СТАТИСТИКА УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2014

POSITIVE TECHNOLOGIES

2015

Оглавление

1. Введение....3

2. Резюме....5

3. Исходные данные....8

4. Статистика за 2014 год. Сравнительный анализ с результатами за 2013 год....10

4.1. Общие результаты тестов на проникновение....10

4.2. Результаты анализа защищенности сетевого периметра....13

4.3. Анализ защищенности ресурсов внутренней сети....22

5. Используемые векторы атак....30

6. Оценка механизмов защиты....31

7. Результаты оценки осведомленности пользователей в вопросах информационной безопасности....32

8. Заключение....34

1. Введение

Уровень развития современных технологий позволяет компаниям создавать сложные корпоративные инфраструктуры, объединяющие в себе множество подсистем. Зачастую архитектура сети настолько сложна, что обеспечить ее полную защиту становится непосильной задачей даже для крупных корпораций, выделяющих солидный бюджет на защиту своих ресурсов. Проведение анализа защищенности позволяет заблаговременно выявить наиболее уязвимые компоненты системы и устранить недостатки в обеспечении защиты.

Тестирование на проникновение представляет собой один из методов проведения анализа защищенности информационных систем. В рамках тестирования на проникновение моделируется поведение потенциального нарушителя, действующего как со стороны сети Интернет, так и из сегментов внутренней сети компании. Такой подход к анализу защищенности позволяет на практике оценить реальный уровень безопасности системы и выявить недостатки используемых механизмов защиты.

В данном отчете представлена ежегодная статистика по результатам работ по тестированию на проникновение, которые проводились компанией Positive Technologies в 2014 году, а также сравнительный анализ данных 2014 года и результатов аналогичного исследования за 2013 год. Отчет позволяет оценить динамику развития современных корпоративных систем с точки зрения обеспечения информационной безопасности на примере проанализированных крупных компаний.

Для исследования были выбраны 18 систем, протестированных в 2014 году. В группу вошли российские и зарубежные организации. В обзоре рассматриваются системы наиболее крупных государственных и коммерческих компаний (в том числе входящих в рейтинг крупнейших в мире компаний 2014 года Fortune Global 500[1] и в рейтинг крупнейших компаний в России в 2014 году по объему реализации продукции по версии агентства «Эксперт»[2]). При выборе систем учитывалась информативность результатов тестирований на проникновение с точки зрения статистики. Так, результаты проектов по анализу защищенности, которые по просьбе владельцев систем проводились на значительно ограниченном количестве узлов и не отражают состояние защищенности корпоративной информационной системы в целом, не были включены в настоящее исследование. Кроме того, во избежание частичного раскрытия информации об уязвимостях, в отчет не включались некоторые системы, владельцы которых публично заявили о фактах проведения работ силами Positive Technologies в указанный период.

[1] http://fortune.com/global500/

[2] http://expert.ru/ratings/rejting-krupnejshih-kompanij-rossii-2014-po-ob_emu-realizatsii-produktsii/

2. Резюме

Сводные результаты:

+ В 2014 году 94% исследованных систем содержали уязвимости, позволяющие получить полный контроль над теми или иными критически важными ресурсами, такими как служба Active Directory, ERP-системы, системы электронной почты, системы управления сетевым оборудованием. При этом в 67% систем получение полного контроля над критически важными ресурсами возможно от лица внешнего злоумышленника, действующего со стороны сети Интернет.

+ Почти для половины исследованных компаний (44%) возможно получение полного контроля над всей информационной инфраструктурой организации от лица внешнего атакующего. Еще в 39% организаций для получения такого уровня доступа достаточно иметь доступ к внутренней сети. Такие результаты близки к результатам 2013 года.

Недостатки защиты сетевого периметра:

+ В 73% систем, в отношении которых было проведено внешнее тестирование на проникновение, внешний нарушитель, действующий со стороны сети Интернет, способен получить доступ к узлам внутренней сети без использования методов социальной инженерии. Если же атакующий использует и технические методы, и социальную инженерию, то доступ к сети извне можно получить в 87% случаев.

+ В 80% случаев, когда атака осуществляется из внешних сетей, злоумышленник может получить максимальные привилегии в тех или иных важных для бизнеса системах; а в 53% систем — получить полный контроль над всей инфраструктурой компании.

+ В среднем для преодоления сетевого периметра внешнему атакующему требуется осуществить эксплуатацию двух различных уязвимостей; при проведении атаки без использования методов социальной инженерии в 74% случаев достаточно иметь среднюю или низкую квалификацию.

+ В 60% случаев вектор проникновения во внутреннюю сеть основывается на уязвимостях в коде веб-приложений. Так, уязвимость типа «Внедрение операторов SQL» встречается в 67% систем, а «Загрузка произвольных файлов» — в 40% систем. В целом различные уязвимости веб-приложений были обнаружены в 89% исследованных систем. Общий уровень защищенности в этой области остается низким, как и в 2013 году.

+ Так же, как и в предыдущий период, использование словарных идентификаторов и паролей является одной из самых распространенных уязвимостей, она была обнаружена на сетевом периметре в 87% исследованных систем, причем в 67% компаний простые пароли использовались и для привилегированных учетных записей. В каждой второй организации (53% от общего числа) для доступа к публичным веб-приложениям используются словарные учетные данные.

+ Уязвимости, получившие наибольшую известность в 2014 году, — Heartbleed и Shellshock, на практике оказались не столь распространены, как изначально опасались СМИ: во многом благодаря широкому распространению информации большинство крупных компаний оперативно устанавливали обновления. Однако, эти действия зачастую были выборочными: устаревшее ПО, содержащее критические уязвимости, было выявлено в 78% систем. Средний возраст наиболее устаревших неустановленных обновлений по системам, где такие уязвимости были обнаружены, составил 73 месяца (более 6 лет).
+ По сравнению с 2013 годом средний уровень защищенности сетевого периметра практически не изменился. При этом для проведения атак внешнему злоумышленнику все чаще требуется более низкая квалификация: низкой квалификации теперь достаточно для успешной атаки на 61% систем, тогда как в 2013 этот показатель составлял 46%. Преодоление периметра, как и в 2013 году, в среднем требует эксплуатации всего двух уязвимостей.

Недостатки защиты внутренней сети:

+ Для всех систем, где тестирование проводилось со стороны внутренней сети, установлено, что внутренний нарушитель, находящийся в пользовательском сегменте сети, может так или иначе расширить свои привилегии и получить несанкционированный привилегированный доступ к критически важным ресурсам (банковским системам, ERP-системам и другим важным для бизнеса компонентам сети). При этом в 78% случаев внутренний нарушитель может получить полный контроль над всей информационной инфраструктурой организации.

+ Более чем в половине случаев (56%) внутреннему атакующему достаточно низкой квалификации для получения доступа к критически важным ресурсам. В среднем, при наличии доступа во внутреннюю сеть, для получения контроля над критическими ресурсами злоумышленнику требуется эксплуатация трех различных уязвимостей, что хуже показателя прошлого года, когда атака насчитывала в среднем 5 этапов.

+ Наиболее распространенной уязвимостью ресурсов внутренней сети по-прежнему является использование слабых паролей, которые были обнаружены во всех без исключения системах, в отношении которых проводились данные работы. При этом в каждой системе выявлены простые пароли администраторов. Следующие по распространенности — недостаточный уровень защиты привилегированных учетных записей, хранение важных данных в открытом виде и недостатки антивирусной защиты. Уязвимости каждой из этих категорий были обнаружены в 88% систем.

+ Уровень защищенности внутренних сетей понизился по сравнению с 2013 годом: понизилось среднее число этапов атаки, требуемая для проведения успешной атаки квалификация злоумышленника также стала ниже. Несмотря на некоторые улучшения в отдельных областях (например, повысился средний уровень сетевой безопасности), применяемых мер защиты все так же недостаточно для противодействия злоумышленникам. При этом, как правило, для успешной атаки достаточно использовать широко распространенные и давно известные типы уязвимостей.

Недостатки осведомленности сотрудников в вопросах информационной безопасности:

+ При оценке осведомленности пользователей в вопросах информационной безопасности с использованием методов социальной инженерии были обнаружены те или иные недостатки во всех исследованных системах. В 67% компаний уровень осведомленности пользователей был оценен как низкий или крайне низкий. В этих системах свыше 20% 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 ссылке, при этом 15% испытуемых загрузили исполняемые файлы либо ввели свои учетные данные в предлагаемой форме аутентификации.

+ Уровень осведомленности сотрудников в вопросах информационной безопасности оценивается существенно ниже по сравнению с предыдущим годом, когда в каждой третьей протестированной системе уровень осведомленности оценивался как приемлемый (в 2014 году ни одна компания не достигла этого показателя).

3. Исходные данные

В исследование были включены корпоративные информационные системы 18 крупных российских и зарубежных компаний. Участниками, как и в 2013 году, стали организации различных сфер экономики: банковский и финансовый сектор, лидеры в сфере промышленности, транспортная компания, одна из крупнейших телекоммуникационных компаний, ведущие компании в области информационных технологий, а также государственная организация. Наибольшее количество проектов относилось к сфере промышленности (44%), на втором месте — банковский сектор, к которому относилась почти треть всех рассмотренных систем (28%).

Более половины исследованных систем были территориально распределенными и включали множество дочерних компаний и филиалов, расположенных в разных городах и странах. В большинстве систем, для которых проводилось внешнее тестирование на проникновение, количество активных узлов, доступных на сетевом периметре, исчислялось сотнями.

Как и в предыдущие годы, в рамках проведенных работ целью тестирований на проникновение в ряде случаев становились сети автоматизированных систем управления технологическими процессами (АСУ ТП). Важность проведения анализа защищенности данных систем и своевременного устранения выявленных уязвимостей подтверждают результаты исследования «», проведенного Positive Technologies.

