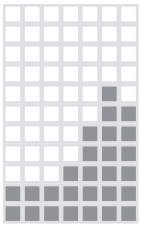


СТАТИСТИКА УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ЗА 2011—2012 ГОДЫ

Москва, 2013

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Тестирование на проникновение представляет собой один из методов аудита информационной безопасности, который позволяет смоделировать действия атакующего и на практике оценить, насколько эффективны используемые меры защиты информации. Зачастую именно в результате тестирования на проникновение владелец информационной системы может узнать о тех недостатках реализации защиты, которые трудно выявить в ходе высокоуровневого аудита информационной безопасности или технического, но поверхностного инструментального сканирования.

В настоящем отчете приведена общая статистика по результатам работ по тестированию на проникновение, проведенных специалистами компании Positive Technologies в 2011—2012 годах. Рассматриваются проекты как по внешнему тестированию на проникновение со стороны сети Интернет, так и по тестированию со стороны внутреннего злоумышленника, находящегося в пользовательском сегменте сети.

Для исследования в каждом году было выбрано по 10 систем. В обзоре рассматриваются системы наиболее крупных государственных и коммерческих компаний (в том числе, входящих в рейтинг 400 крупнейших компаний России в 2012 г. по объему реализации продукции по версии агентства «Эксперт»[1]). Результаты работ по анализу защищенности, которые по просьбе владельцев систем проводились на ограниченном количестве узлов и не отражают состояние защищенности корпоративной информационной системы в целом, — не были включены в исследование.

[1] http://expert.ru/dossier/rating/expert-400/

1 РЕЗЮМЕ

По результатам исследования защищенности корпоративных информационных систем в 2011—2012 годах был проведен статистический анализ полученных данных.

В данном разделе приведены наиболее значимые заключения по статистическому анализу уязвимостей, выявленных в корпоративных системах.

1 НЕДОСТАТКИ ЗАЩИТЫ СЕТЕВОГО ПЕРИМЕТРА

В каждом третьем случае любой внешний злоумышленник может получить полный контроль над всей инфраструктурой

- В 74% исследованных систем любой внешний нарушитель, действующий со стороны сети Интернет, способен получить доступ к узлам внутренней сети. При этом в 32% случаев внешний злоумышленник может развить атаку и получить полный контроль над всей инфраструктурой предприятия.
- В среднем для преодоления сетевого периметра внешнему атакующему требуется осуществить эксплуатацию трех различных уязвимостей, при этом в 74% случаев для проведения атаки достаточно иметь среднюю или низкую квалификацию.
- Почти в половине случаев вектор проникновения во внутреннюю сеть основывается на слабости парольной защиты. Данная уязвимость является самой распространенной, она была обнаружена на сетевом периметре 79% исследованных систем, при этом в 74% случаев словарные пароли использовались для привилегированных учетных записей.
- В каждой третьей системе доступ во внутреннюю сеть осуществляется через уязвимости веб-приложений. Так, уязвимость типа «Внедрение операторов SQL» встречается в 63% систем. Уязвимости веб-приложений были обнаружены во всех исследованных системах.

2 НЕДОСТАТКИ ЗАЩИТЫ ВНУТРЕННЕЙ СЕТИ

Внутренний непривилегированный злоумышленник в 84% случаев может получить максимальные привилегии в критически важных системах

- Во всех исследованных системах непривилегированный внутренний нарушитель, находящийся в пользовательском сегменте сети, может так или иначе расширить свои привилегии и получить несанкционированный доступ к ресурсам. При этом в 67% случаев внутренний нарушитель может получить полный контроль над всей информационной инфраструктурой организации.

- Только в 30% случаев внутренний атакующий должен обладать высокой квалификацией для получения доступа к критическим ресурсам, тогда как для 40% систем успешные атаки возможны со стороны любого неквалифицированного пользователя внутренней сети.

- В среднем при наличии доступа во внутреннюю сеть для получения контроля над критическими ресурсами злоумышленнику требуется эксплуатация 7 различных уязвимостей.

- Наиболее распространенными уязвимостями ресурсов внутренней сети являются использование слабых паролей и недостатки фильтрации и защиты служебных протоколов канального и сетевого уровней, таких как ARP, STP, DHCP, CDP. Обе этих уязвимости встречаются в 92% систем. Следующий по распространенности недостаток — использование открытых протоколов передачи данных, таких как Telnet, FTP, HTTP, которое встречается в 75% случаев.

- Почти все рассмотренные системы (95%) содержат критические уязвимости; во всех системах были обнаружены уязвимости среднего уровня риска.

3 НЕДОСТАТКИ ОСВЕДОМЛЕННОСТИ СОТРУДНИКОВ В ВОПРОСАХ ИБ

В среднем каждый пятый пользователь переходил по фишинговым ссылкам и осуществлял ввод учетных данных либо запуск предложенных файлов

- При оценке осведомленности пользователей в вопросах информационной безопасности во всех случаях были обнаружены те или иные недостатки. В каждой третьей системе уровень осведомленности пользователей был оценен как крайне низкий, в этих системах свыше 30% адресатов рассылки, эмулирующей фишинг, перешли по предложенным ссылкам и запустили предложенный файл или ввели свои учетные данные.

- В среднем каждый пятый пользователь осуществлял переход по предлагаемой в сообщении ссылке, при этом 1% пользователей попытались вступить в диалог с автором небезопасного письма.

POSITIVE TECHNOLOGIES

АНАЛИТИКА 2011 • 2012 СТАТИСТИКА УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ НА СЕТЕВОМ ПЕРИМЕТРЕ

79%	Словарные пароли пользователей
63%	Внедрение операторов SQL
58%	Интерфейсы управления оборудованием доступны любому пользователю сети Интернет
53%	Межсайтовое выполнение сценариев
47%	Хранение важных данных в открытом виде
47%	Раскрытие конфигурационной информации в веб-приложениях
47%	Недостаточная защита от подбора учетных данных
47%	Использование открытых протоколов передачи данных
42%	Выход за пределы каталога (Path Traversal)
32%	Раскрытие информации об идентификаторах

ВЕКТОРЫ ПРЕОДОЛЕНИЯ ПЕРИМЕТРА

УРОВЕНЬ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНЕШНЕГО ЗЛОУМЫШЛЕННИКА

32%	Полный контроль над инфраструктурой
11%	Максимальные локальные привилегии на узле ЛВС
25%	Максимальные локальные привилегии на внешнем веб-сервере
11%	Администратор веб-приложения
5%	Пользователь веб-приложения
16%	Не установлен в рамках заданных границ проведения работ

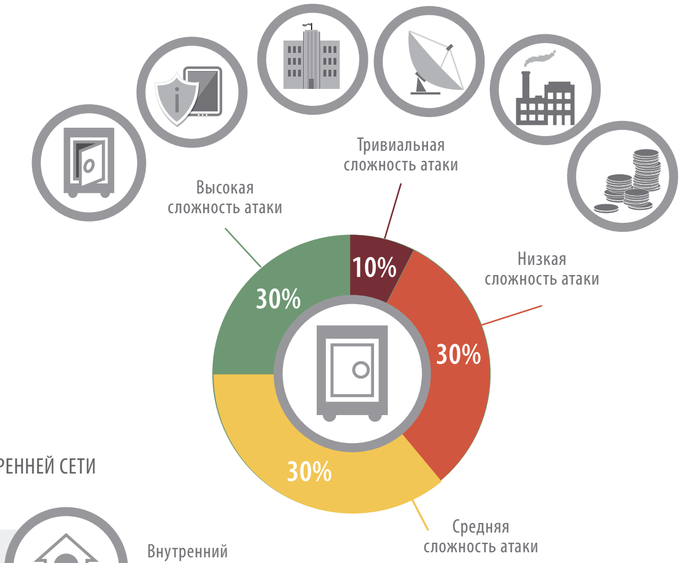
Высокая степень риска Средняя степень риска Низкая степень риска

3 ШАГА
требуется в среднем
для преодоления периметра

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ

7 ШАГОВ
требуется в среднем для получения доступа
к критически важным системам

КРИТИЧЕСКИ ВАЖНЫЕ РЕСУРСЫ



НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ ВО ВНУТРЕННЕЙ СЕТИ

92%	Словарные пароли пользователей
92%	Недостатки защиты служебных протоколов канального и сетевого уровней
75%	Использование открытых протоколов передачи данных
58%	Хранение важной информации в открытом виде
58%	Стандартное значение SNMP Community String с правами на чтение (public)
58%	Возможность подключения стороннего оборудования без его предварительной авторизации
50%	Стандартное значение SNMP Community String с правами на чтение и запись (private)
42%	Использование слабых алгоритмов шифрования при хранении паролей
42%	Интерфейсы управления оборудованием доступны любому пользователю локальной сети
42%	Недостаточная защита от подбора учетных данных

УРОВЕНЬ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНУТРЕННЕГО ЗЛОУМЫШЛЕННИКА

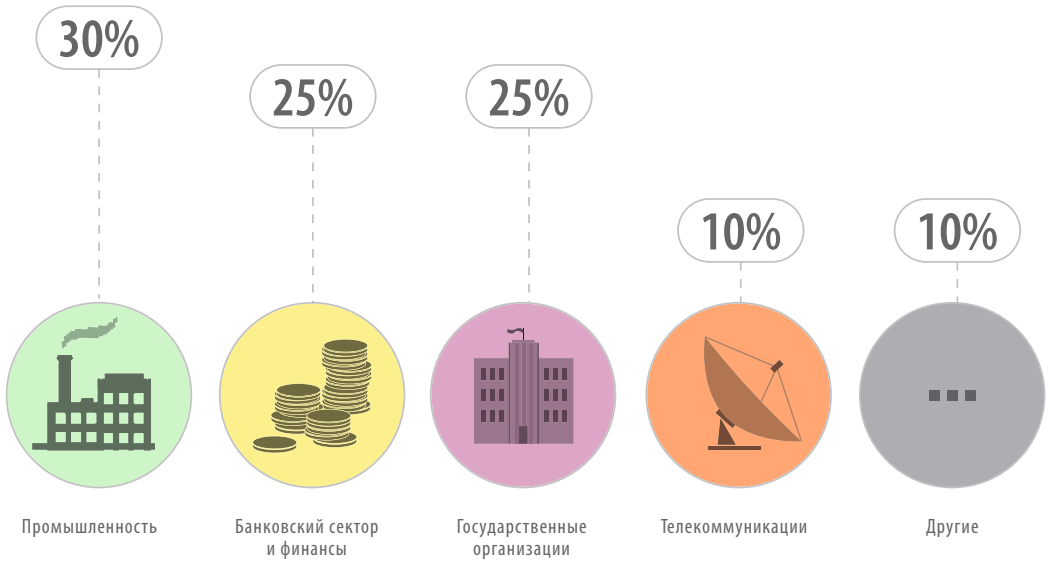
67%	Полный контроль над инфраструктурой
17%	Максимальные привилегии в критических системах
8%	Администратор СУБД в ЛВС
8%	Максимальные привилегии в критических системах (доступ возможен только из административного сегмента)

2 ИСХОДНЫЕ ДАННЫЕ

В рамках проведенного исследования были рассмотрены корпоративные информационные системы 20 российских и зарубежных компаний. Работы проводились в 2011 и 2012 годах, по 10 систем в каждом году. Результаты работ по анализу защищенности, которые по просьбе владельцев систем проводились на ограниченном количестве узлов и не отражают состояние защищенности корпоративной информационной системы в целом, не были включены в исследование.

Участниками исследования стали организации различных сфер экономики: телекоммуникационные компании, государственные организации, банковский и финансовый сектор, а также строительные и торговые компании.

ДОЛЯ СИСТЕМ, ОТНОСЯЩИХСЯ К РАЗЛИЧНЫМ ОТРАСЛЯМ ЭКОНОМИКИ



Треть всех исследованных систем относится к промышленным организациям. Чуть меньшую долю составляют компании банковской сферы и государственные учреждения. Незначительная доля систем принадлежит строительным компаниям и торговым организациям.

