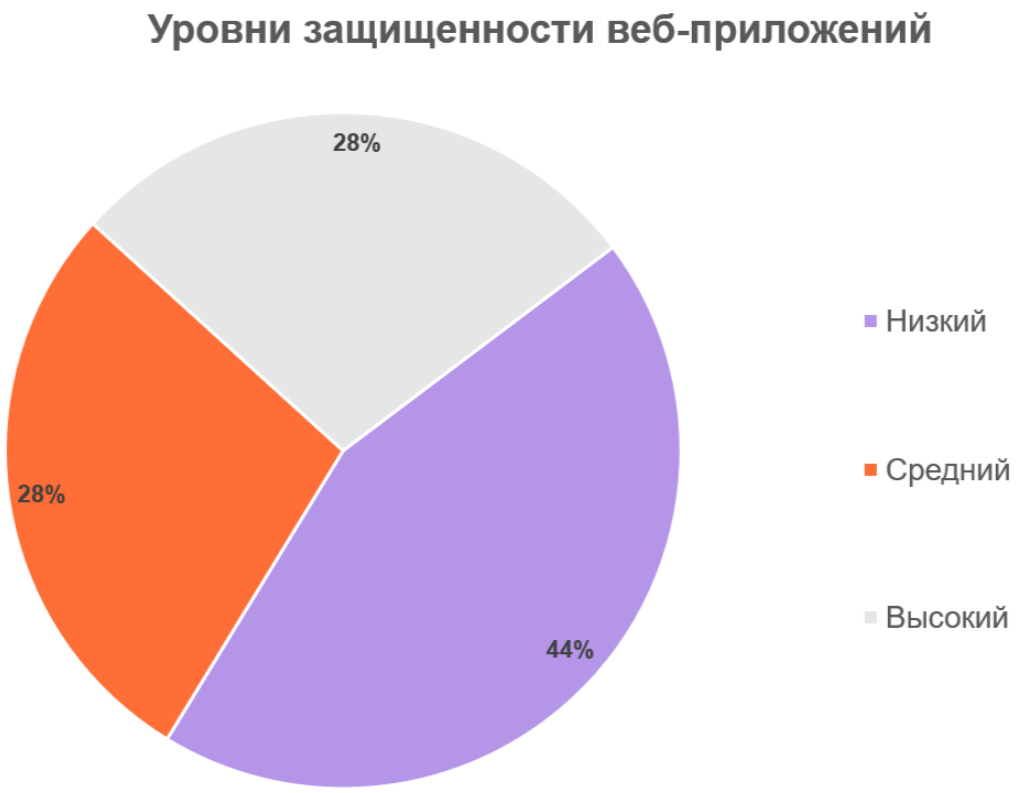
Дополнительно отметим, что атаки с помощью беспроводных сетей могут проводиться без физического присутствия в офисе компании, и злоумышленник может находиться на удалении от беспроводных точек доступа.

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

В минувшем году нами было исследовано более **100** веб-приложений различных заказчиков. **Низким** уровнем защищенности было отмечено **28%** исследованных приложений, столько же приложений имело **средний** уровень защищенности. То есть, как и в 2023 году, более чем **в половине случаев** были обнаружены уязвимости и недостатки высокой и/или средней степени критичности, успешная эксплуатация которых может позволить злоумышленнику нанести существенный ущерб информационным активам и репутации компании. Хотя бы одна критичная уязвимость была обнаружена в **46%** исследованных приложений.



Распространенные уязвимости и недостатки веб-приложений

Распространенной проблемой веб-приложений остаются недостатки, связанные с **раскрытием отладочной и конфигурационной информации**. Так, в **70%** приложений раскрывались переменные окружения, учетные данные, исходный код приложения, внутренние IP-адреса и прочие сведения, которые могут быть использованы злоумышленником для последующего поиска известных уязвимостей и подготовки дальнейших атак.