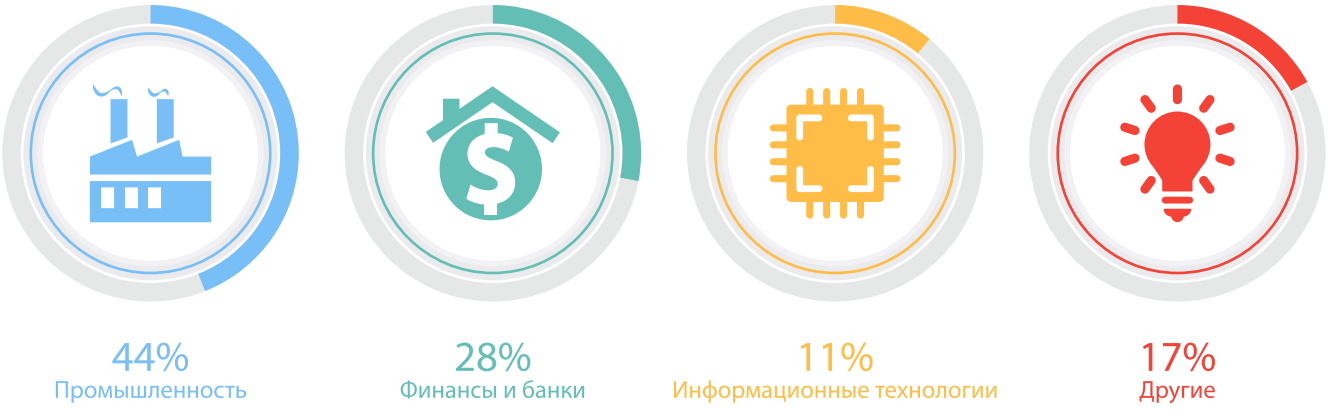


Рис. 1. Распределение исследованных систем по отраслям

В состав оказанных услуг для рассматриваемых систем входили несколько видов тестирования на проникновение — внешнее, внутреннее и комплексное (последнее включало как внешнее, так и внутреннее тестирование).

Ровно половина компаний воспользовалась услугой внешнего тестирования на проникновение. В отношении каждой третьей системы в 2014 году было проведено комплексное тестирование, которое 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. Внутреннее тестирование на проникновение осуществляется из заданного сегмента внутренней сети (как правило, рассматривается подключение к пользовательскому сегменту). Отдельная услуга по внутреннему тестированию на проникновение была оказана для 17% рассмотренных систем.

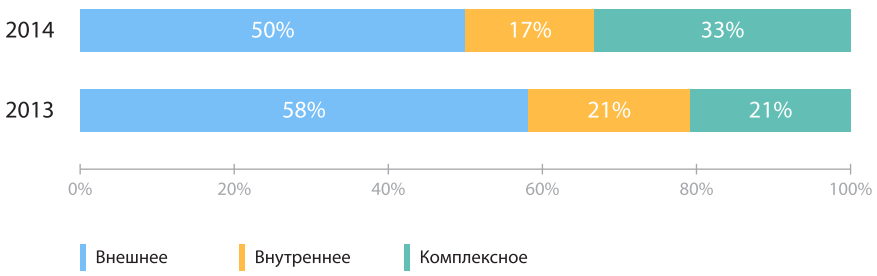


Рис. 2. Виды тестирования на проникновение (доли систем)

Для каждой третьей компании (33%) в рамках работ по анализу защищенности была предоставлена услуга по оценке осведомленности сотрудников в вопросах информационной безопасности. В рамках таких работ проводились различные проверки, эмулирующие распространенные атаки, основанные на методах социальной инженерии (например, фишинговые рассылки). Статистические данные об уровне осведомленности пользователей приведены в разд. 7.

4.1. Общие результаты тестов на проникновение

В 2014 году 94% систем, включенных в данное исследование, содержали уязвимости, позволяющие получить полный контроль над отдельными критически важными ресурсами, такими как служба Active Directory, ERP-системы, системы электронной почты, системы управления сетевым оборудованием. При этом в 67% случаев получение полного контроля над важнейшими ресурсами оказалось возможно от лица любого внешнего злоумышленника. Еще в 27% случаев для получения контроля над важными ресурсами достаточно иметь доступ к пользовательскому сегменту внутренней сети.

Рис. 3. Минимальный уровень доступа нарушителя, необходимый для получения полного контроля над отдельными критическими ресурсами

Почти для половины исследованных компаний (44%) возможно получение полного контроля над всей IT-инфраструктурой от лица внешнего атакующего. Еще в 39% организаций для получения такого контроля достаточно иметь доступ к внутренней сети. Данная статистика близка к результатам 2013 года.

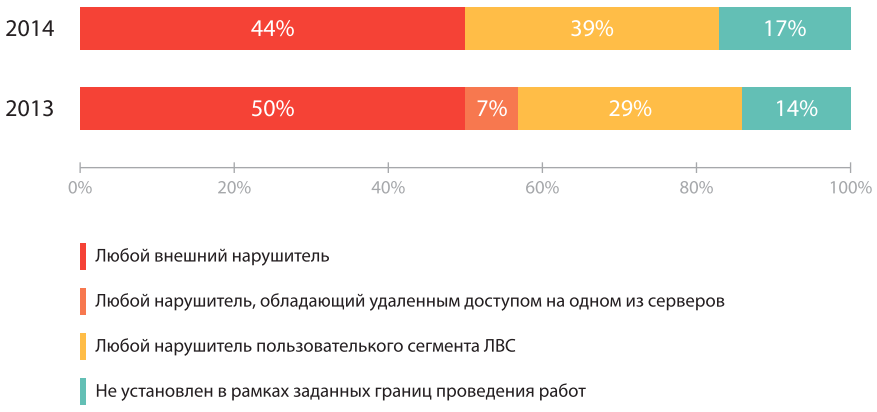


Рис. 4. Минимальный уровень доступа нарушителя, необходимый для получения полного контроля над всей инфраструктурой

Практически все исследованные в 2014 году системы оказались подвержены уязвимостям высокой степени риска, лишь одна система не содержала ни критических уязвимостей, ни уязвимостей средней степени риска. В 2013 году критические уязвимости также были выявлены более чем в 90% исследованных систем, при этом уязвимости средней степени риска были выявлены абсолютно во всех системах, в отличие от 2014 года.

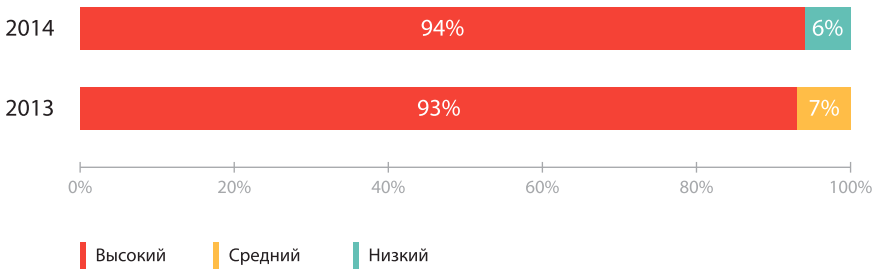


Рис. 5. Доля систем по максимальному уровню уязвимостей

Аналогичная ситуация прослеживается для недостатков, обусловленных некорректной конфигурацией: только одна система (6%) не содержала уязвимостей средней и высокой степени риска, связанных с недостатками конфигурации. Практически во всех системах были выявлены критически уязвимости данной категории — как в 2014, так и в 2013 году.

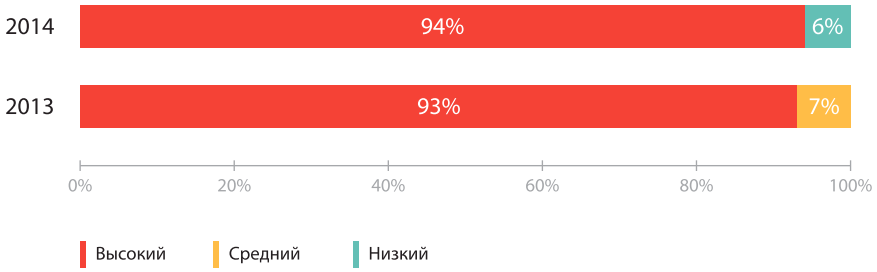


Рис. 6. Максимальный уровень риска уязвимостей, связанных с недостатками конфигурации (доли систем)

Большинство систем, исследованных в 2014 году (78%), содержали доступные потенциальному злоумышленнику критические уязвимости, связанные с использованием устаревших версий операционных систем и прикладного программного обеспечения, что существенно хуже результатов предыдущего года, когда таких систем было немногим более половины. Средний возраст наиболее устаревших неустановленных обновлений по системам, где такие уязвимости были обнаружены, составляет 73 месяца (более шести лет), тогда как в 2013 году данный показатель был более чем в два раза ниже — 32 месяца. В трех системах из 18 в 2014 году все еще можно было встретить критическую уязвимость ОС Windows шестилетней давности MS08-067 (CVE-2008-4250), активно используемую не только хакерами, но и сетевым червем Conficker.

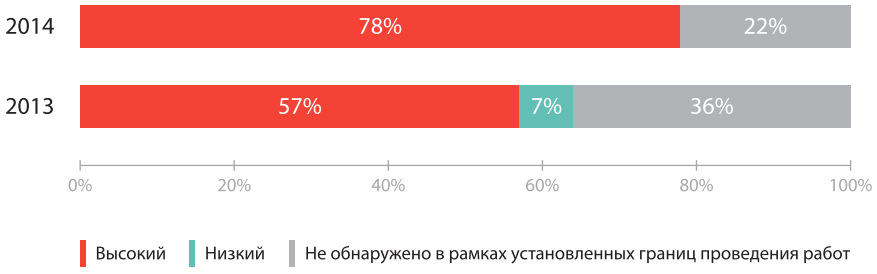


Рис. 7. Максимальный уровень риска уязвимостей, связанных с отсутствием обновлений безопасности (доля уязвимых систем)

В 22% систем в 2014 году не было обнаружено уязвимостей, связанных с отсутствием актуальных обновлений ПО, что на 14% ниже уровня предыдущего года. Поскольку внешнее тестирование на проникновение осуществляется с привилегиями, идентичными привилегиям потенциального атакующего, и не включает в себя полный аудит всех ресурсов сети, в действительности уязвимости, связанные с отсутствием актуальных обновлений, все же могут присутствовать во всех исследованных системах.