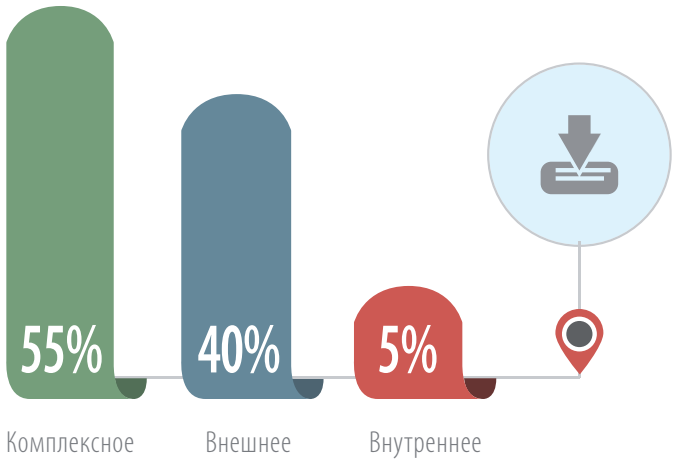
В исследованную выборку вошли не только крупнейшие в своей области коммерческие предприятия, но и ключевые государственные организации. Исследуемые корпоративные системы насчитывают тысячи узлов, зачастую эти системы распределены территориально и имеют десятки филиалов. В рамках исследований 25% систем рассматривались вместе с филиалами. Сложность сетевой инфраструктуры таких систем является причиной множества ошибок в настройках сетевого оборудования и в администрировании серверов, таким образом, проведение комплексного анализа защищенности является необходимой мерой при обеспечении информационной безопасности.

В состав оказанных услуг входили несколько видов тестирования на проникновение:

- внешнее тестирование на проникновение;
- внутреннее тестирование на проникновение;
- комплексное тестирование (включающее как внешнее, так и внутреннее тестирование на проникновение).

Общее соотношение систем, для которых были оказаны отдельные виды услуг, представлено на диаграмме.

СООТНОШЕНИЕ СИСТЕМ ПО ВИДАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ



Более половины компаний воспользовались услугой комплексного тестирования на проникновение, которая включает не только анализ защищенности сетевого периметра и проверку возможности развития атаки во внутреннюю сеть со стороны сети Интернет, но и внутреннее тестирование на проникновение, которое осуществляется из заданного сегмента внутренней сети (как правило, рассматривается подключение к пользовательскому сегменту). Отдельная услуга по внутреннему тестированию на проникновение была оказана лишь для одной рассмотренной системы.

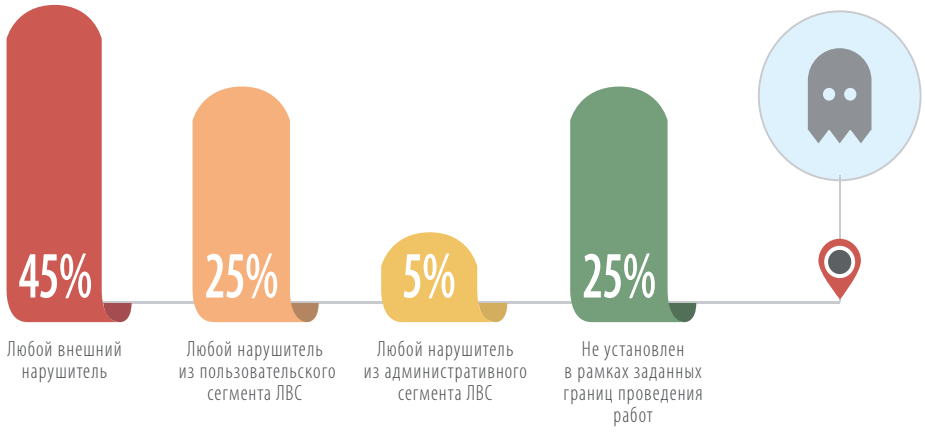
Перечисленные виды работ в 30% случаев сочетались с проверкой осведомленности пользователей систем в вопросах информационной безопасности.

3 СВОДНАЯ СТАТИСТИКА ЗА 2011—2012 ГОДЫ

3.1. ОБЩИЕ РЕЗУЛЬТАТЫ ТЕСТОВ НА ПРОНИКНОВЕНИЕ

В результате проведенных работ в 75% случаев специалистам Positive Technologies удалось получить полный контроль над критическими ресурсами тестируемых систем, при этом почти в половине случаев (45%) подобный уровень доступа мог быть получен со стороны любого внешнего нарушителя. В четверти случаев получение полного контроля над критическими ресурсами было возможно со стороны внутреннего нарушителя, находящегося в пользовательском сегменте локальной вычислительной сети и не имеющего никаких дополнительных привилегий.

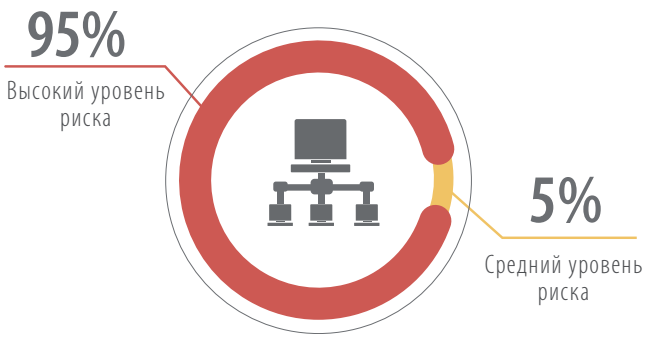
МИНИМАЛЬНЫЙ УРОВЕНЬ НАРУШИТЕЛЯ, НЕОБХОДИМЫЙ ДЛЯ ПОЛУЧЕНИЯ ПОЛНОГО КОНТРОЛЯ НАД КРИТИЧЕСКИМИ РЕСУРСАМИ



Зачастую внешний злоумышленник, действующий со стороны сети Интернет, может не только получить доступ к критическим системам, расположенным на сетевом периметре (таким как официальные веб-сайты компаний), но и получить доступ к внутренней сети и далее развить атаку вплоть до получения полного контроля над инфраструктурой. Так, почти три четверти рассмотренных систем (74%) позволяют любому внешнему злоумышленнику преодолеть защиту и получить доступ к узлам внутренней сети. Подробная статистика результатов анализа защищенности сетевого периметра приведена в разд. 3.2.

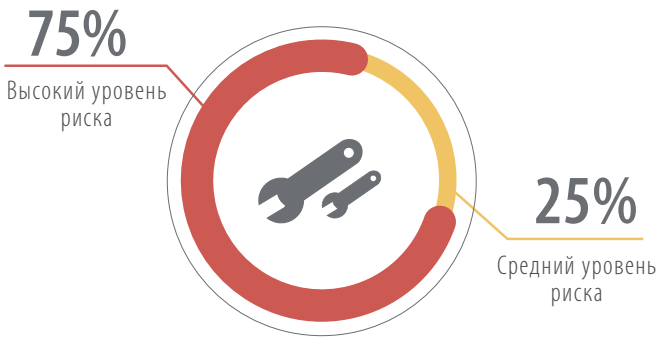
Практически все системы оказались подвержены уязвимостям высокой степени риска, и только в одной системе не было выявлено критических уязвимостей, однако присутствовали уязвимости среднего уровня риска.

СООТНОШЕНИЕ СИСТЕМ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ



Три четверти рассмотренных систем содержат уязвимости высокого уровня риска, связанные с недостатками конфигурации. Еще в 25% систем были выявлены недостатки среднего уровня риска.

МАКСИМАЛЬНЫЙ УРОВЕНЬ РИСКА УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С НЕДОСТАТКАМИ КОНФИГУРАЦИИ (ДОЛЯ СИСТЕМ)

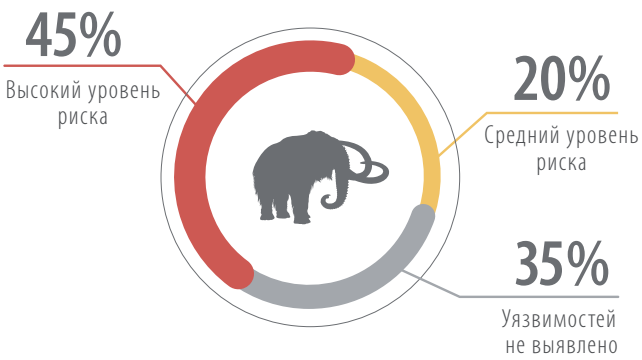


В 65% систем были выявлены уязвимости, связанные с отсутствием актуальных обновлений безопасности, среднего или высокого уровня риска. Почти половина систем содержала критические уязвимости. Средний возраст неустановленных обновлений по системам, где такие уязвимости были обнаружены, составляет 51 месяц, то есть **более 4 лет.** В одном из исследуемых государственных учреждений обновления не устанавливались в течение более чем 7 лет, в результате было обнаружено множество уязвимостей, в том числе критические уязвимости, позволяющие выполнять произвольный код на системе.

Минимальный возраст уязвимости, связанной с отсутствием обновлений безопасности, составил 16 месяцев. Данная уязвимость (CVE-2010-3856) была использована для повышения привилегий локального пользователя в операционной системе, получения контроля над сервером на сетевом периметре и дальнейшнего развития атаки во внутреннюю сеть.

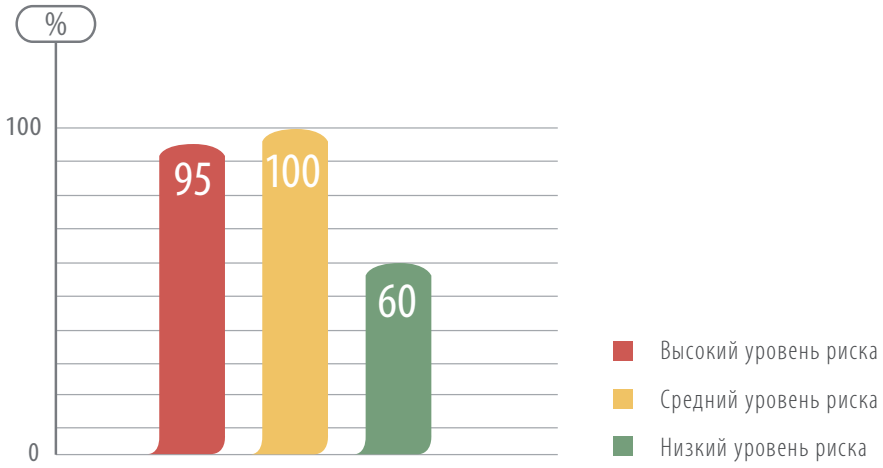
В системах, где уязвимости программного обеспечения не были обнаружены и использованы в ходе тестирования на проникновение (35%), в действительности могут использоваться устаревшие уязвимые версии программного обеспечения, однако в силу особенностей проведения работ по тестированию на проникновение данные системы могли не попасть в область проведения работ. Для выявления уязвимостей необходимо проводить комлексные работы по анализу защищенности.

МАКСИМАЛЬНЫЙ УРОВЕНЬ РИСКА УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ОТСУТСТВИЕМ ОБНОВЛЕНИЙ (ДОЛЯ СИСТЕМ)



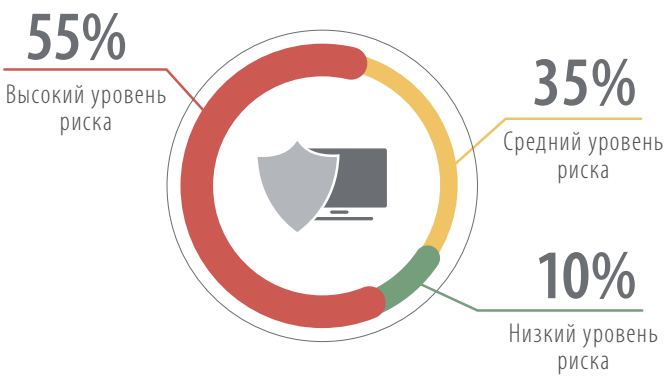
Абсолютно все исследованные системы оказались подвержены уязвимостям среднего уровня риска. Уязвимости высокой степени риска были обнаружены в 95% систем. Наименее распространенными оказались уязвимости низкой степени риска, которые обнаружены в 60% случаев.

ДОЛИ СИСТЕМ, ПОДВЕРЖЕННЫХ УЯЗВИМОСТЯМ РАЗЛИЧНЫХ УРОВНЕЙ РИСКА



В целом наиболее распространены оказались уязвимости высокой степени риска: более половины всех обнаруженных уязвимостей являются критическими. Треть уязвимостей относятся к уязвимостям среднего уровня риска и всего 10% — низкого.