Стоит отметить, что в ряде случаев такие недостатки могут позволить реализовать угрозы, приводящие к **существенному ущербу** для информационных активов компании. Например, одно из исследованных приложений позволяло получить доступ к документации API, раскрывающей сценарий для получения доступа к переменным окружения, в том числе к ключу шифрования JWT токена и парольной фразе. Эти данные позволили выполнить эксплуатацию другого недостатка, связанного с возможностью обхода механизмов аутентификации. В результате удалось сформировать корректный JWT токен для другого пользователя и **получить доступ к его данным.**

Более половины приложений оказались подвержены **недостаткам контроля доступа**, которые из года в год также остаются одними из самых распространенных. Успешная эксплуатация таких недостатков может позволить получить доступ к данным других пользователей, в том числе к **персональным** (например, ФИО, номер телефона, паспортные данные, СНИЛС, адрес электронной почты). Подобная информация в дальнейшем может быть использована для проведения атак методами социальной инженерии.

Кроме того, недостатки контроля доступа могут привести к повышению привилегий, возможности чтения и изменения обрабатываемой в приложении информации, а также выполнению действий, недоступных из графического интерфейса.

Стоит отметить, что больше всего **критичных** уязвимостей и недостатков было обнаружено именно среди недостатков контроля доступа. Так, хотя бы один критичный недостаток этого типа был обнаружен в **26%** приложений.

По-прежнему остаются распространенными уязвимости, приводящие к возможности проведения атак «**Межсайтовое внедрение сценариев (XSS)**» (обнаружены в **38%** приложений). В результате успешного проведения такой атаки могут быть реализованы следующие угрозы:

Стоит отметить, что успешная реализация подобной атаки может позволить злоумышленнику отобразить для пользователей произвольные изображения, текст и прочие данные, в том числе противоправного характера. Нелегитимная информация,

размещенная на официальном ресурсе организации, может вводить пользователей в заблуждение, так как она будет восприниматься как информация из официального источника. Это в свою очередь может привести к репутационному ущербу для компании и распространению заведомо ложных данных, в том числе через средства массовой информации.

Также в число распространенных проблем веб-приложений вошли недостатки, приводящие к **раскрытию информации об используемом программном обеспечении** (**37%**) и **недостатки бизнес-логики** (**30%**).

Наша система оценки обнаруженных уязвимостей и недостатков также включает в себя оценку сложности эксплуатации. Сложность считается **высокой**, если для успешной эксплуатации уязвимости необходимы дополнительные условия, которые не зависят от атакующего (например, действия пользователя, определенное состояние или конфигурация системы и т.п.).

В минувшем году **77%** всех обнаруженных уязвимостей и недостатков были отмечены **низкой** сложностью, то есть для их успешной эксплуатации не требуется выполнение никаких дополнительных условий.

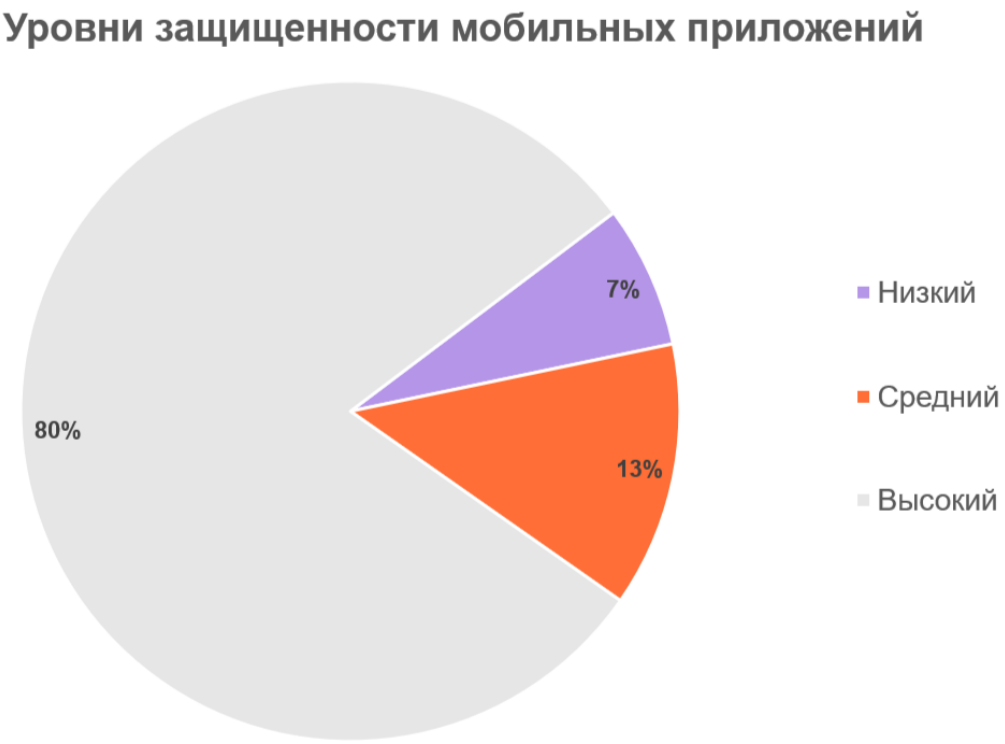
Для успешной эксплуатации **51%** выявленных уязвимостей и недостатков не требуется **авторизованный доступ** к приложению (то есть их эксплуатация возможна без каких-либо привилегий).