Практически для каждой исследованной в 2014 году организации (89%) на ресурсах сети были выявлены уязвимости, связанные с ошибками в коде веб-приложений. При этом более чем в половине компаний (61% от общего числа) присутствовали подобные уязвимости высокой степени риска, такие как «Внедрение операторов SQL» или «Загрузка произвольных файлов». И вновь стоит отметить, что в действительности уязвимости в веб-приложениях могли присутствовать во всех исследованных корпоративных сетях, однако в связи с тем, что тестирование на проникновение проводится методом черного ящика, эти недостатки могли остаться невыявленными в границах проведения работ.

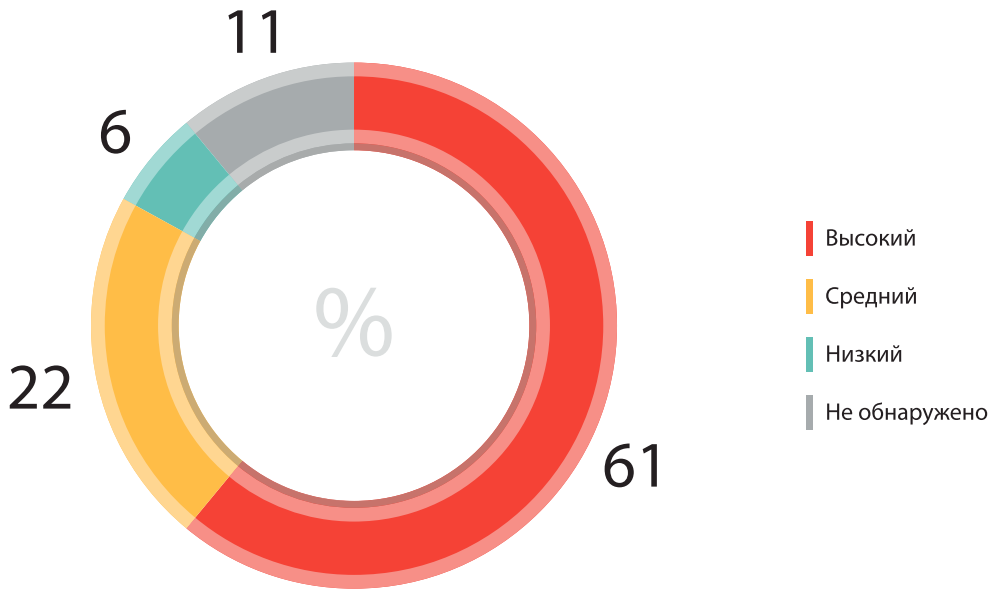


***Рис. 8.** Максимальный уровень риска уязвимостей, связанных с ошибками в коде веб-приложений (доля уязвимых систем)*

4.2. Результаты анализа защищенности сетевого периметра

В 87% систем, для которых проводилось внешнее тестирование на проникновение, была выявлена возможность получения доступа к ресурсам локальной вычислительной сети из внешних сетей. Для 73% компаний получение доступа ко внутренним сетям возможно со стороны любого внешнего нарушителя, не использующего методы социальной инженерии, что в точности соответствует уровню 2013 года. В двух системах из 15 преодоление периметра со стороны внешнего атакующего оказалось возможно только с использованием методов социальной инженерии, при этом в одной из них преодоление периметра только техническими методами оказалось возможно со стороны администратора официального веб-сайта компании.

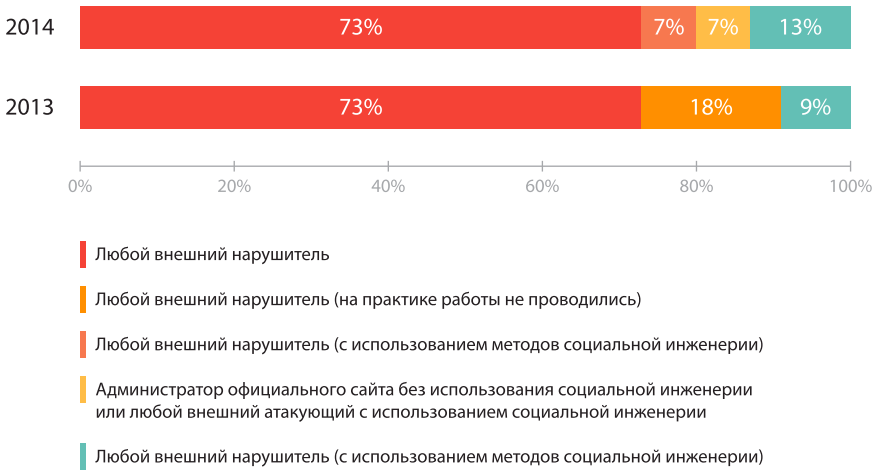


Рис. 9. Минимальный уровень нарушителя, достаточный для преодоления периметра

В большинстве случаев (87%) для преодоления периметра злоумышленнику достаточно иметь средний или низкий уровень квалификации, при этом в одной из 15 протестированных систем преодоление периметра требовало и вовсе тривиальных действий со стороны нарушителя — подбора словарного пароля администратора для доступного из внешней сети интерфейса RDP. В 13% случаев для преодоления периметра необходимо применить методы социальной инженерии в отношении сотрудников компании. В 2013 году сложность преодоления периметра в целом была оценена выше: тривиальная сложность атаки была присвоена 9% систем, низкая — 37%, средняя — 36%.

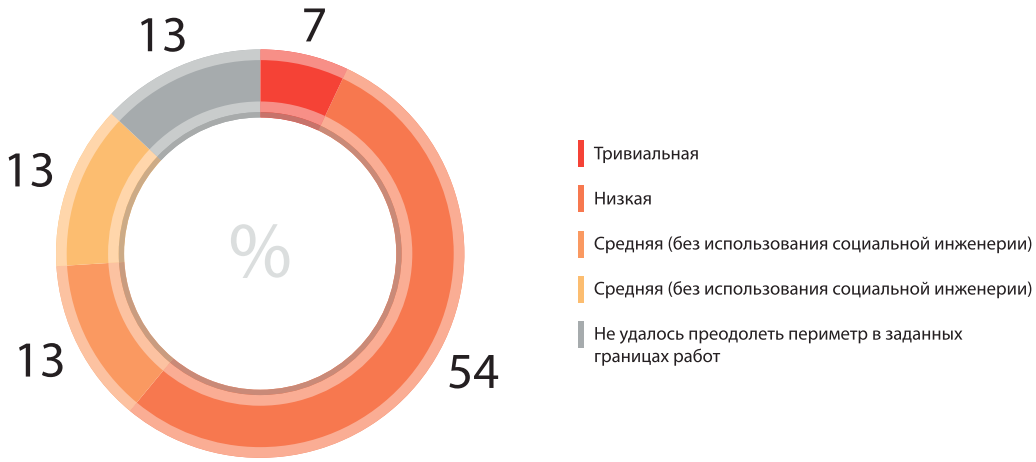


Рис. 10. Сложность преодоления периметра

Согласно полученным данным, для преодоления периметра необходима эксплуатация в среднем двух различных уязвимостей, как и в 2013 году. Однако при этом более чем для половины систем, где в 2014 году удалось преодолеть периметр (6 из 11), это было сделано в результате эксплуатации всего одной уязвимости. В 2014 году в большинстве случаев (60%) вектор проникновения во внутреннюю сеть был основан на эксплуатации уязвимостей в веб-приложениях, тогда как доля проникновений с использованием словарных паролей и уязвимостей в устаревших версиях ПО сократилась по сравнению с 2013 годом. В среднем, для каждой из систем, где удалось преодолеть сетевой периметр без использования социальной инженерии, в границах проведения работ было выявлено по два вектора проникновения во внутреннюю сеть.

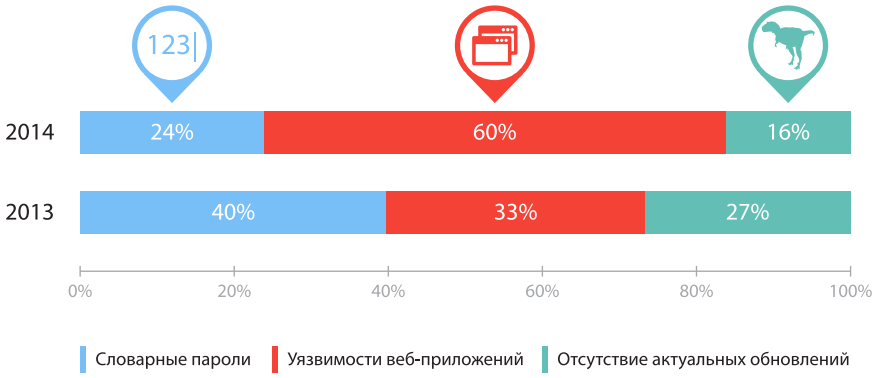


Рис. 11. Векторы атак для преодоления сетевого периметра

Наиболее распространенные уязвимости на сетевом периметре это:

+ наличие доступных из внешних сетей интерфейсов удаленного доступа и управления сетевым оборудованием и серверами, которые должны быть доступны только ограниченному числу администраторов;
+ использование словарных паролей, в том числе установленных производителями по умолчанию и пустых;
+ использование открытых протоколов передачи данных (Telnet, FTP, HTTP и др.).

Каждая из этих проблем встретилась более чем в 80% исследованных систем.

Аналогичные уязвимости были наиболее распространены и в предыдущем году. В 2013 году наиболее распространенной являлась уязвимость высокого уровня риска, связанная с использованием словарных паролей. В 2014 году данная уязвимость заняла вторую строчку рейтинга, но при этом доля систем, в которых она была обнаружена, почти не изменилась. Практически в каждой системе (93%) выявлены доступные любому пользователю внешней сети интерфейсы управления серверами и сетевым оборудованием.

Рис. 12. Наиболее распространенные уязвимости на сетевом периметре

4.2.1. Доступные интерфейсы управления оборудованием (1)

На сетевом периметре компаний из внешних сетей бывает доступно множество различных служб, многие из которых связаны с дополнительными рисками.