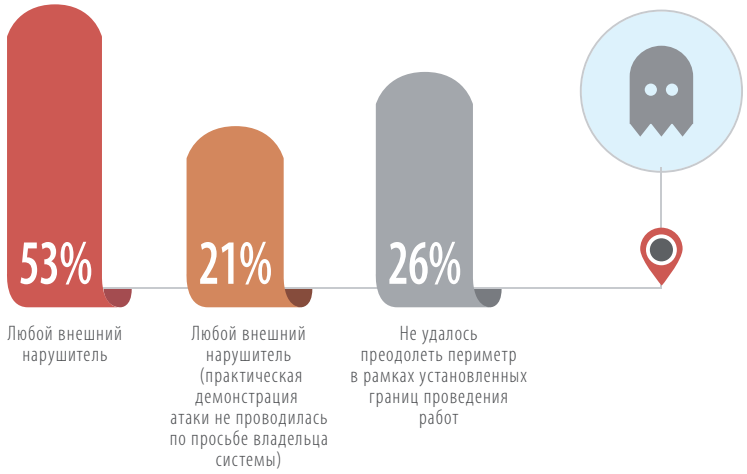
СООТНОШЕНИЕ УЯЗВИМОСТЕЙ РАЗЛИЧНОГО УРОВНЯ РИСКА (ДОЛЯ ОТ ОБЩЕГО КОЛИЧЕСТВА УЯЗВИМОСТЕЙ)



3.2. РЕЗУЛЬТАТЫ АНАЛИЗА ЗАЩИЩЕННОСТИ СЕТЕВОГО ПЕРИМЕТРА

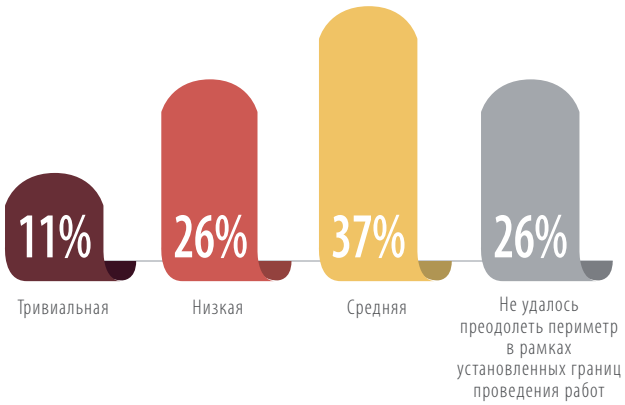
В 74% исследованных систем внешний злоумышленник, не имеющий никаких привилегий и дополнительных данных о сети, способен преодолеть сетевой периметр и попасть во внутреннюю сеть. При этом в каждом втором случае данная возможность была продемонстрирована специалистами Positive Technologies на практике. Если учитывать, что работы проводились для крупнейших компаний, подобная стастистика говорит о крайне низком уровне защищенности от атак со стороны внешнего нарушителя.

МИНИМАЛЬНЫЙ УРОВЕНЬ НАРУШИТЕЛЯ ДЛЯ ПРЕОДОЛЕНИЯ ПЕРИМЕТРА



В большинстве случаев для преодоления периметра злоумышленнику достаточно было иметь средний или низкий уровень квалификации.

СЛОЖНОСТЬ ПРЕОДОЛЕНИЯ ПЕРИМЕТРА

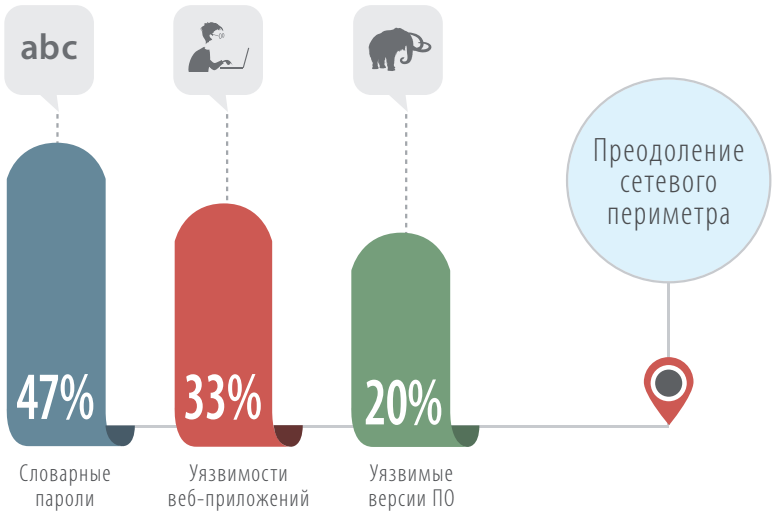


Для преодоления сетевого периметра требуется последовательная эксплуатация в среднем трех различных уязвимостей. Почти в половине случаев (47%) первым этапом служит подбор словарных паролей пользователей в различных системах, далее осуществляется расширение привилегий и получение контроля над каким-либо из ресурсов, относящихся ко внутренней сети.

В каждой третьей системе первым этапом преодоления защиты служила эксплуатация уязвимостей веб-приложений. Далее, в зависимости от полученного уровня доступа, атака распространялась до получения конроля над операционной системой уязвимого сервера. Различные уязвимости веб-приложений были обнаружены во всех исследуемых системах. Наиболее полный обзор об актуальных уязвимостях веб-приложений, подготовленный специалистами Positive Technologies, приведен в очете «Статистика уязвимостей веб-приложений (2012 г.)».

Наконец, в каждой пятой из систем, в которых удалось преодолеть сетевой периметр, это было сделано за счет эксплуатации различных уязвимостей, связанных с отсутствием актуальных обновлений безопасности.

ВЕКТОРЫ АТАК ДЛЯ ПРЕОДОЛЕНИЯ СЕТЕВОГО ПЕРИМЕТРА



Наиболее распространенные уязвимости, встречающиеся на ресурсах сетевого периметра исследованных компаний, приведены на диаграме ниже.

В тройку лидеров вошли:

- использование словарных паролей (в том числе — установленных производителями по умолчанию);
- внедрение операторов SQL;
- наличие на сетевом периметре интерфейсов удаленного доступа и управления сетевым оборудованием и серверами, которые должны быть доступны только ограниченному числу администраторов.

ДЕСЯТКА НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ СЕТЕВОГО ПЕРИМЕТРА

3.2.1. ИСПОЛЬЗОВАНИЕ СЛОВАРНЫХ ПАРОЛЕЙ

Уязвимость была обнаружена на сетевом периметре в 79% исследованных систем, при этом **в 74% таких случаев словарные пароли использовались для привилегированных учетных записей.** Этот недостаток в 47% случаев позволяет преодолеть сетевой периметр.

Словарные пароли используются как на уровне веб-приложений, так и для доступа к различному сетевому оборудованию и серверам, при этом зачастую эксплуатация этой уязвимости становится возможной благодаря наличию на сетевом периметре соответствующих интерфейсов удаленного доступа (таких как SSH, Telnet, RDP).

3.2.2. ВНЕДРЕНИЕ ОПЕРАТОРОВ SQL

Уязвимости типа «Внедрение операторов SQL» (SQL Injection) были обнаружены в 65% исследованных систем. Данная уязвимость оценивается как критическая и заключается в том, что веб-приложение некорректно проверяет поступившие от пользователя данные, которые в дальнейшем используются для генерации SQL-запросов к базе данных. Злоумышленник получает возможность работать с SQL-сервером в обход логики приложения, получать и модифицировать произвольную информацию на SQL-сервере в рамках привилегий веб-приложения.

Эксплуатация уязвимостей «Внедрение операторов SQL» зачастую является первым шагом атаки с целью проникновения во внутреннюю сеть. Так, в одной из крупных государственных организаций с филиалами в разных городах в ходе тестирования на проникновение данная уязвимость была обнаружена во множестве различных публичных веб-приложений, принадлежащих разным филиалам. В результате успешной эксплуатации уязвимостей проникновение во внутреннюю сеть было осуществлено сразу из нескольких точек на сетевом периметре. В дальнейшем атака была развита до получения полного контроля над сетью головной организации и, как следствие, над инфраструктурой предприятия целиком.

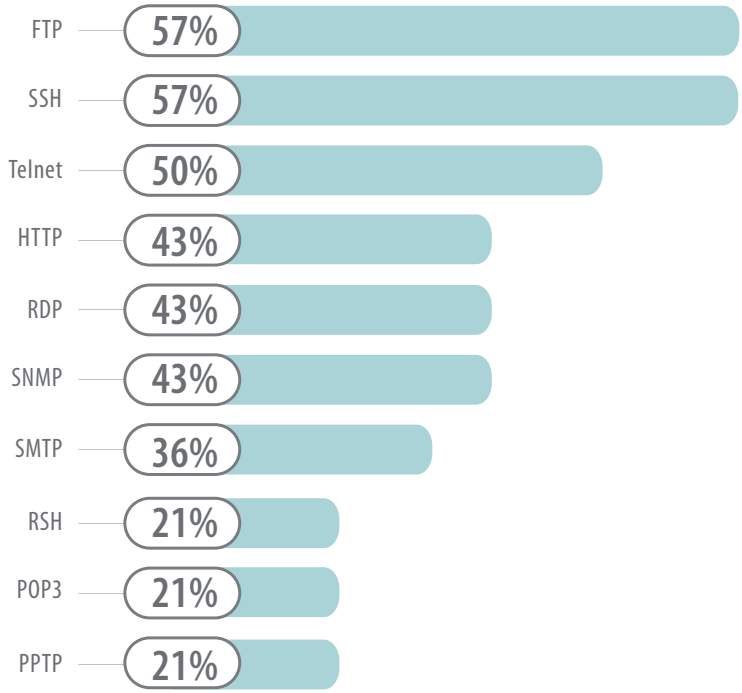
Как правило, наибольшую опасность представляет сочетание SQL Injection с уязвимостями, связанными с избыточными привилегиями пользователей. В частности, в описанном выше примере проникновение во внутреннюю сеть было возможно за счет того, что веб-приложения использовали для взаимодействия с СУБД учетные записи, обладающие правами администратора СУБД с возможностями выполнения команд ОС. Уязвимости, связанные с избыточностью привилегий пользователей, были выявлены в 21% исследованных систем.

3.2.3. НАЛИЧИЕ НА СЕТЕВОМ ПЕРИМЕТРЕ ИНТЕРФЕЙСОВ УПРАВЛЕНИЯ ОБОРУДОВАНИЕМ

Данная уязвимость имеет низкую степень риска и сама по себе не позволяет получить контроль над ресурсами. Как правило, обнаружение доступного интерфейса управления является лишь начальным этапом атаки, однако при наличии данного недостатка атакующий получает возможность подбирать идентификационные данные пользователей, а также обнаруживать и эксплуатировать различные уязвимости доступной сетевой службы. В случае успеха злоумышленник сразу получает возможность управления уязвимыми ресурсами с использованием уже имеющегося доступа, без необходимости развертывания собственных средств для взаимодействия.

На диаграмме представлено соотношение различных интерфейсов удаленного доступа на сетевом периметре в исследованных системах. Для протокола HTTP приведена доля систем, в которых со стороны сети Интернет были доступны веб-интерфейсы управления различным оборудованием, например сетевыми устройствами или веб-камерами.

ИСПОЛЬЗУЕМЫЕ НА СЕТЕВОМ ПЕРИМЕТРЕ ПРОТОКОЛЫ, В ТОМ ЧИСЛЕ ИНТЕРФЕЙСЫ УДАЛЕННОГО ДОСТУПА (ДОЛЯ СИСТЕМ)



Наличие на внешнем периметре сетевых служб, передающих данные по открытым протоколам, таким как Telnet, FTP, HTTP, упрощает задачу злоумышленника по преодолению периметра. Так, в 50% систем на сетевом периметре используется служба Telnet, в результате чего со стороны внешних сетей при успешной атаке «человек посередине» возможен перехват передающейся по данному открытому протоколу информации, например учетных данных администратора.

Зачастую администраторы оставляют заводские настройки у сетевых устройств со стандартными значениями строки подключения SNMP Community String. Протокол SNMP позволяет удаленно работать с данными конфигурации ОС в виде отдельных переменных. Компрометация переменной SNMP Community String с правами только на чтение (стандартное значение «public») позволяет получить дополнительную информацию о системе и затем использовать ее в ходе реализации других сценариев атаки. Компрометация переменной SNMP Community String с правами на чтение и запись (стандартное значение «private») разрешает вносить изменения в настройки системы, что в свою очередь позволяет нарушителю проводить различные атаки, в том числе с целью получения привилегированного доступа в системе.

Согласно полученным результатам, в 4 из 20 компаний на сетевом периметре присутствовали устройства, доступные по SNMP со стандартными значениями SNMP Community String. У одной из телекоммуникационных компаний на сетевом периметре было обнаружено сразу 34 устройства со стандартными значениями на чтение «public», а в одном из крупнейших государственных ведомств помимо узлов, доступных с правами на чтение, было обнаружено 7 узлов с возможностью чтения и записи («private»).