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

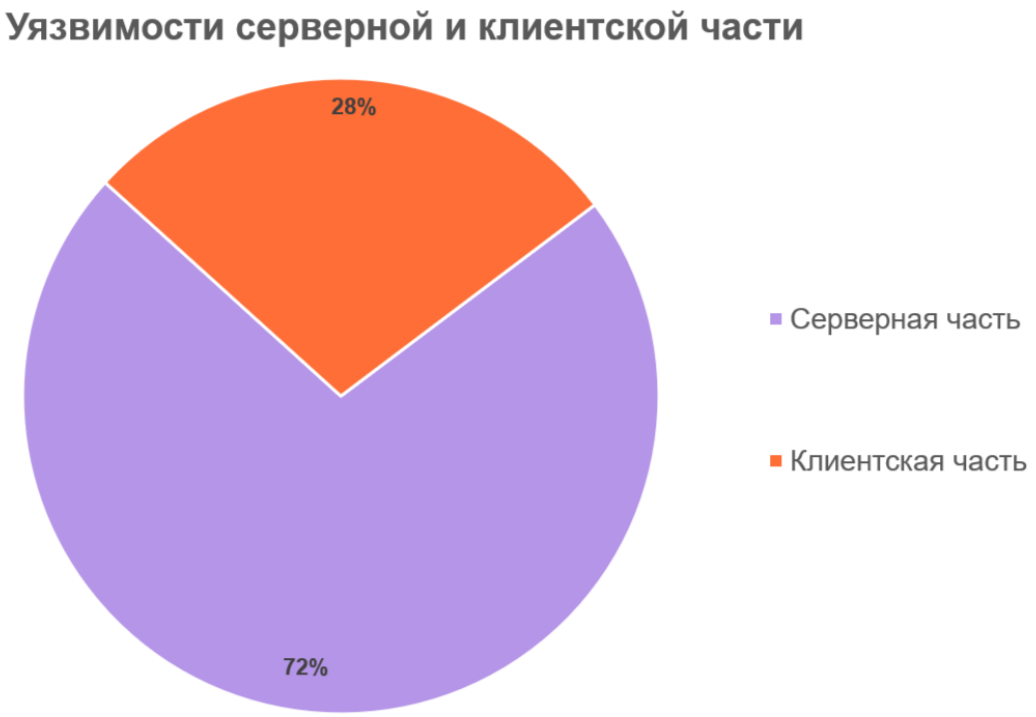
В минувшем году **80%** исследованных мобильных приложений было отмечено **высоким** уровнем защищенности. При этом некоторые приложения, получившие такую оценку, ранее неоднократно исследовались специалистами «Солара» на протяжении нескольких лет. Таким образом, высокие показатели уровня защищенности во многом были достигнуты благодаря регулярному проведению анализа защищенности и своевременному устранению выявленных уязвимостей и недостатков.



При этом, несмотря на положительную динамику, в мобильных приложениях по-прежнему присутствуют уязвимости и недостатки **высокой** и/или **средней** степени критичности, снижающие уровень защищенности и позволяющие нанести ущерб компании.

Больше всего уязвимостей и недостатков было обнаружено в **серверной части** приложений (**72%**). Это обусловлено в первую очередь тем, что эксплуатация уязвимостей клиентской части затруднительна, так как для нее зачастую требуется физический или удаленный доступ к устройству.

Также отметим, что **71%** уязвимостей и недостатков серверной части был отмечен **низкой** сложностью эксплуатации, что говорит об отсутствии необходимости соблюдения каких-либо дополнительных условий для их успешной эксплуатации.