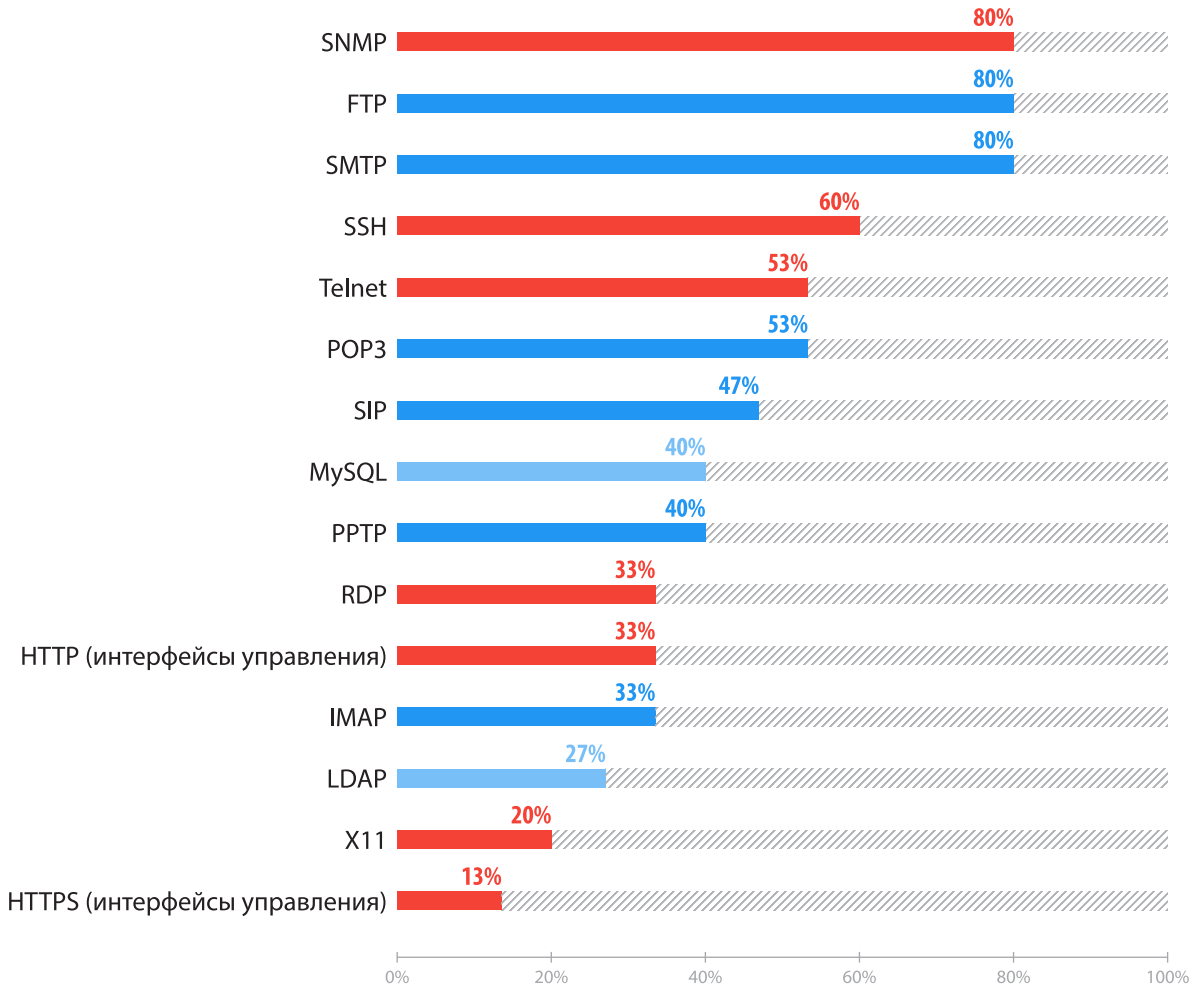


Рис. 13. Статистика использования различных протоколов, в том числе интерфейсов удаленного доступа, на сетевом периметре (доли систем)

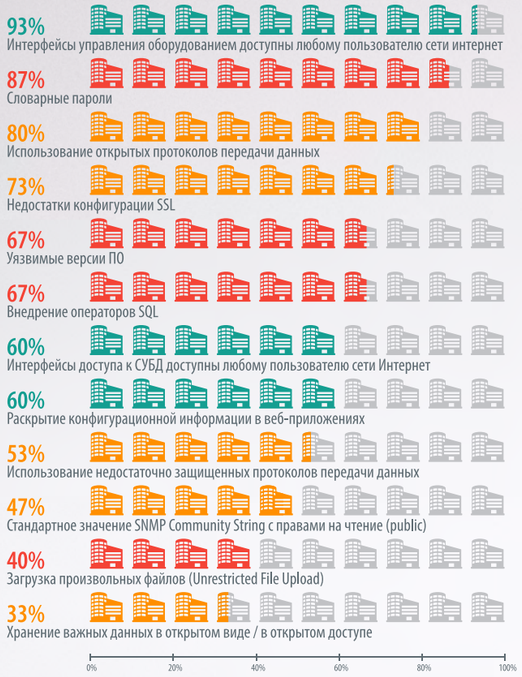
Доля уязвимостей, связанных с доступностью интерфейсов управления серверами и сетевым оборудованием из сети Интернет, возросла за последний год с 82 до 93%. Заметно увеличилось (с 64 до 80%) количество систем, на сетевом периметре которых доступна для подключения любому пользователю сети Интернет служба SNMP. Зачастую администраторы оставляют заводские настройки оборудования со стандартными значениями строки подключения SNMP Community String. Стандартное значение SNMP Community String с правами на чтение (public) было обнаружено на сетевом периметре почти половины (47%) исследованных систем, с правами на запись (private) — в одной системе.

Несколько снизилась доля систем, где были выявлены доступные для подключения из сети Интернет интерфейсы управления оборудованием по протоколам SSH (с 73 до 60%) и Telnet (с 64 до 53%). Однако, при этом возросли доли доступных интерфейсов MySQL (с 27 до 40%), LDAP (с 18 до 27%); интерфейс X11, не фигурировавший в прошлогоднем отчете, занял долю в 20%.

POSITIVE TECHNOLOGIES

СТАТИСТИКА УЯЗВИМОСТЕЙ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ 2014

Наиболее распространенные уязвимости на сетевом периметре



Векторы атак для преодоления сетевого периметра

Уровень привилегий, полученных от лица внешнего нарушителя (доли систем)

Уязвимости, получившие наибольшую известность в 2014 г., – Heartbleed и Shellshock, на практике оказались не столь распространены, как изначально опасались СМИ: во многом благодаря широкому распространению информации большинство крупных компаний оперативно устанавливали обновления. Однако эти действия зачастую были выборочными: устаревшее ПО, содержащее критические уязвимости, было выявлено в 78% систем.

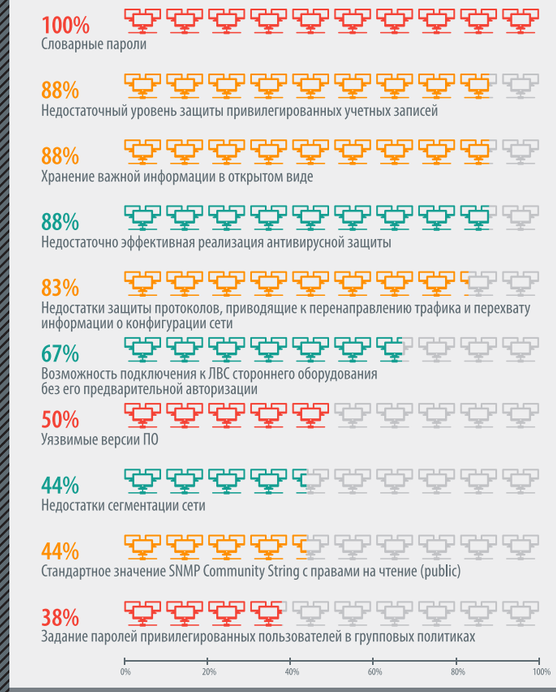
Сложность преодоления периметра

Критически важные ресурсы

Сложность получения доступа к критическим ресурсам со стороны внутреннего нарушителя

3 ШАГА требуется в среднем для получения доступа к критически важным системам

Наиболее распространенные уязвимости внутренней сети



Уровень привилегий, полученных от лица внутреннего нарушителя (доли систем)

4.2.2. Словарные идентификаторы и пароли (2)

В ходе тестирования на проникновение получение паролей пользователей может осуществляться различными способами. Это может быть подбор паролей для учетных записей по умолчанию (таких как Administrator, admin, root); подбор паролей для учетных записей, имена которых удалось получить за счет эксплуатации различных уязвимостей на предыдущих этапах; подбор паролей на базе хэш-значений; восстановление учетных данных из зашифрованных значений и другие методы. В даном исследовании при анализе используемых паролей рассматривались все пароли, полученные в ходе тестирования на проникновение тем или иным образом, при этом словарными признавались пароли, которые могут быть в короткие сроки подобраны злоумышленником путем перебора по распространенным словарям при знании лишь идентификатора пользователя.

По сравнению с предыдущим годом данная уязвимость опустилась на второе место в рейтинге наиболее распространенных, при этом доля уязвимых систем в 2014 году почти не изменилась по сравнению с 2013 годом и составила 87%. На сетевом периметре наиболее распространены словарные учетные данные для доступа к веб-приложениям, которые были обнаружены в каждой второй системе; лидер в данной категории — учетная запись «admin» с паролем «admin». На втором месте по распространности на внешних ресурсах в 2014 году оказались словарные пароли для домена Active Directory и электронной почты, которые обнаружены в 40% исследованных систем.