Подчеркнем, что речь идет о системах, интерфейсы управления оборудованием которых доступны на периметре сети, то есть любому внешнему атакующему.

Управление устройствами не должно быть доступно из внешних сетей. Во внутренней сети рекомендуется использовать безопасные протоколы (SSH, HTTPS и др.). Кроме того, рекомендуется настраивать списки контроля доступа таким образом, чтобы удаленное управление устройством было разрешено адресам только тех сетевых диапазонов, которые авторизованы для управления устройством.

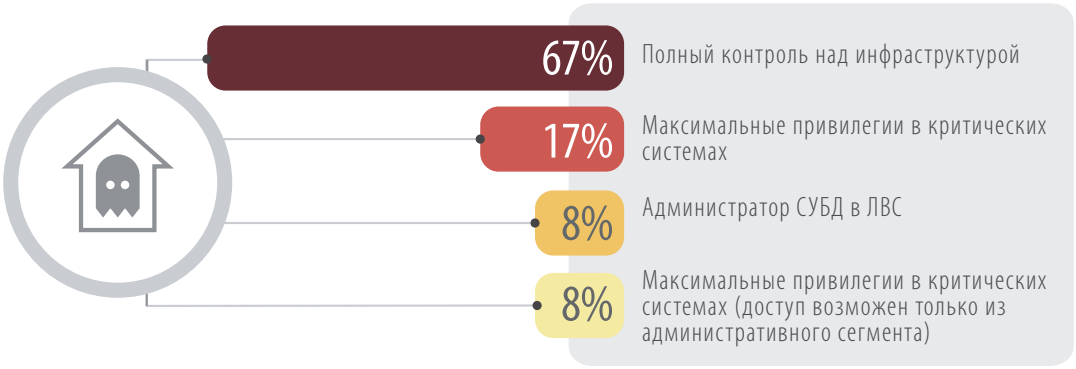
3.3. АНАЛИЗ ЗАЩИЩЕННОСТИ РЕСУРСОВ ВНУТРЕННЕЙ СЕТИ

В трети случаев внешний нарушитель после получения доступа к внутренней сети имеет возможности для развития атаки и получения полного контроля над всей IT-инфраструктурой компании. В целом для 84% исследованных систем в результате внешнего тестирования на проникновение со стороны сети Интернет удалось получить несанкционированный доступ к ресурсам с различными привилегиями.

СООТНОШЕНИЕ СИСТЕМ С РАЗЛИЧНЫМИ УРОВНЯМИ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНЕШНЕГО НАРУШИТЕЛЯ

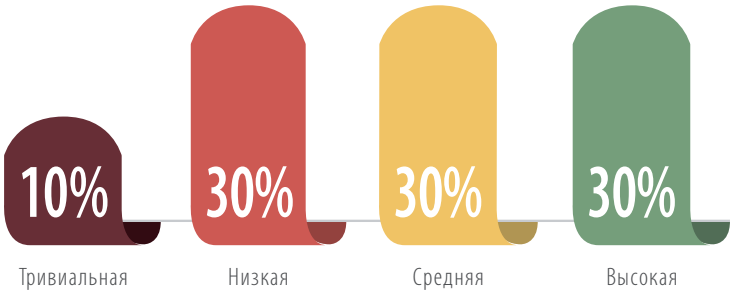
Что касается защиты от атак со стороны внутренних сетей, ситуация в данной сфере вызывает еще большие опасения. Если злоумышленник уже имеет доступ к сети (это может быть любой сотрудник компании или представитель сторонней организации, подключившийся к свободной сетевой розетке), то, согласно статистике, у него есть все шансы для повышения своих привилегий и получения доступа к критическим ресурсам. Для всех исследованных систем удалось получить несанкционированный доступ к критическим ресурсам при наличии доступа к сети. При этом в 67% случаев был получен полный контроль над всей инфраструктурой.

СООТНОШЕНИЕ СИСТЕМ С РАЗЛИЧНЫМИ УРОВНЯМИ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНУТРЕННЕГО НАРУШИТЕЛЯ



Сложность развития векторов атак до получения доступа к критическим ресурсам распределяется согласно диаграмме ниже. В 40% случаев получение доступа к таким ресурсам не составляет труда для внутреннего злоумышленника. При этом в 10% исследованных систем получение доступа к критическим ресурсам осуществляется тривиальными действиями, не требующими особых навыков и применения специальных технических или программных средств.

СЛОЖНОСТЬ ПОЛУЧЕНИЯ ДОСТУПА К КРИТИЧЕСКИМ РЕСУРСАМ СО СТОРОНЫ ВНУТРЕННЕГО НАРУШИТЕЛЯ



При проведении работ (как при преодолении периметра, так и при развитии атак внутри сети) в каждой системе были обнаружены и использованы для атаки новые, неизвестные ранее уязвимости веб-приложений. **При этом в 35% систем новые уязвимости обнаруживались не только в проприетарном ПО заказчика, но и в широко известных системах, распространяемых различными вендорами (уязвимости нулевого дня).** В случае обнаружения подобных уязвимостей, специалисты компании Positive Technologies уведомляли вендоров о данном факте. Информация о новых уязвимостях, обнаруживаемых экспертами центра Positive Research, регулярно публикуется на сайте Security Lab.

В среднем при наличии доступа во внутреннюю сеть для контроля над критическими ресурсами злоумышленнику требуется эксплуатация 7 уязвимостей. Самая короткая атака включала три шага:

1. Получение доступа к файлам конфигурации сетевого оборудования Cisco, хранящимся на общедоступных сетевых ресурсах.
2. Восстановление паролей, хранящихся в файлах конфигурации с использованием обратимого алгоритма кодирования Type 7.
3. Успешный подбор паролей привилегированных пользователей для множества критических ресурсов с использованием словаря, включающего пароли, восстановленные на предыдущем этапе.

Самая длинная атака насчитывала 13 шагов и заключалась в поэтапном расширении привилегий от рядового пользователя на веб-сервере во внутренней сети одного из филиалов крупной корпорации до получения полного контроля над головным офисом и всеми ресурсами предприятия в целом.

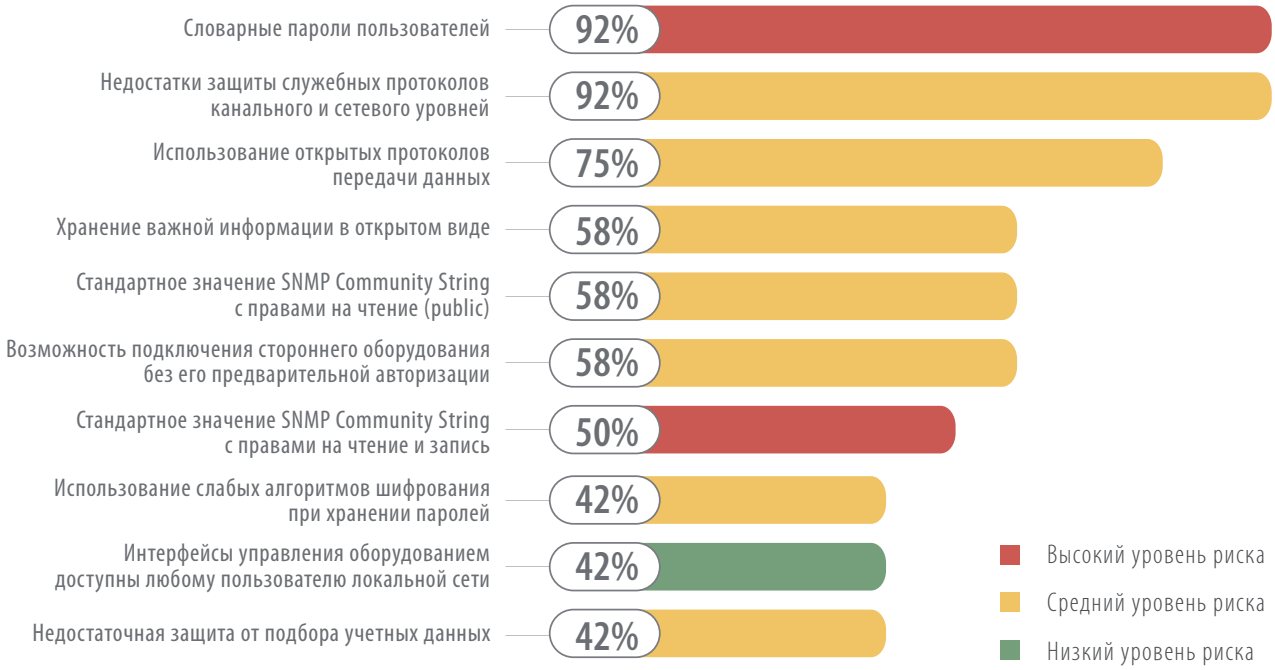
Стоит отметить, что одной из характерных особенностей управления IT-инфраструктурой на крупных предприятиях в последние два года является централизация управления (в основном средствами Active Directory), которая при недостаточном уровне защищенности играет на руку не только администраторам, но и злоумышленникам. Так, например, крайне распространена следующая комбинация недостаков реализации защиты, которая зачастую позволяет атакующему получить полный контроль над инфраструктурой с использованием доступных в открытом доступе утилит для взлома:

- наличие на компьютерах домена Active Directory стандартной учетной записи локального администратора;
- использование для данной учетной записи словарных паролей (например, фиксированного пароля, который администраторы устанавливают на все рабочие станции домена по умолчанию);
- отсутствующие или некорректно настроенные средства антивирусной защиты, либо антивирусы без функции самозащиты;
- отсутствие двухфакторной аутентификации для привилегированных учетных записей.

В такой ситуации злоумышленник может подобрать пароль локального администратора, с использованием полученных привилегий отключить средства антивирусной защиты (при необходимости) и запустить программное обеспечение для сбора данных о паролях активных пользователей компьютера из оперативной памяти. Если с системой в это время также работает привилегированный пользователь домена, злоумышленник получит его пароль, каким бы сложным он ни был, и сможет расширить свои привилегии. Подобная атака возможна из-за архитектурных особенностей ОС семейства Windows, при этом для ее реализации необходимо обладать привилегиями локального администратора, которые, как показывает практика, можно довольно быстро получить тем или иным методом.

Наиболее распространенные уязвимости, обнаруженные при анализе защищенности внутренних сетей исследованных систем, представлены на диаграмме.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ, ОБНАРУЖЕННЫЕ ПРИ АНАЛИЗЕ ЗАЩИЩЕННОСТИ ВНУТРЕННЕЙ СЕТИ



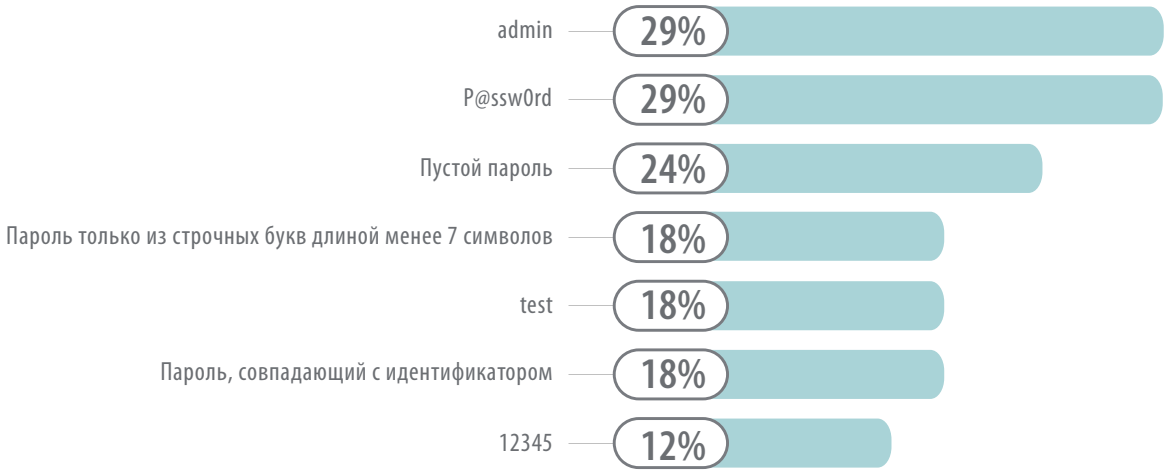
3.3.1. СЛОВАРНЫЕ ПАРОЛИ

Использование словарных паролей было выявлено во внутренних сетях 92% исследованных в 2011 и 2012 годах систем. Данная уязвимость в большинстве случаев является следствием недостатков действующей парольной политики. Однако даже строгая политика безопасности не всегда может гарантировать, что пользователь задаст действительно стойкий пароль к учетной записи. Примером может служить один из популярных паролей — P@ssw0rd. Даже если в компании реализована строгая парольная политика, подобный пароль формально удовлетворяет всем требованиям: в нем используются как заглавные, так и строчные буквы латинского алфавита, специальный символ и цифра. При этом пароль P@ssw0rd входит в словари наиболее часто используемых паролей и легко может быть подобран злоумышленниками. Другими примерами распространенных словарных паролей, подбор которых зачастую позволял специалистам Positive Technologies в ходе работ получать доступ к критическим ресурсам, являются: 12345678, qwerty12345, qwert и даже пароль из единственной цифры 1.