Распространенные уязвимости и недостатки серверной части мобильных приложений:

1. **Раскрытие отладочной и конфигурационной информации** (53%)

Более половины мобильных приложений содержат уязвимости, раскрывающие отладочную и конфигурационную информацию, которая позволяет получить сведения о текущих настройках, окружении и/или отдельных компонентах приложения, например, данные из документации API, сведения о внутренних и тестовых адресах, версиях программного обеспечения и прочую информацию. Такая информация помогает злоумышленнику упростить исследование приложения и подготовку дальнейших атак.

2. **Недостатки контроля доступа (40%)**

Некорректная реализация проверки прав доступа позволяет пользователю совершать действия вне установленных для него привилегий, что может быть использовано злоумышленником для повышения привилегий, получения данных других пользователей и/или получения дополнительных функциональных возможностей.

3. **Использование JWT-ключа по умолчанию (27%)**

В **27%** исследованных в 2024 году мобильных приложений для подписи JWT-токена с помощью алгоритма HS256 используется ключ по умолчанию. Такие ключи могут быть легко подобраны или получены из публичных источников, что может позволить злоумышленнику подделать токен и получить несанкционированный доступ к защищенным ресурсам. Использование предсказуемых ключей снижает уровень защищенности приложения и делает его уязвимым для дальнейших атак.

Распространенные уязвимости и недостатки клиентской части мобильных приложений:

1. **Отсутствие обфускации исходного кода мобильного приложения (40%)**

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

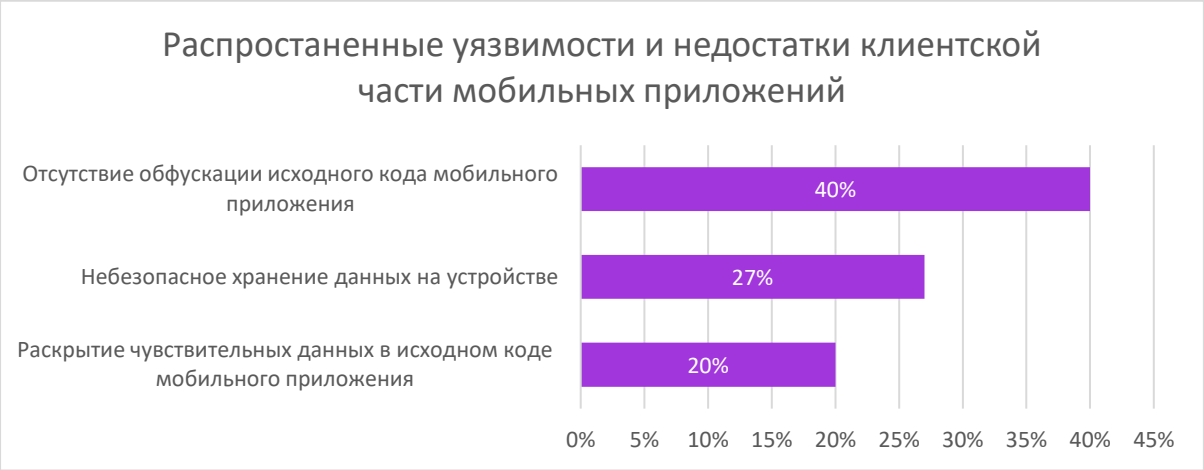
2. **Небезопасное хранение данных на устройстве (27%)**

В **27%** мобильных приложений данные пользователей сохраняются в незашифрованных базах данных, журналах событий или в прочих файлах непосредственно на устройстве. Например, исследованные в минувшем году приложения сохраняли на устройстве различную информацию о пользователях, включая **персональные данные**, такие как ФИО, СНИЛС, дата рождения и прочие сведения.

При этом после выхода из профиля или удаления приложения чувствительная информация сохраняется на устройстве. При наличие физического доступа (например, в случае потери или кражи) или установке на устройство вредоносного программного обеспечения злоумышленник может получить доступ к директории приложения, а следовательно, и ко всей хранимой в ней информации.

3. **Чувствительные данные в исходном коде мобильного приложения (20%)**

В исходных кодах клиентской части **20%** приложений содержатся 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

Своевременное обнаружение и устранение 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 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 для компаний-разработчиков 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;

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