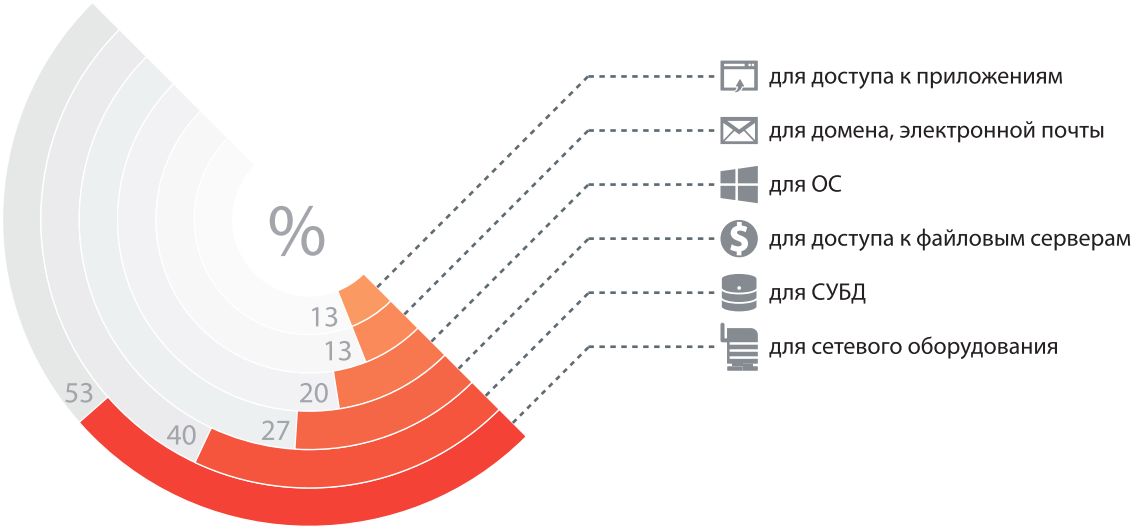


Рис. 14. Словарные пароли на сетевом периметре

При этом в 67% всех систем на сетевом периметре выявлены словарные идентификаторы и пароли привилегированных пользователей, что зачастую приводило к получению доступа к внутренней сети.

4.2.3. Использование открытых протоколов (3)

Как и прежде, использование открытых протоколов передачи данных остается распространной уязвимостью в корпоративных информационных системах и занимает третью строчку рейтинга уязвимостей сетевого периметра. По сравнению с 2013 годом доля уязвимых систем остается на прежнем уровне и составляет 80%. Выявлено множество систем с доступными службами FTP, Telnet и другими открытыми протоколами. Благодаря им потенциальный злоумышленник получает возможность перехвата передаваемой информации, в том числе учетных данных привилегированных пользователей.

4.2.4. Недостатки конфигурации SSL (4)

В 2014 году было выявлено множество уязвимостей средней степени риска, связанных с недостатками конфигурации SSL. Данная уявимость встречалась в 73% систем, и заняла 4-ю строчку рейтинга наиболее распространенных. К недостаткам данной категории относится использование самоподписанных или устаревших сертификатов SSL. Используя уязвимости в конфигурации SSL, нарушитель может осуществить атаку «человек посередине» и перехватить передаваемые по данному протоколу чувствительные данные.

4.2.5. Отсутствие актуальных обновлений безопасности (5-6)

В 2014 году доля уязвимостей, связанных с отсутствием актуальных обновлений безопасности, осталась на уровне 2013 года и составила 67%. Наибольшее количество уязвимостей данной категории в этом году выявлено в веб-серверах, используемых на периметре: 67% от общего числа исследованных организаций уязвимы. В 40% компаний подобные уязвимости обнаружены в прикладном ПО, таком как PHP и OpenSSL. Для такой же доли систем были выявлены уязвимости в устаревших версиях различных веб-приложений, поставляемых вендорами «как есть», — систем управления содержимым сайтов (CMS), систем телеконференцсвязи. Примером может служить загрузка произвольных файлов в CMS Joomla (CVE-2013-5576), которая позволяет нарушителю загрузить веб-интерпретатор командной строки на сервер и выполнять команды ОС — и которая позволила преодолеть периметр при тестировании на проникновение в одной из организаций.

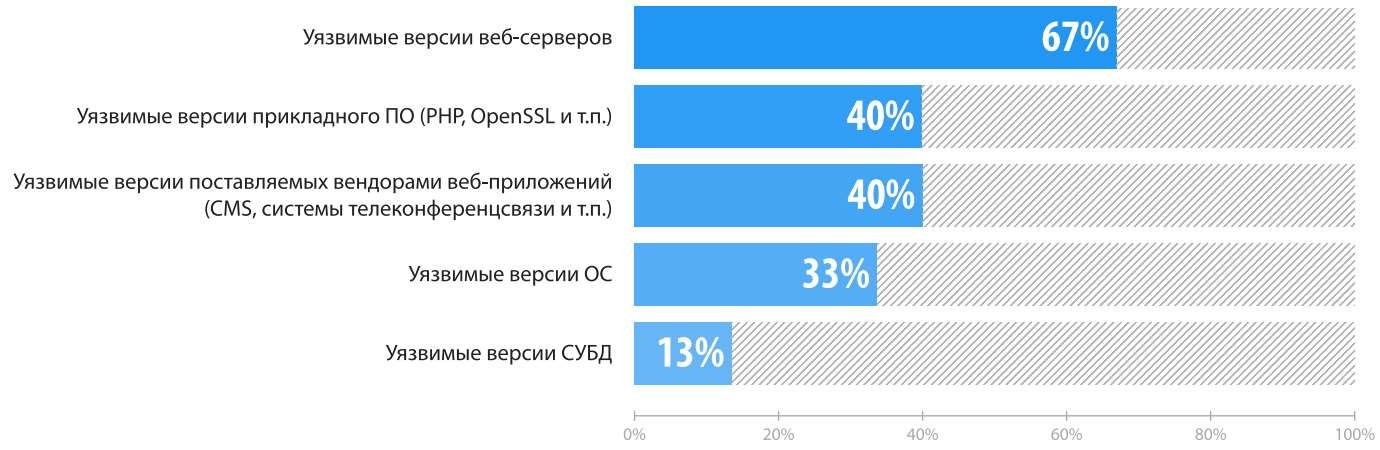


Рис. 15. Устаревшие версии ПО на периметре систем

Уязвимость Heartbleed (CVE-2014-0160), информация о которой была опубликована в апреле 2014 года, позволяет нарушителю использовать ошибки библиотеки OpenSSL и получать чувствительные данные из памяти серверного процесса. Данная уязвимость встретилась в 33% протестированных после ее выхода систем, при этом для двух из этих систем тестирование проводилось вскоре после публикации информации об уязвимости — в апреле и мае. Уже с июня уязвимых систем почти не встречалось. Однако в тех случаях, когда уязвимость присутствовала, она несла серьезные риски для системы. Так, в результате проведения данной атаки на одном из проектов было получено множество учетных данных клиентов компании для доступа к важному бизнес-приложению.

В 2014 году также было объявлено о критической уязвимости Shellshock (CVE-2014-6271), которая позволяет удаленному нарушителю использовать недостатки в обработке команд интерпретатором Bash версий ниже 4.3 и выполнять произвольные команды ОС, например с помощью CGI. На практике, в отличие от Heartbleed, в ходе тестов на проникновение данная уязвимость не эксплуатировалась. Это может быть связано с тем, что наличие уязвимости в большей степени зависит от конфигурации ресурса, что были установлены исправляющие ошибку обновления либо с тем, что уязвимые ресурсы не вошли в область работ.

4.2.6. Внедрение операторов SQL (5-6)

Как и в 2013 году, уязвимость типа «Внедрение операторов SQL», связанная с ошибками в коде веб-приложения и позволяющая получить несанкционированный доступ к системе управления базами данных (СУБД) в обход логики приложения, занимает высокую позицию в рейтинге и встречается в 67% организаций. Другая критическая уязвимость в веб-приложениях — «Загрузка произвольных файлов» — опустилась с 6-й на 11-ю строчку рейтинга, однако по-прежнему встречается часто: уязвимы оказались 40% компаний.

В целом в 2014 году уровень защищенности веб-приложений продолжил понижаться, что прослеживается в результатах исследования «Статистика уязвимостей веб-приложений в 2014 г.», проведенного Positive Technologies.

4.3. Анализ защищенности ресурсов внутренней сети

После получения доступа к внутреней сети внешний злоумышленник имеет возможности для развития атаки. При этом получение полного контроля над различными критически важными ресурсами было продемонстрировано от лица внешнего нарушителя для 80% исследованных систем (то есть, почти во всех случаях, когда удалось преодолеть сетевой периметр). Эти показатели практически идентичны результатам, полученным в 2013 году.

Рис. 16. Уровень привилегий, полученных от лица внешнего нарушителя (доли систем)

При тестировании от лица внутреннего злоумышленника (например, рядового сотрудника, находящегося в пользовательском сегменте сети) во всех случаях удалось получить максимальные привилегии в критически важных системах (в банковских, ERP-системах и других важных для бизнеса компонентах сети). Полный контроль над инфраструктурой компании был получен в 78% систем, что также близко к показателям предыдущего года.

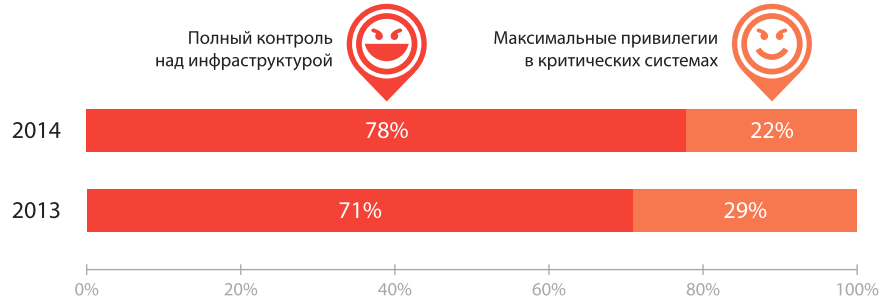


Рис. 17. Уровень привилегий, полученных от лица внутреннего нарушителя (доли систем)

Сложность получения максимальных привилегий в критически важных системах значительно снизилась по сравнению с предыдущим годом. В половине случаев (56%) получение полного контроля над такими ресурсами требует незначительных усилий со стороны нарушителя. В остальных системах (44%) сложность получения доступа к критическим ресурсам оценена как средняя. В 2013 году в 17% систем для получения максимальных привилегий потребовалось реализовать сложные векторы атак, а также использовать ранее неизвестные уязвимости (уязвимости нулевого дня), что требует высокой квалификации атакующего.