Слабые пароли были обнаружены среди учетных записей доменов Active Directory, учетных записей для доступа к СУБД, для доступа к интерфейсам управления веб-приложений и другим ресурсам. При этом словарные пароли часто используются не только рядовыми сотрудниками организаций, но и администраторами.

Наиболее распространенные словарные пароли привилегированных учетных записей представлены на диаграмме.

РАСПРОСТРАНЕННЫЕ СЛОВАРНЫЕ ПАРОЛИ АДМИНИСТРАТОРОВ
(УКАЗАНА ДОЛЯ СИСТЕМ ПО ОТНОШЕНИЮ К КОЛИЧЕСТВУ СИСТЕМ СО СЛАБЫМИ ПАРОЛЯМИ)

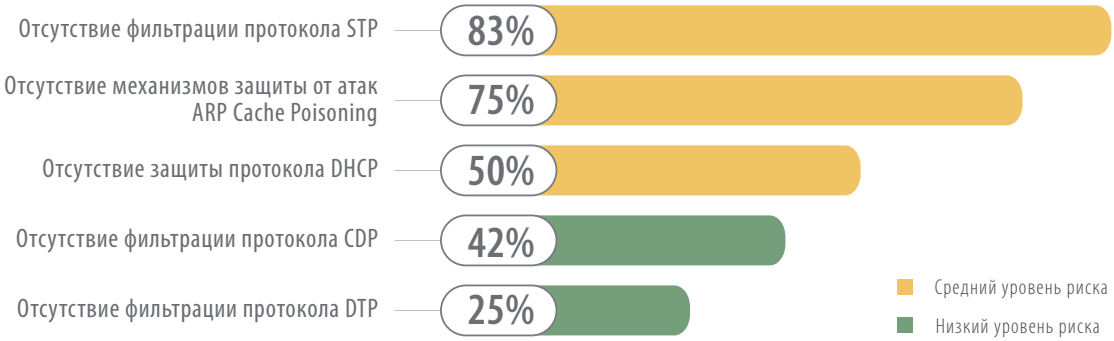


Лишь в 25% исследованных систем не было обнаружено словарных паролей учетных записей администраторов во внутренней сети. Пароли admin или P@ssw0rd являются самыми распространенными среди выявленных паролей администраторов и встречаются в 29% систем, где были обнаружены словарные учетные данные. При этом в 24% таких систем для привилегированных учетных записей было выявлено отсутствие пароля.

3.3.2. НЕДОСТАТКИ ЗАЩИТЫ СЛУЖЕБНЫХ ПРОТОКОЛОВ КАНАЛЬНОГО И СЕТЕВОГО УРОВНЕЙ

Наряду со слабостью парольной защиты широко распространены недостатки защиты различных служебных протоколов канального и сетевого уровней. Большинство уязвимостей этой категории связано с недостатками администрирования сетей, при этом атаки на некоторые из служебных протоколов, «забытых» на клиентских портах сетевого оборудования, могут привести к крайне серьезным последствиям для сети в целом.

НЕДОСТАТКИ ЗАЩИТЫ СЛУЖЕБНЫХ ПРОТОКОЛОВ КАНАЛЬНОГО И СЕТЕВОГО УРОВНЕЙ (ДОЛЯ УЯЗВИМЫХ СИСТЕМ)



Так, например, протокол STP является служебным протоколом, предназначенным для обнаружения ошибок коммутации. При наличии незащищенного трафика STP в пользовательских сегментах сети (что встречается в 83% рассмотренных компаний) внутренний нарушитель получает возможность управлять потоками передачи данных, изменяя топологию сети на канальном уровне. В результате злоумышленник получает возможность перехватывать конфиденциальную информацию, изменять данные в процессе передачи и блокировать сетевое взаимодействие, при этом для проведения атаки используются широко распространенные средства, опубликованные в открытом доступе. Таким образом, чтобы вызвать отказ в обслуживании сети, злоумышленнику не обязательно обладать ни высокой квалификацией, ни редким инструментарием. Любой пользователь, подключившийся к сети, способен полностью парализовать сетевое взаимодействие в соответствующем сегменте. А ведь для того, чтобы избежать подобных атак, достаточно обеспечить фильтрацию протокола STP на клиентских портах сетевого оборудования.

Другая распространенная уязвимость — отсутствие защиты от атак ARP Spoofing (ARP Cache Poisoning), которое встречается в 75% случаев и, также как и предыдущая уязвимость, позволяет перенаправлять сетевой трафик, реализуя атаки типа «человек посередине». Кроме того, атака ARP Cache Poisoning может привести к блокированию сетевого взаимодействия. Для того чтобы избежать подобных, крайне распространенных, атак следует использовать функции коммутаторов, предназначенные для защиты от данного типа атак (Dynamic ARP Inspection) и статические ARP-записи для критических узлов внутренней сети (шлюз по умолчанию, серверы).

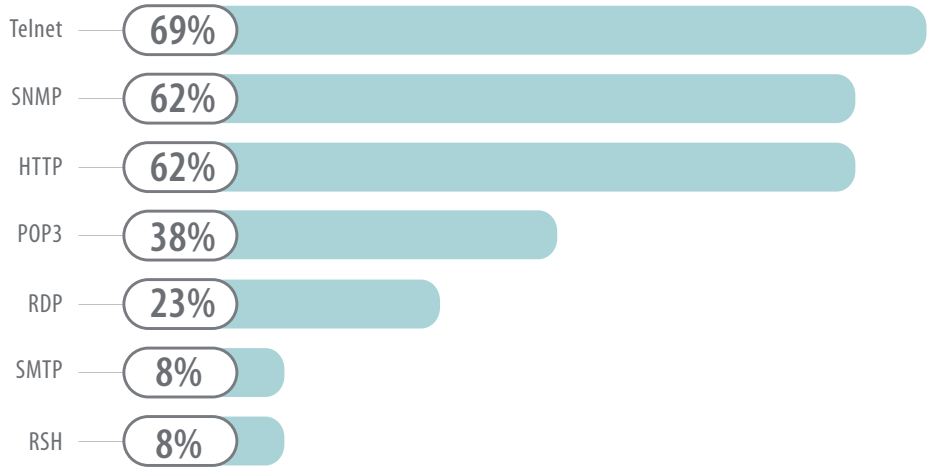
Помимо наиболее распространенных уязвимостей, описанных выше, а также недостатков защиты DHCP, CDP и DTP, в сетях крупных компаний в пользовательских сегментах иногда встречаются в незащищенном виде такие служебные протоколы, как HSRP, EIGRP и VRRP.

3.3.3. ИСПОЛЬЗОВАНИЕ ОТКРЫТЫХ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ

Использование открытых протоколов во внутренней сети, которое было выявлено в 75% систем, позволяет любому внутреннему злоумышленнику осуществить перехват чувствительной информации, в том числе учетных данных администраторов, в результате атаки «человек посередине», которая в свою очередь оказывается возможна также в 75% случаев из-за отсутствия защиты от ARP Spoofing (ARP Cache Poisoning). Комбинация этих двух недостатков позволяет перехватывать конфиденциальную информацию и изменять данные в процессе передачи.

Общая статистика использования открытых протоколов во внутренней сети по итогам проведенных в 2011—2012 годах исследований представлена на диаграмме.

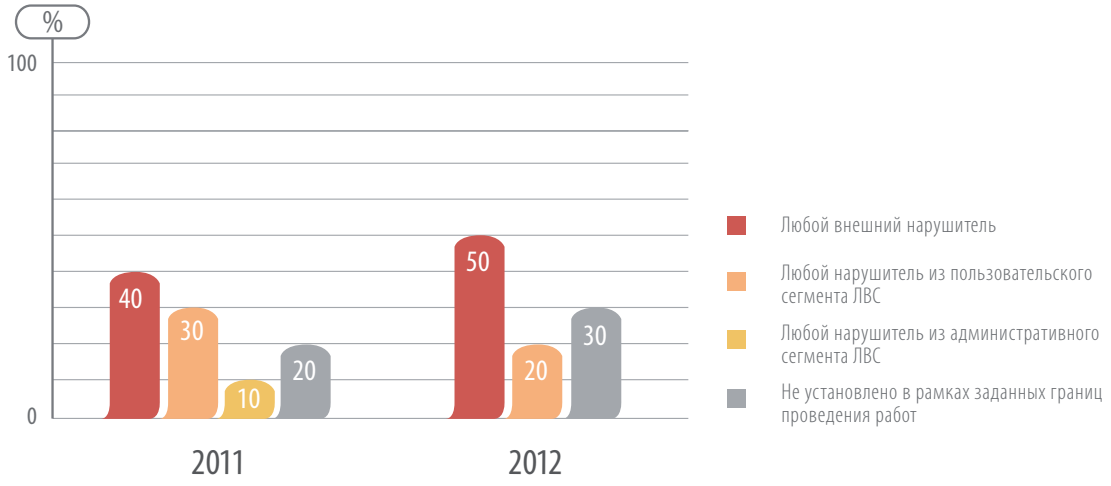
ПРОТОКОЛЫ, ИСПОЛЬЗУЕМЫЕ ВО ВНУТРЕННЕЙ СЕТИ (ДОЛИ СИСТЕМ)



4 СРАВНЕНИЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЙ НА ПРОНИКНОВЕНИЕ ЗА 2011 И 2012 ГОДЫ

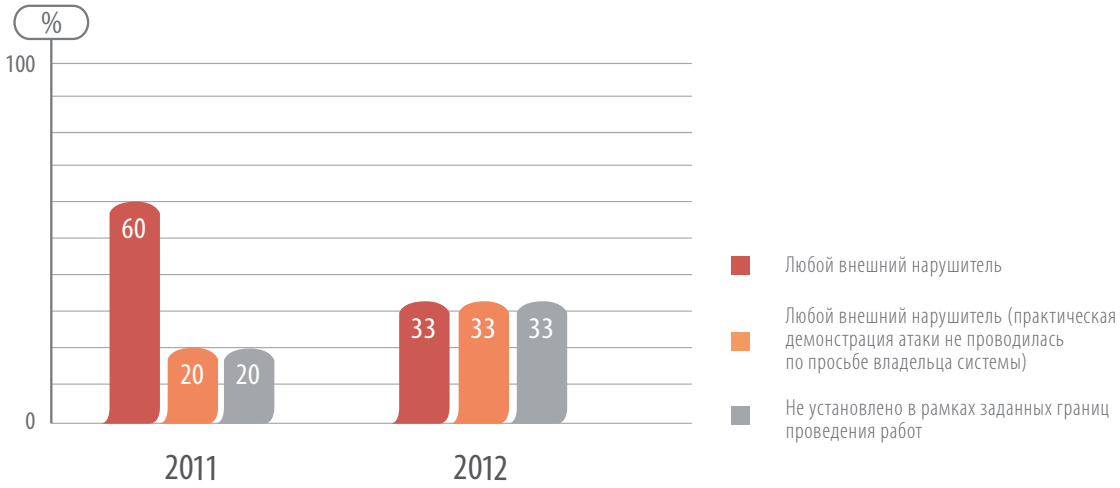
Доля систем, для которых в ходе работ не удалось получить полный контроль над критическими системами, выросла за последний год с 20% до 30%. Однако при этом увеличился и процент систем, для которых возможно получение контроля над критическими системами со стороны внешнего злоумышленника (в 2012 году это половина исследованных систем).

МИНИМАЛЬНЫЙ УРОВЕНЬ НАРУШИТЕЛЯ, НЕОБХОДИМЫЙ ДЛЯ ПОЛУЧЕНИЯ ПОЛНОГО КОНТРОЛЯ НАД КРИТИЧЕСКИМИ РЕСУРСАМИ



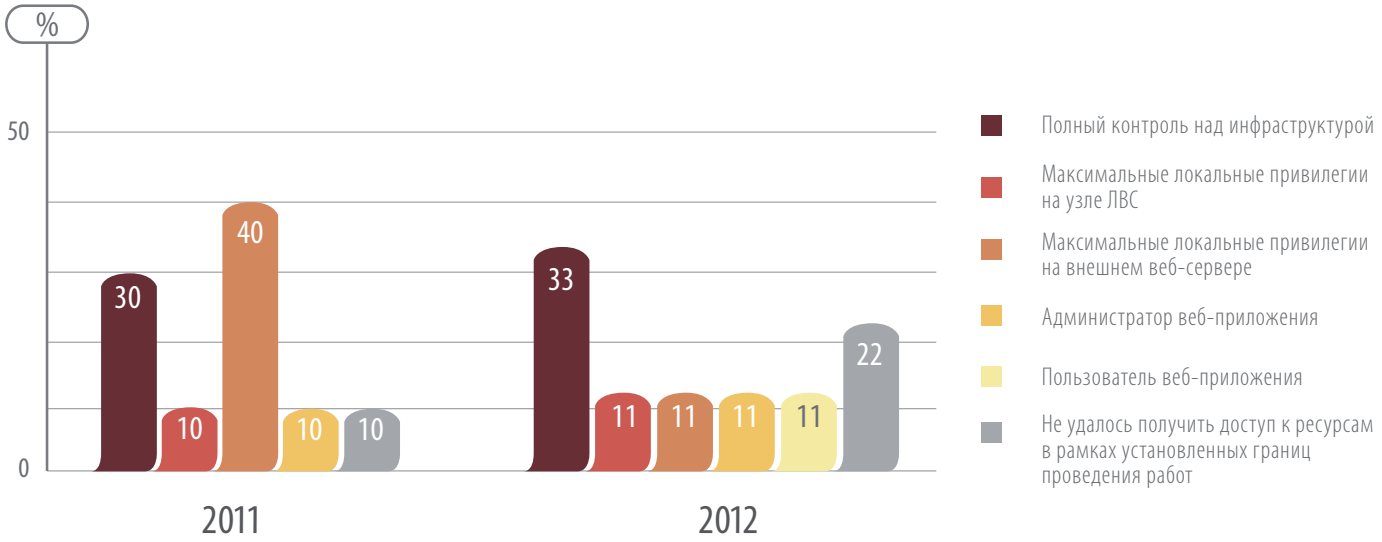
В 2012 году доля систем, в которых не удалось преодолеть сетевой периметр, также выросла — с 20% до 33%.

МИНИМАЛЬНЫЙ УРОВЕНЬ НАРУШИТЕЛЯ, НЕОБХОДИМЫЙ ДЛЯ ПРЕОДОЛЕНИЯ ПЕРИМЕТРА



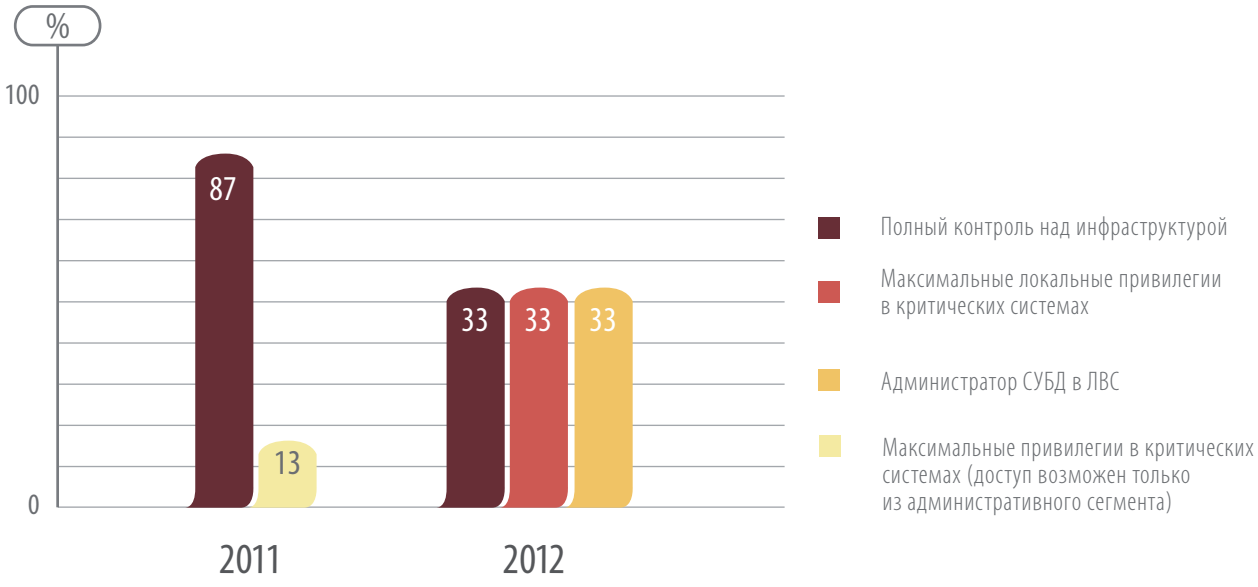
В 2012 году несколько увеличился уровень защищенности внешних веб-приложений корпоративных информационных систем с точки зрения атак со стороны внешнего злоумышленника с целью проникновения во внутреннюю сеть. Кроме того, доля систем с приемлемым уровнем защищенности по отношению к внешнему нарушителю выросла в два раза — с 10% до 22% (см. диаграмму ниже). Однако, несмотря на положительную динамику, в целом уровень защищенности от атак со стороны внешнего нарушителя остается крайне низким: как и в 2011 году, для трети систем возможно получение полного контроля над всей инфраструктурой со стороны внешнего злоумышленника.

УРОВЕНЬ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНЕШНЕГО НАРУШИТЕЛЯ



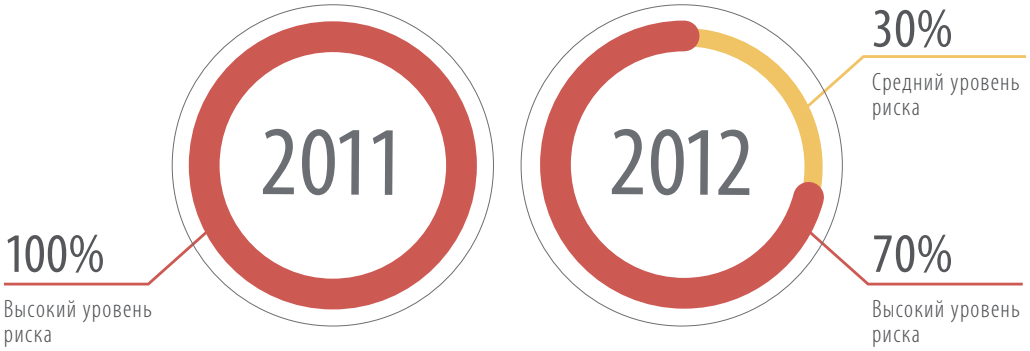
Доля систем, для которых удалось получить полный контроль над инфраструктурой со стороны внутреннего злоумышленника из пользовательского сегмента сети, уменьшилась, но при этом в 2012 году в каждой из рассмотренных систем удалось получить привилегированный доступ хотя бы к одному из узлов для данной категории нарушителя.

УРОВЕНЬ ПРИВИЛЕГИЙ, ПОЛУЧЕННЫХ ОТ ЛИЦА ВНУТРЕННЕГО НАРУШИТЕЛЯ



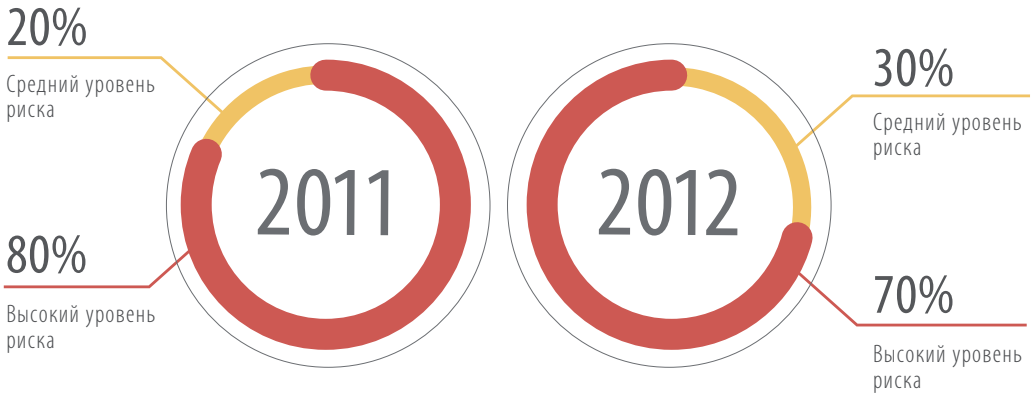
В 2012 году на треть меньше систем содержали уязвимости высого риска, однако оставшиеся системы содержали уязвимости среднего уровня риска. Максимальный уровень значения базовой оценки критичности обнаруженных уязвимостей по методике CVSS (Common Vulnerability Scoring System) для всех систем, рассмотренных в 2011 году, достигает максимального значения 10. В 2012 году для всех 70% систем, где были обнаружены критические уязвимости, максимальное значение базовой метрики CVSS уязвимостей также достигло 10.

МАКСИМАЛЬНЫЙ УРОВЕНЬ РИСКА ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ



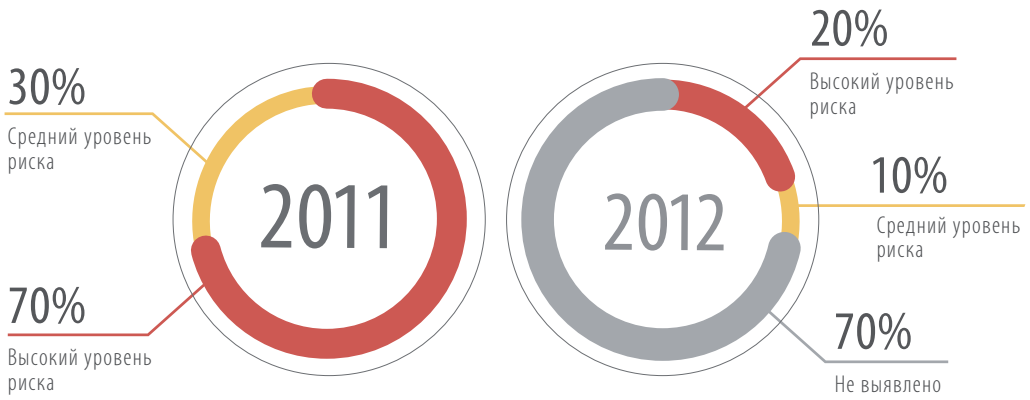
Доля систем, содержащих уязвимости конфигурации высокого уровня риска, сократилась с 80% до 70%. Однако остальные системы по-прежнему содержат уязвимости конфигурации среднего уровня риска.

МАКСИМАЛЬНЫЙ УРОВЕНЬ РИСКА УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С НЕДОСТАТКАМИ КОНФИГУРАЦИИ



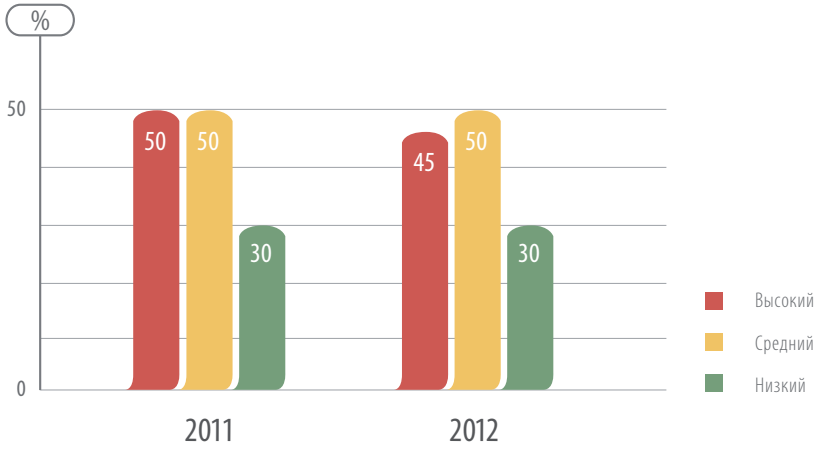
Доля систем, содержащих критические уязвимости в программном обеспечении, сократилась с 70% до 20%. В 70% систем в 2012 году в ходе работ по тестированию на проникновение не было выявлено уязвимостей, связанных с неустановленными обновлениями. Однако, стоит отметить, что в ряде случаев отсутствие уязвимостей данного класса означает выявление других, более перспективных векторов атаки с использованием недостатков конфигурации.