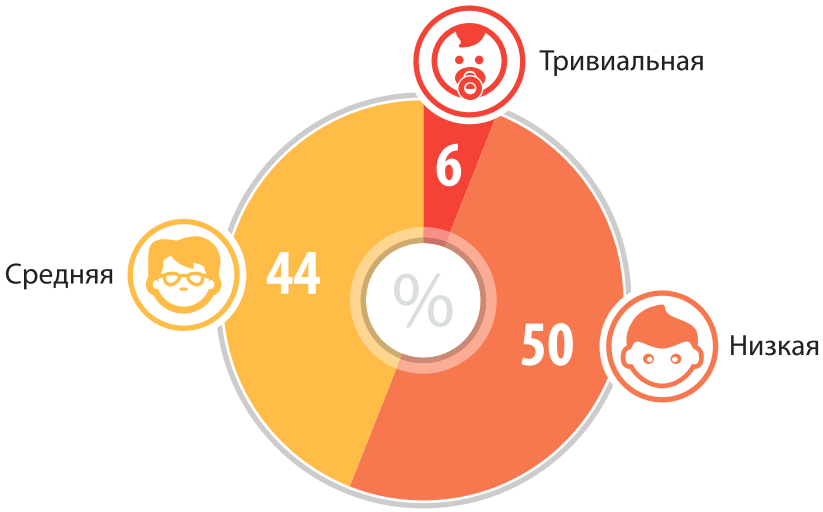


Рис. 18. Сложность получения доступа к критическим ресурсам со стороны внутреннего нарушителя

В среднем при наличии доступа во внутреннюю сеть для контроля над критически важными ресурсами злоумышленнику требуется эксплуатация трех уязвимостей, что на два шага меньше, чем в предыдущий год, и на четыре шага меньше, чем в 2012 году. Самая длинная атака в 2014 году насчитывала 6 этапов.

Наиболее распространенный сценарий развития атаки во внутренней сети по-прежнему состоит всего из трех этапов и близок к сценарию 2013 года:

1. Получение доступа к ресурсам домена Active Directory с правами пользователя в результате подбора учетных данных.
2. Получение максимальных локальных привилегий на рабочих станциях пользователей в результате получения пароля локального администратора из настроек групповой политики в общей сетевой директории контроллера домена.
3. Загрузка на рабочие станции специализированного ПО и получение с его помощью учетных данных администратора домена, сессия которого активна на узле.

В целом в 2014 году оказались наиболее распространены уязвимости, связанные с использованием словарных учетных данных: они были обнаружены во всех без исключения системах, при этом во всех случаях были выявлены простые пароли привилегированных пользователей. Кроме того, были широко распространены такие ошибки, как недостаточная защита привилегированных учетных записей, хранение важной информации в открытом виде и недостаточная эффективность антивирусной защиты. Эти три уязвимости встретились в 88% систем и занимают в рейтинге 2014 года строки со второй по четвертую.

Отсутствие защиты и фильтрации различных служебных протоколов, приводящее к перенаправлению и перехвату сетевого трафика, а также к раскрытию важных данных, выявлено в 83% рассмотренных систем и заняло пятое место среди наиболее распространенных уязвимостей ресурсов ЛВС.

Полученные в 2014 году результаты отражают общее повышение доли уязвимых систем по всем видам уязвимостей по сравнению с предыдущими периодами исследования.

Рис. 19. Наиболее распространенные уязвимости внутренней сети

4.3.1. Словарные пароли (1)

Использование словарных паролей, в том числе для привилегированных пользователей, было выявлено во внутренних сетях во всех исследованных в 2014 году системах. При этом наиболее распространено использование словарных паролей для домена Active Directory (88% систем), на втором месте — локальные учетные записи для доступа к различным операционным системам (75%). В каждой третьей протестированной компании (38%) пользователи используют словарные пароли для доступа к важным бизнес-системам, таким как SAP.

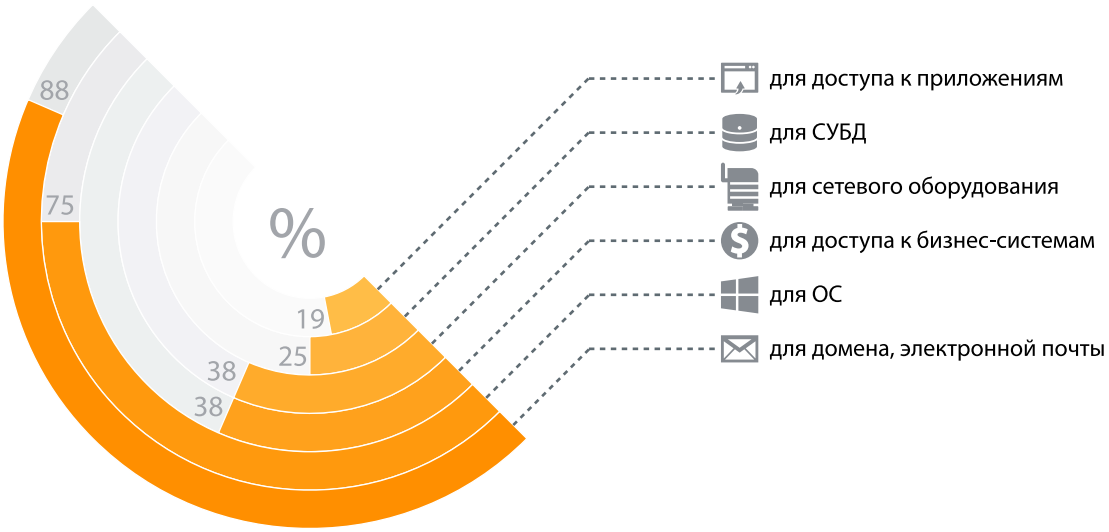


Рис. 20. Словарные пароли во внутренней сети

В каждой второй системе (56%), где были выявлены слабые пароли, администраторы использовали буквенный пароль длиной до 6 символов, в частности в 44% систем использовался пароль admin. В каждой третьей системе (38%) привилегированные пользователи использовали пароль P@ssw0rd. Эти пароли были распространены и в предыдущие годы.

В целом широко распространено использование цифровых паролей длиной до 10 символов (81% систем), при этом наиболее часто встречалось значение 123456 (четверть всех систем). Данный пароль был наиболее популярен и в 2013 году, в том числе среди администраторов. Кроме того, популярны короткие пароли, состоящие из строчных букв латинского алфавита (69% систем) и пароль P@ssw0rd (56% систем).

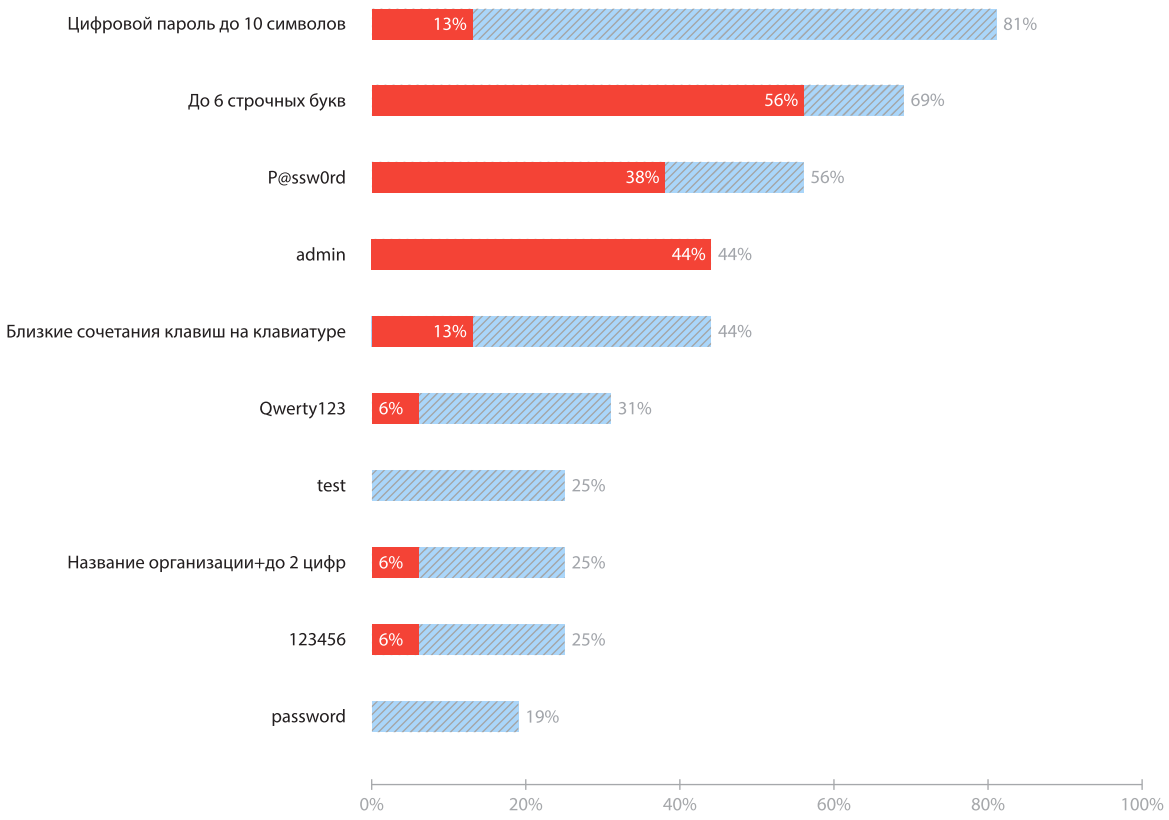


Рис. 21. Доли систем, где были обнаружены слабые пароли

4.3.2. Недостаточный уровень защиты привилегированных учетных записей (2—4)

В 88% исследованных компаний выявлены факты недостаточной защиты для привилегированных пользователей. В системах на базе ОС Linux зачастую недостаточно защищена учетная запись суперпользователя root: в ряде систем был возможен удаленный доступ для данной учетной записи, а также повышение привилегий до root без дополнительной аутентификации.