МАКСИМАЛЬНЫЙ УРОВЕНЬ РИСКА УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ОТСУТСТВИЕМ ОБНОВЛЕНИЙ



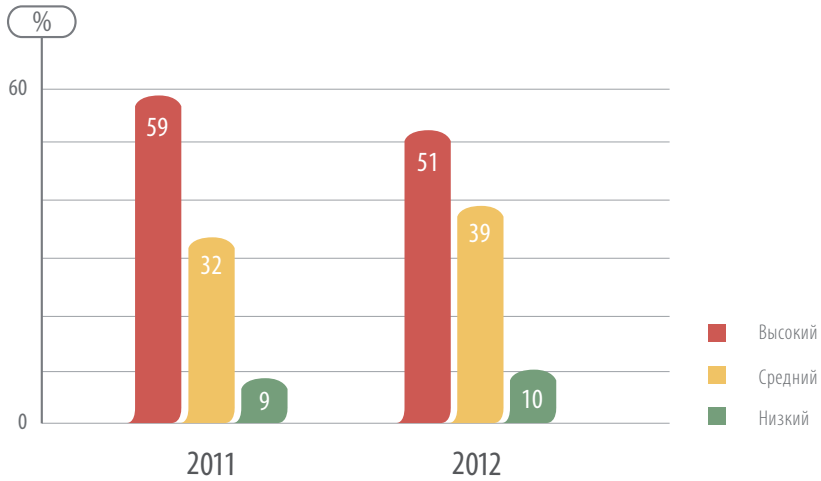
Незначительная тенденция к повышению уровня защищенности просматривается в снижении доли систем, содержащих уязвимости высокой степени риска. В 2012 году доля таких систем снизилась с 50% до 45%. Доли систем, подверженных уязвимостям средней и низкой степени риска, остались на уровне 2011 года и составили 50% и 30% соответственно.

ДОЛЯ УЯЗВИМЫХ СИСТЕМ ПО УРОВНЮ РИСКА УЯЗВИМОСТЕЙ



Доля обнаруженных уязвимостей высокой степени риска в 2012 году снизилась на 8%, но осталась на достаточно высоком уровне в 51%. Таким образом, более половины всех обнаруженных уязвимостей, как в 2011, так и в 2012 году, характеризуются высоким уровнем риска. Доли уязвимостей среднего и низкого уровней риска также изменились незначительно.

ДОЛЯ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ ДЛЯ КАЖДОГО УРОВНЯ РИСКА



5 ИСПОЛЬЗУЕМЫЕ ВЕКТОРЫ АТАК

В рамках проведенного исследования специалистами Positive Technologies была дана средняя оценка уровня защищенности рассмотренных систем относительно различных векторов проникновения.

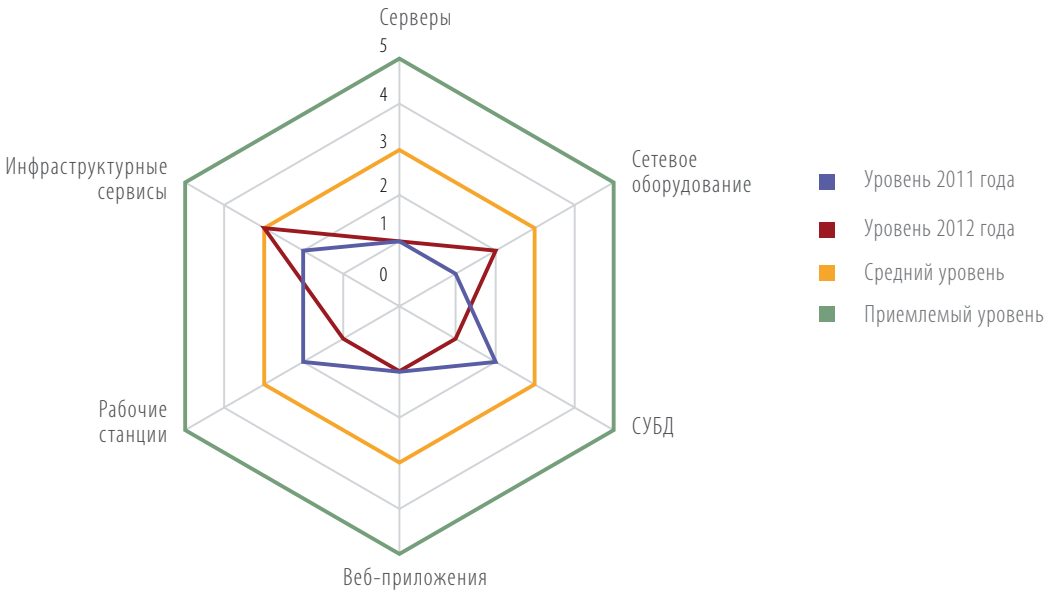
Векторы проникновения были классифицированы в зависимости от компонентов системы, эксплуатация уязвимостей позволяла получить несанкционированный доступ к ресурсам. Были рассмотрены следующие виды систем:

- инфраструктурные сервисы (электронная почта, службы каталогов),
- серверы,
- сетевое оборудование,
- СУБД,
- веб-приложения,
- рабочие станции.

Оценка уровня защищенности рассчитывалась по следующему принципу: по каждому направлению выставлялась оценка от 0 до 5, где 0 соответствует крайне низкому уровню защищенности (уязвимости данной категории позволяют напрямую получить доступ к критическим ресурсам либо присутствует множество критических уязвимостей), а оценка 5 соответствует приемлемому уровню защищенности (уязвимостей не обнаружено, средства защиты реализованы корректно).

На диаграмме ниже представлена динамика изменения средних уровней защищенности различных компонентов систем в 2011 и 2012 годах.

ИЗМЕНЕНИЕ СРЕДНИХ УРОВНЕЙ ЗАЩИЩЕННОСТИ
РАЗЛИЧНЫХ КОМПОНЕНТОВ СИСТЕМ С 2011 ПО 2012 ГОДЫ



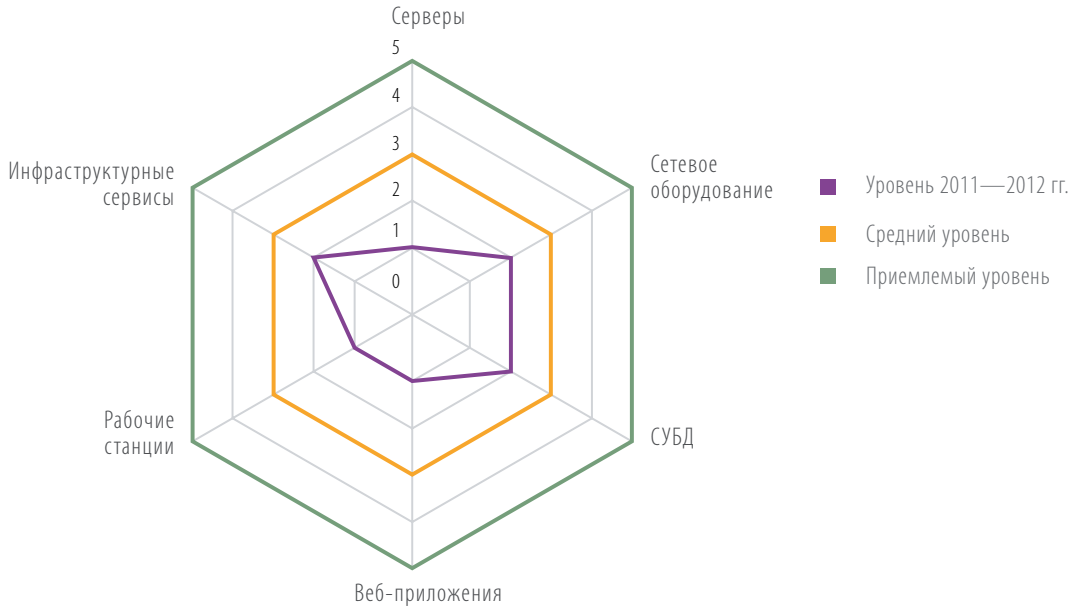
Наиболее уязвимыми компонентами систем в 2011 году стали серверы, сетевое оборудование и веб-приложения. Уязвимости именно в этих компонентах позволили осуществить несанкционированный доступ к критическим компонентам систем, в отдельных случаях такой доступ был получен напрямую при эксплуатации данных уязвимостей. Ни один из компонентов систем, исследованных в 2011 году, не достиг даже средней оценки уровня защищенности.

В 2012 году наиболее уязвимыми оказались серверы, рабочие станции, веб-приложения и СУБД. Данным компонентам системы был присвоен низкий уровень защищенности. По сравнению с 2011 годом несколько улучшилась ситуация в области защиты инфраструктурных сервисов и сетевого оборудования, однако о достижении даже уровня «выше среднего» говорить пока не приходится.

Динамика изменения средних уровней защищенности отдельных компонентов систем за 2011—2012 годы показывает, что уровни защищенности серверов и веб-приложений остаются по-прежнему низкими. Снижение среднего уровня защищенности наблюдается для СУБД и рабочих станций.

На графике представлено общее соотношение средних уровней защищенности различных компонентов систем за 2011—2012 годы.

ОБЩЕЕ СООТНОШЕНИЕ СРЕДНИХ УРОВНЕЙ ЗАЩИЩЕННОСТИ РАЗЛИЧНЫХ КОМПОНЕНТОВ СИСТЕМ



Общее соотношение средних уровней защищенности отдельных компонентов исследованных систем показывает низкий уровень защищенности серверов и веб-приложений, а также рабочих станций пользователей по итогам двух лет. Уровень защищенности по всем направлениям не превышает значения «ниже среднего».

Согласно статистическим данным, наиболее распространенной является уязвимость «Использование слабых паролей». В большинстве случаев получение доступа к критическим ресурсам на серверах, рабочих станциях и СУБД связано именно с подбором простых паролей. Данный факт отражен и в результатах оценки уровня защищенности систем с точки зрения различных механизмов защиты, приведенных в разд. 6.

6 ОЦЕНКА МЕХАНИЗМОВ ЗАЩИТЫ

В рамках проведенного исследования специалистами Positive Technologies была дана средняя оценка уровня защищенности рассмотренных систем относительно используемых механизмов защиты.

Механизмы были классифицированы в зависимости от выявленных недостатков в реализации защиты, которые были использованы в ходе тестирований на проникновение. Были рассмотрены следующие основные виды механизмов защиты:

- сетевая безопасность,
- разграничение доступа,
- криптографическая защита,
- управление конфигурациями,
- управление уязвимостями и обновлениями,
- управление учетными записями и паролями,
- антивирусная защита.

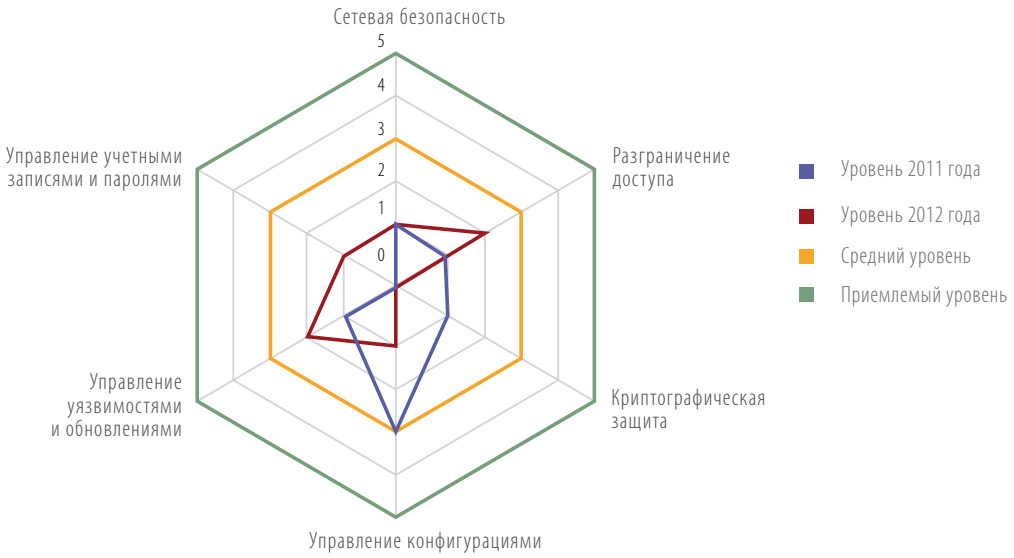
Оценка уровня защищенности основывается на экспертном мнении специалистов и ранжируется от 0 до 5. Уровни защищенности распределяются аналогично классификации, представленной в разд. 5.

На графике представлено соотношение средних уровней защищенности систем в зависимости от механизма защиты в 2011 и 2012 годах.

Наиболее серьезные недостатки в 2011 году были выявлены для механизмов управления учетными записями и паролями. Учитывая результаты аналогичного исследования, описанного в разд. 6, где показаны средние уровни защищенности отдельных подсистем, стоит отметить, что уязвимости, связанные с учетными записями пользователей, встречаются чаще всего именно в сервисах уровня инфраструктуры (в частности, в доменах на базе Active Directory, службах электронной почты), серверных компонентах и веб-приложениях. Велика доля подобных уязвимостей и для СУБД и рабочих станций. Наряду с крайне низким уровнем реализации механизмов управления учетными записями и паролями во множестве систем были выявлены серьезные недостатки реализации криптографической защиты, механизмов разграничения доступа и отсутствием актуальных обновлений безопасности. Ни в одной из категорий оценка уровня защищенности не превышает средней.

В 2012 году средний уровень защищенности систем относительно механизмов криптографической защиты снизился до крайне низкой отметки: практически везде используются открытые протоколы передачи данных, важная информация хранится в открытом виде. Незначительно улучшились показатели в отношении механизмов управления актуальными версиями систем, разграничения доступа и антивирусной защиты.

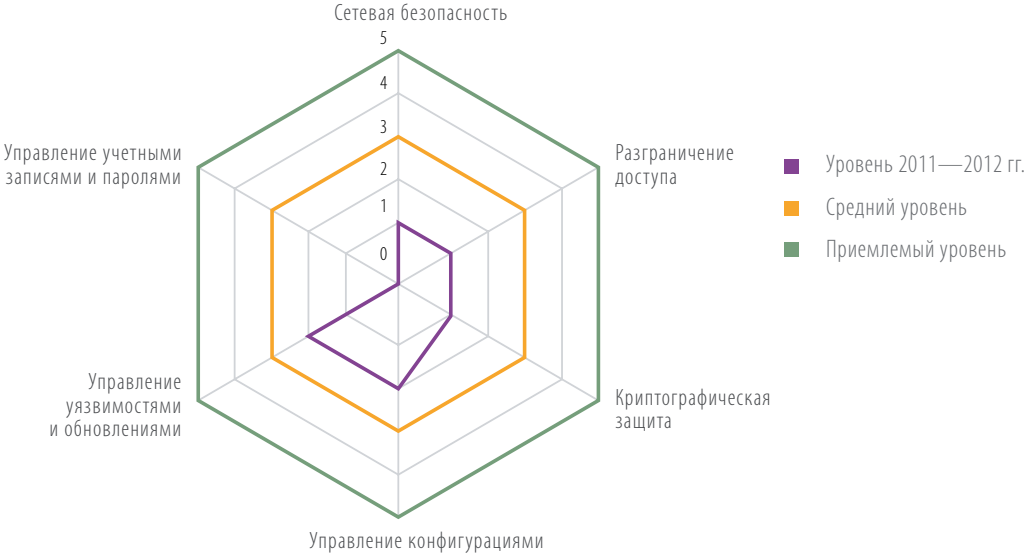
ИЗМЕНЕНИЕ СРЕДНИХ УРОВНЕЙ ЗАЩИЩЕННОСТИ СИСТЕМ (ПО МЕХАНИЗМАМ ЗАЩИТЫ)



Динамика изменения уровней защищенности систем относительно различных механизмов защиты отражает снижение уровня обеспечения криптографической защиты в системах. При этом наблюдается значительное повышение уровня защищенности с точки зрения механизмов управления конфигурациями. Незначительное улучшение наблюдается в остальных видах данной классификации. Однако стоит отметить, что общий уровень защищенности для всех видов механизмов защиты по итогам 2012 года также не превышает среднего значения.

В целом за 2011—2012 годы общий уровень защищенности по различным направлениям защиты не превысил оценку «ниже среднего», при этом наиболее критическая ситуация наблюдается в области управления учетными записями и паролями.

СООТНОШЕНИЕ СРЕДНИХ УРОВНЕЙ ЗАЩИЩЕННОСТИ СИСТЕМ В ЗАВИСИМОСТИ ОТ МЕХАНИЗМА ЗАЩИТЫ



Недостатки парольной политики в большинстве исследованных систем позволили получить доступ к критическим ресурсам и повысить привилегии до максимальных. Слабые пароли повсеместно использовались как для учетных записей обычных пользователей, так и для привилегированных. Практически во всех исследованных системах были встречены подобные уязвимости.

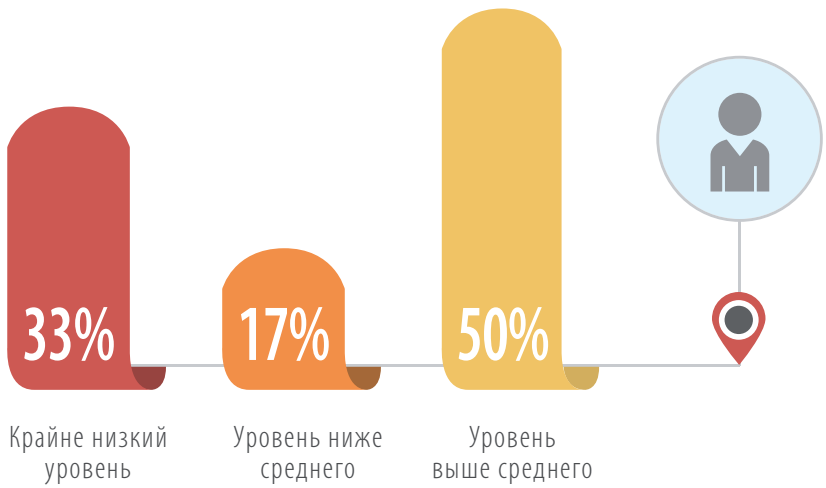
7 РЕЗУЛЬТАТЫ ОЦЕНКИ ОСВЕДОМЛЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ В ВОПРОСАХ ИБ

В рамках работ по тестированию на проникновение корпоративных информационных систем, проводимых в 2011—2012 годах, в ряде случаев осуществлялись проверки осведомленности пользователей систем в вопросах обеспечения информационной безопасности.

Работы по оценке осведомленности пользователей проводились посредством серии согласованных с заказчиком атак, эмулирующих реальную деятельность злоумышленников и отслеживание реакции пользователей на них. Тестирование проводилось различными методами по индивидуальным сценариям, для взаимодействия с сотрудниками заказчика могли использоваться электронная почта, системы обмена мгновенными сообщениями, социальные сети и телефонная связь. В данном исследовании рассматриваются лишь результаты по наиболее распространенному виду тестирования: рассылки по электронной почте. Проверки заключались в рассылке электронных сообщений с вложением в виде файла либо содержащих ссылку на внешний источник. Отслеживались факты перехода по предложенной ссылке, факты запуска исполняемого файла, приложенного к письму или ввода учетных данных при эмуляции фишинговой атаки, а также факты вступления в диалог с автором рассылок. Как правило, рассылка писем по электронной почте осуществлялась якобы от лица сотрудника организации.

Оценка уровня осведомленности производилась на основании экспертного мнения специалистов Positive Technologies по результатам проведенных работ. Общая статистика осведомленности сотрудников в вопросах информационной безопасности представлена на диаграмме.

ОЦЕНКА УРОВНЯ ОСВЕДОМЛЕННОСТИ ПОЛЬЗОВАТЕЛЕЙ В ВОПРОСАХ ИБ



В каждой из исследованных компаний сотрудники переходили по предлагаемым ссылкам, запускали предложенные файлы и вводили учетные данные. Среди всех исследованных за два года компаний в 33% случаев уровень осведомленности сотрудников в вопросах информационной безопасности был оценен как крайне низкий. В таких системах пользователи осуществляли переход по предоставленным в письмах ссылкам, а также ввод учетных данных при реализации фишинговой атаки более чем в 30% случаев. По сценарию проведения работ данные рассылки осуществлялись от лица авторизованного пользователя (например, автором рассылки мог выступать якобы сотрудник технической поддержки или службы по управлению персоналом компании). В качестве одного из наиболее ярких примеров можно назвать исследование по оценке осведомленности сотрудников, в результате которого 44% всех пользователей из фокус-группы совершили переход по предоставленной ссылке, и 40% участников фокус-группы ввели учетные данные в предложенную форму авторизации.

В 17% случаев уровень осведомленности пользователей в вопросах информационной безопасности был оценен как «ниже среднего». Половина всех исследованных компаний показала уровень осведомленности сотрудников выше среднего.

На диаграмме представлено среднее отношение событий безопасности к общему числу сообщений, отправленных при проведении анализа защищенности в 2011 и 2012 годах. В среднем в 19% случаев пользователи осуществляли переход по предоставленной в письме ссылке на внешний ресурс, и почти все из них (18%) осуществляли ввод учетных данных либо запуск предложенного ПО. Таким образом, практически пятая часть всех пользователей, включенных в соответствующие фокус-группы при проведении работ по анализу защищенности, проявила недостаточную осведомленность в вопросах информационной безопасности. При этом в среднем 1% участников фокус-групп предпринимал попытки вступить в диалог с автором рассылок.

ДОЛЯ ЗАФИКСИРОВАННЫХ СОБЫТИЙ ОТ ОБЩЕГО КОЛИЧЕСТВА ОТПРАВЛЕННЫХ СООБЩЕНИЙ

Подобные действия пользователей могут привести к заражению рабочих станций вредоносным программным обеспечением. Злоумышленник получает учетные данные при реализации фишинговой атаки и может осуществить доступ к критическим ресурсам сети с правами данного пользователя. Кроме того, при запуске файла или переходе по предоставленной ссылке злоумышленник зачастую может провести эксплуатацию уязвимостей прикладного программного обеспечения. Так, в процессе исследования осведомленности практически во всех случаях зафиксированы факты использования сотрудниками уязвимых версий программного обеспечения, в том числе тех, для которых существуют общеизвестные и общедоступные эксплойты.

Учитывая полученные результаты, можно сделать вывод о важности разработки и внедрения эффективных мер по повышению осведомленности сотрудников в вопросах обеспечения информационной безопасности. Результаты проверок, полученные в 2011 и 2012 годах, свидетельствуют о том, что атаки методами социальной инженерии могут быть серьезным оружием в руках злоумышленника.

8 ЗАКЛЮЧЕНИЕ

Проведенное исследование продемонстрировало, насколько уязвимы современные корпоративные информационные системы. Наиболее существенные проблемы были выявлены в централизованных системах уровня инфраструктуры (таких так Microsoft Active Directory), серверных компонентах, СУБД и веб-приложениях. Именно через эти системы удавалось в большинстве случаев получать доступ к критическим ресурсам, а также преодолевать внешний периметр сети. Важно отметить, что в ходе проведения работ в 15% исследованных систем были обнаружены следы взлома системы злоумышленниками.

Самые распространенные уязвимости ресурсов сетевого периметра связаны с недостатками парольной политики и уязвимостями веб-приложений. При этом многие атаки оказываются возможными из-за доступности интерфейсов управления серверами и сетевым оборудованием (SSH, Telnet, RDP, веб-интерфейсов) из внешних сетей. Для внутрисетевых ресурсов характерны недостатки парольной политики, некорректной настройки сетевого оборудования, а также разграничения доступа. Кроме того, передача и хранение чувствительной информации в открытом виде во многих случаях значительно упрощали развитие атак.

Другим существенным недостатком в обеспечении информационной безопасности систем стал низкий уровень осведомленности пользователей в вопросах информационной безопасности. Это говорит о необходимости повышения качества образования сотрудников, а также периодических проверок и тестирований.

Основным выводом по результатам проведенного исследования является недостаточный уровень обеспечения безопасности корпоративных информационных сетей независимо от сферы экономики и типа системы. В большинстве рассмотренных систем полученные результаты свидетельствуют об отсутствии или некачественной реализации процессов обеспечения информационной безопасности. Так, множественные ошибки в веб-приложениях говорят о неэффективности процесса аудита информационной безопасности в области веб-приложений, а не устанавливаемые в течение нескольких лет обновления — об отсутствии процесса управления уязвимостями и обновлениями.

В целом для обеспечения должного уровня безопасности требуется комплексный подход и периодическое проведение анализа защищенности, в том числе в виде тестирования на проникновение, которое позволяет на практике оценить возможность проведения атак на важнейшие ресурсы компании.