В доменах Active Directory не используется механизм двухфакторной аутентификации для администраторов, в результате локальные администраторы могут извлечь ученые данные этих пользователей из оперативной памяти и далее воспользоваться ими для доступа к домену. Как правило, данный недостаток становится заключительным этапом атаки, приводящей к получению полного контроля над доменом Active Directory — и впоследствии над другими критически важными системами.

Особое внимание следует уделить внедрению двухфакторной аутентификации для привилегированных пользователей домена еще и потому, что в случае успешной атаки со стороны злоумышленника далее можно воспользоваться полученными правами для реализации атаки Kerberos Golden Ticket. Данная атака позволяет получать доступ к домену

с максимальными привилегиями от имени произвольной учетной записи за счет использования недостатков архитектуры протокола Kerberos (при этом отслеживание действий атакующего крайне затруднительно).

4.3.3. Хранение чувствительных данных в открытом виде (2—4)

Как и в 2013 году, еще одной распространенной уязвимостью в корпоративных системах оказалось хранение чувствительной информации в открытом виде (88%). В рамках проведенных работ по анализу защищенности специалисты Positive Technologies выявили множество фактов хранения важных данных в открытом виде: автоматизированные сценарии с паролями администраторов, конфигурационные файлы сетевого оборудования, текстовые файлы с паролями для доступа к критически важным ресурсам, а также персональные данные пользователей и финансовую информацию на общедоступных ресурсах.

4.3.4. Недостаточно эффективная реализация антивирусной защиты (2—4)

В 88% проанализированных организаций был выявлен недостаток безопасности, заключающийся в недостаточно эффективной реализации антивирусной защиты. Этот недостаток выражается, в частности, в возможности нарушителя с привилегиями администратора запускать на серверах и рабочих станциях под управлением ОС Windows специализированное ПО для проведения атак. На тех узлах, где антивирус выявлял действия нарушителя и блокировал запуск вредоносного ПО, привилегии локального администратора позволяли отключать антивирус либо добавлять данное ПО в список исключений.

В результате подобных действий, а также из-за недостаточной защиты привилегированных учетных записей, в большинстве исследованных в 2014 году систем удалось получить учетные данные пользователей ОС Windows, в том числе учетные данные администраторов доменов, в открытом виде.

4.3.5. Недостатки защиты служебных протоколов, приводящие к перенаправлению и перехвату сетевого трафика (5)

В 2014 году по-прежнему широко распространены недостатки защиты различных служебных протоколов, таких как ARP, STP, NBNS, LLMNR и других. Например, отсутствие механизмов защиты от атак ARP Cache Poisoning было обнаружено в 83% исследованных систем, а отсутствие фильтрации и защиты протокола STP — в 42%. В ЛВС многих компаний выявлено отсутствие защиты таких протоколов, как NBNS и LLMNR, которые по умолчанию используются в системах на базе ОС Windows для разрешения имен при недоступности DNS-серверов (56 и 38% соответственно). Атаки на эти протоколы позволяли перехватывать хэши паролей пользователей и подбирать на их основе пароли.

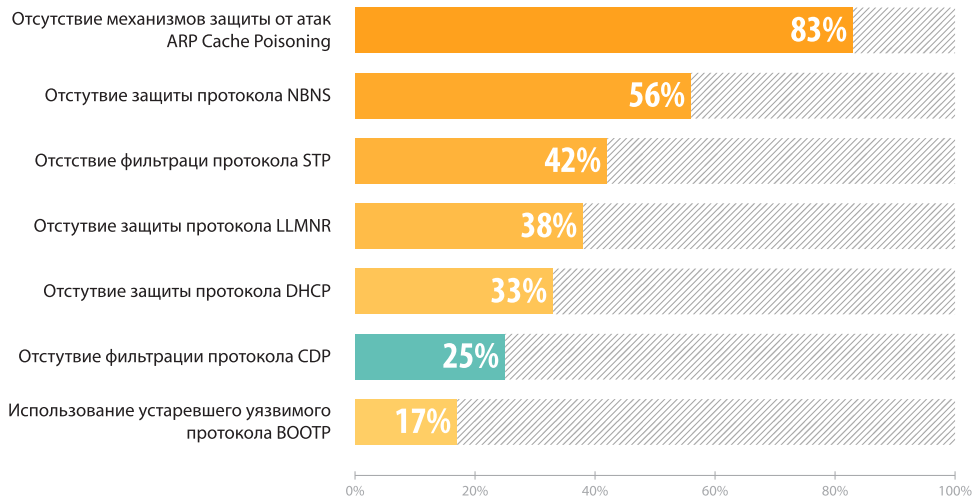


Рис. 22. Недостатки защиты служебных протоколов (доля уязвимых систем)

В отсутствие необходимости использовать те или иные протоколы — их следует отключать, а при наличии такой необходимости следует принимать превентивные меры защиты.

5. Используемые векторы атак

В данном разделе приведена оценка среднего уровня защищенности информационных систем по различным векторам атак. Векторы атак были классифицированы в зависимости от компонентов системы, эксплуатация уязвимостей в которых позволяла получить несанкционированный доступ к ресурсам.

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

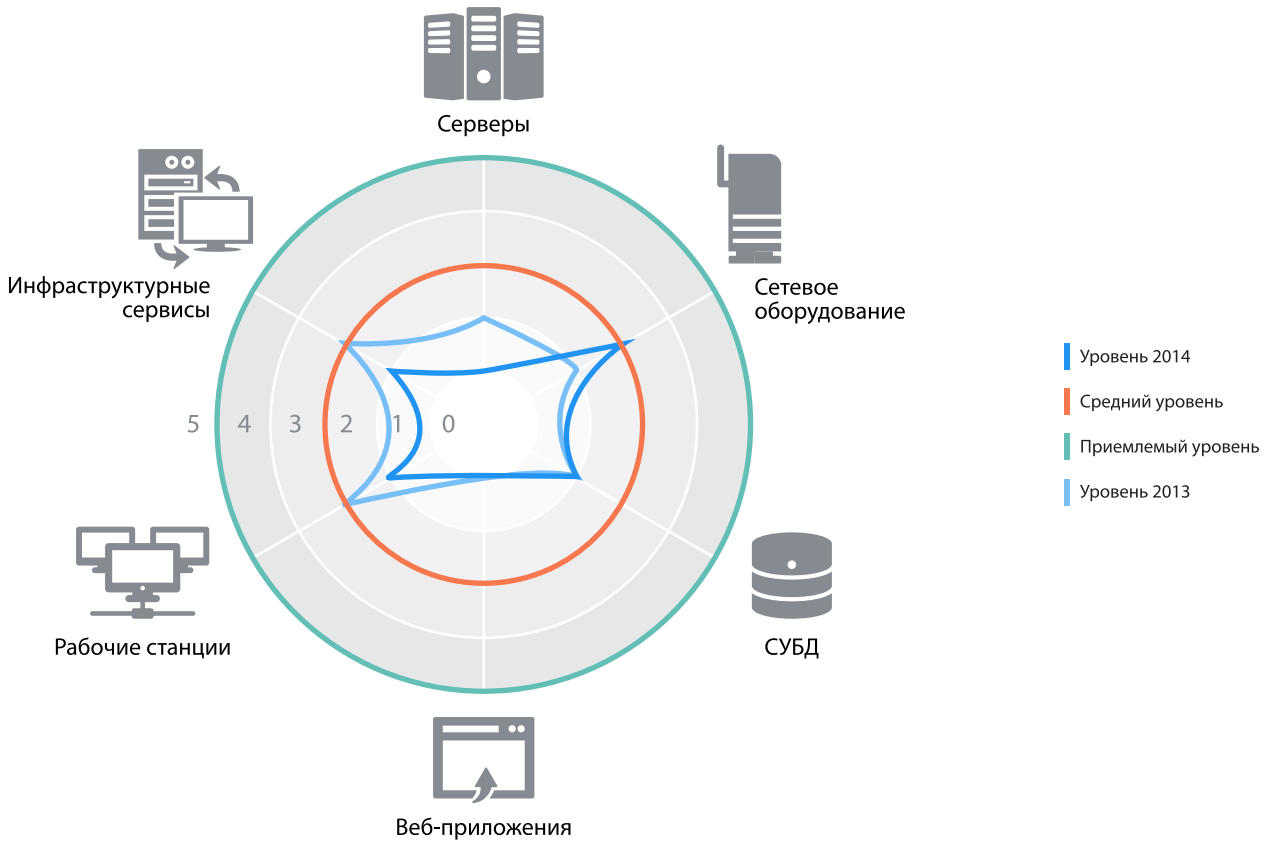


Рис. 23. Общие уровни защищенности отдельных компонентов систем

В 2014 году общий уровень информационной безопасности снизился по сравнению с предыдущим годом. За исключением сетевого оборудования, где уровень защищенности достиг средней отметки, в других областях защищенность понизилась или не изменилась.

6. Оценка механизмов защиты

Оценки уровня защищенности для различных механизмов защиты по большинству направлений остались на уровне 2013 года. Лишь в области сетевой безопасности уровень защищенности поднялся до среднего. Антивирусная защита по-прежнему реализована лучше всего, сохраняя при этом недостатки, связанные с атаками со стороны привилегированных пользователей.

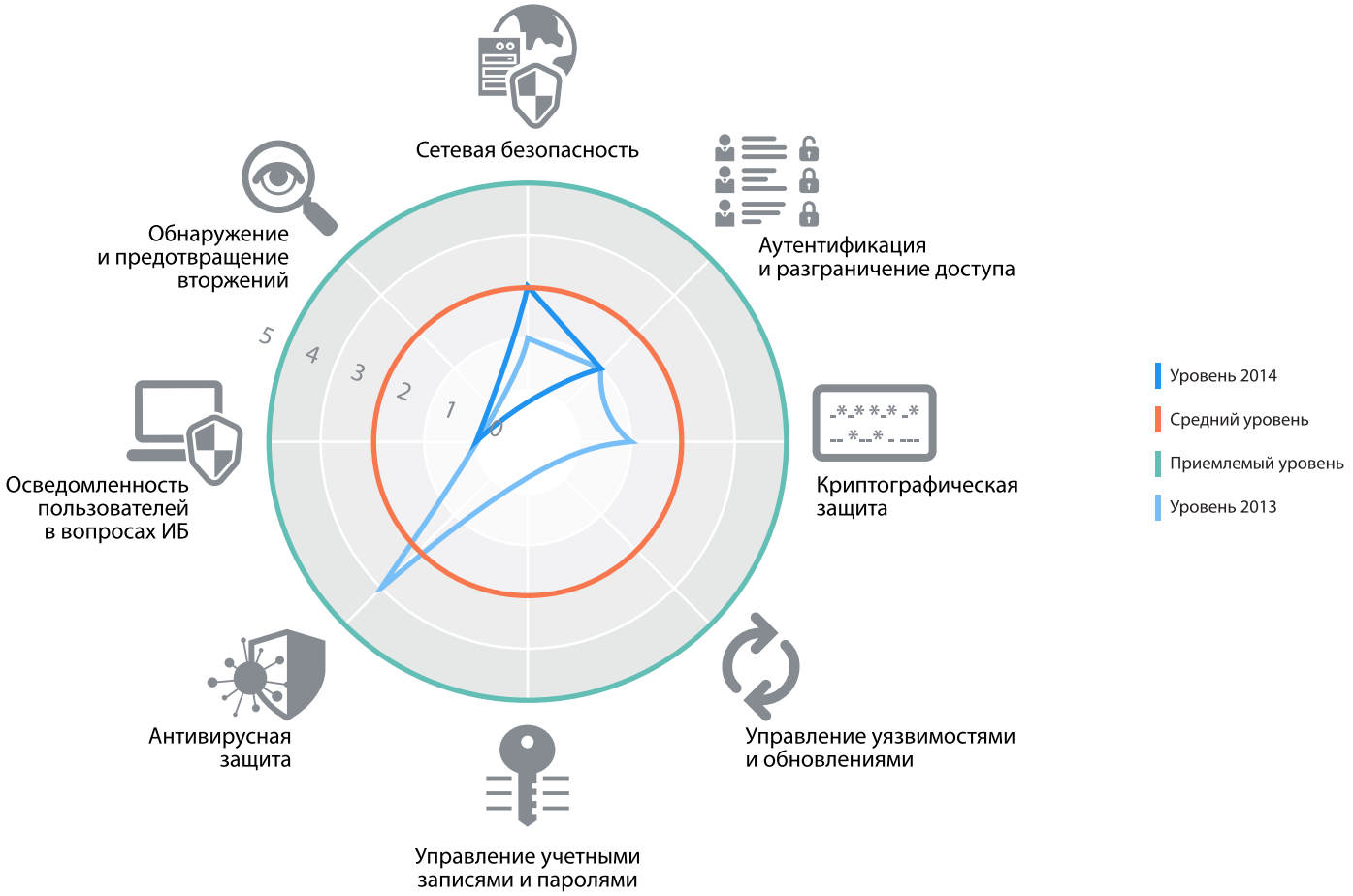


Рис. 24. ***Общие уровни защищенности систем в зависимости от механизма защиты***

7. Результаты оценки осведомленности пользователей в вопросах информационной безопасности

В рамках работ по тестированию на проникновение корпоративных информационных систем в 2014 году для ряда компаний проводились проверки осведомленности пользователей систем в вопросах информационной безопасности. Проверки представляли собой 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 — рассылка 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. Как правило, рассылка писем по электронной почте осуществлялась якобы от лица сотрудника организации, но также применялись сценарии, при которых письма отправлялись от какого-либо внешнего лица или организации.

Оценка уровня осведомленности производилась на основании экспертного мнения специалистов Positive Technologies по результатам проведенных работ.

Полученные результаты отражают существенное снижение уровня осведомленности пользователей систем в вопросах ИБ. Ровно половина систем, в отношении которых проводилось исследование, показали крайне низкий уровень по этому показателю. В 17% систем, в отношении которых были проведены данные работы, уровень осведомленности сотрудников оказался на низком уровне, а каждой третьей системе присвоена оценка осведомленности «ниже среднего».

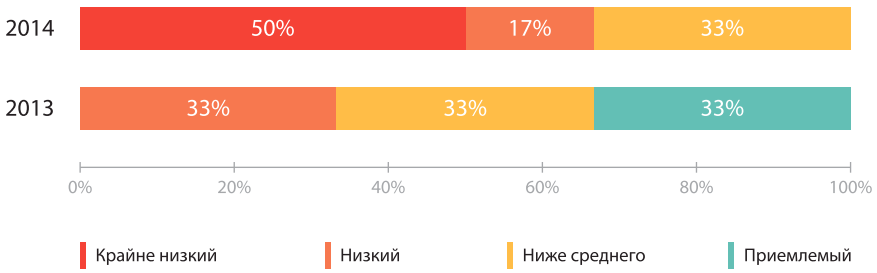


Рис. 25. Уровень осведомленности пользователей в вопросах ИБ (доли систем)

В 2014 году почти в два раза увеличилось среднее количество переходов пользователей по предоставленной в письме ссылке (с 11 до 20%), также было зафиксировано в четыре раза больше фактов ввода учетных данных и запуска приложенных к письму файлов (15%).

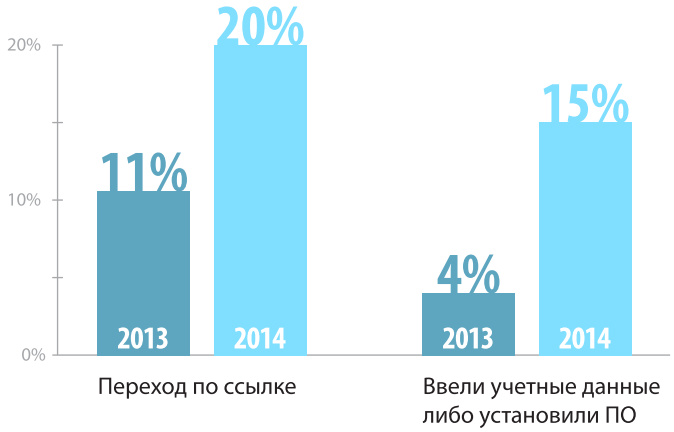


Рис. 26. Доля зафиксированных событий относительно общего количества отправленных сообщений

8. Заключение

Исследование показывает, что корпоративные системы крупных компаний в 2014 году не стали менее уязвимы для атак со стороны внешних и внутренних злоумышленников по сравнению с 2013 годом. Наиболее существенные проблемы, как и ранее, были выявлены в области управления учетными данными (в частности, слабая парольная политика) и в веб-приложениях, через уязвимости которых чаще всего можно проникнуть в корпоративную сеть извне. В 2014 году доли систем, для которых возможно преодоление периметра и получение несанкционированного доступа к важным ресурсам от лица различных категорий атакующих, остались примерно на том же уровне, что и в 2013 году. При этом сложность проведения атак как для внешнего, так и для внутреннего атакующего оказалась заметно ниже, чем в предыдущие годы.

Самые распространенные уязвимости ресурсов сетевого периметра в 2014 году связаны с доступностью интерфейсов управления серверами и сетевым оборудованием (SSH, Telnet, RDP) из внешних сетей. Доля систем, в которых были обнаружены словарные учетные данные, в том числе привилегированных пользователей, по-прежнему высока. Также широко распространены уязвимости, связанные с ошибками в коде веб-приложений.

Для внутрисетевых ресурсов в 2014 году тоже распространены недостатки парольной политики. В корпоративных сетях большинства организаций выявлены недостатки антивирусной защиты и защиты привилегированных учетных записей. Выявлены множественные факты хранения чувствительных данных в открытом виде. По-прежнему распространены недостатки защиты служебных протоколов, позволяющие перенаправлять и перехватывать сетевой трафик.

В отношении уровня осведомленности пользователей в вопросах информационной безопасности в 2014 году наблюдается существенное снижение показателей: значительно увеличилась доля компаний, сотрудники которых осуществляли переход по предоставленным в письмах ссылкам или запускали недоверенное ПО. Более чем для половины исследованных в 2014 году систем уровень осведомленности пользователей в вопросах ИБ оценен как низкий и крайне низкий.

Для проведения атак в большинстве случаев достаточно использовать все те же уязвимости и атаки, которые были распространены в предыдущие годы. Даже в случаях, когда компании спешно устанавливали обновления для такой уязвимости как Heartbleed, другие базовые меры защиты (межсетевое экранирование, сложные пароли, обновления для других компонентов системы) зачастую не применялись.

Факты получения доступа к критически важным ресурсам большинства рассмотренных компаний позволяют сделать вывод о необходимости усовершенствования используемых средств и мер обеспечения информационной безопасности, в частности в области парольной политики, защиты веб-приложений, обеспечения регулярных обновлений безопасности и защиты привилегированных учетных записей. Также следует на регулярной основе проводить аудит безопасности информационных систем и работы по тестированию на проникновение со стороны как внешнего, так и внутреннего нарушителя.

СТАТИСТИКА УЯЗВИМОСТЕЙ
КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
2014

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Более тысячи компаний со всего мира используют наши продукты, надежная работа которых позволяет обеспечить безопасность разрабатываемых приложений, оценить уровень защищенности сетей, контролировать выполнение требований стандартов, блокировать атаки в режиме реального времени. В центре нашего внимания пожелания клиента и исследовательская деятельность, благодаря чему специалисты Positive Technologies заслужили репутацию экспертов в вопросах обеспечения безопасности SCADA- и ERP-систем, веб-приложений, а также банковских и телекоммуникационных технологий. По данным отчета IDC*, Positive Technologies — самая быстроразвивающаяся компания среди поставщиков решений для управления уязвимостями. Более подробную информацию можно получить на сайте www.ptsecurity.ru

* Отчет IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares (№ 242465), опубликованный в августе 2013 года и основанный на данных о выручке от продаж в 2012 году (для вендоров с выручкой больше 20 млн долл. США).

© 2015 Positive Technologies. Наименование Positive Technologies и логотип Positive Technologies являются товарными знаками или зарегистрированным товарными знаками компании Positive Technologies. Все остальные товарные знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев.

POSITIVE TECHNOLOGIES