СТАТИСТИКА УЯЗВИМОСТЕЙ
КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2016

POSITIVE TECHNOLOGIES

Оглавление

Введение

На сегодняшний день вопрос обеспечения информационной безопасности один из наиболее актуальных не только в сфере информационных технологий и в банковской отрасли, где защита информации всегда была на ведущих ролях, но и во множестве других отраслей экономики. Корпоративные инфраструктуры компаний, особенно крупных, ежедневно претерпевают изменения — появляются новые узлы и целые системы, изменяется топология сетей и конфигурация оборудования. Эти динамичные системы нуждаются в регулярном анализе защищенности и незамедлительном устранении обнаруженных угроз безопасности. Обеспечение комплексной защиты информации в режиме 24/7 является для большинства крупных корпораций непростой задачей вследствие высокой сложности архитектуры и большого числа взаимосвязей внутри подсистем.

Тестирование на проникновение — эффективный метод анализа защищенности. Он позволяет выявить уязвимые места в корпоративной инфраструктуре и получить объективную, независимую оценку ее текущего уровня защищенности. В ходе тестирования на проникновение моделируются действия потенциального нарушителя, осуществляющего атаки как со стороны сети Интернет, так и из сегментов внутренней сети компании. Такой подход позволяет воссоздать ситуацию, наиболее приближенную к реальным условиям, в которых обычно действуют нарушители, и оперативно устранить недостатки защиты.

Данный отчет содержит статистику, собранную в ходе работ по тестированию на проникновение, проведенных специалистами компании Positive Technologies в 2015 году. Кроме того, в рамках исследования данные, полученные в 2015 году, сравниваются с результатами аналогичных исследований 2014 и 2013 годов. Представленная информация дает возможность оценить динамику развития современных информационных систем с точки зрения обеспечения информационной безопасности.

В итоговую статистику за год вошли результаты анализа защищенности 17 корпоративных систем, принадлежащих компаниям из различных сфер экономики. В обзоре представлены российские и зарубежные организации, рассматриваются системы наиболее крупных государственных и коммерческих компаний (в том числе входящих в рейтинг 400 крупнейших компаний России в 2015 году по объему реализации продукции по версии агентства «Эксперт»[1]).

При выборе систем учитывалась информативность результатов тестов 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 исследование.

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

1. Резюме

Сводные результаты:

+ В 76% исследованных систем была выявлена возможность получения злоумышленником полного контроля над отдельными критически важными ресурсами. При этом в 35% систем такой уровень привилегий может быть получен от лица любого внешнего нарушителя.
+ В половине исследованных систем возможно получение полного контроля над всей корпоративной инфраструктурой. При этом в 19% случаев такие привилегии могут быть получены со стороны внешнего нарушителя, а еще в 31% компаний — от лица внутреннего нарушителя из пользовательского сегмента сети.

Недостатки защиты сетевого периметра:

+ В каждой второй системе (55%), в отношении которой проводились работы по внешнему тестированию на проникновение, внешний нарушитель, действующий со стороны сети Интернет, способен получить доступ к узлам внутренней сети без использования методов социальной инженерии. А в случае применения таких методов получение доступа к локальной вычислительной сети возможно в 82% случаев.
+ В 54% проектов, где проводились работы по внешнему тестированию на проникновение, были получены максимальные привилегии в каких-либо критически важных для бизнеса системах; в 28% случаев — полный контроль над всей инфраструктурой компании.
+ В каждой второй системе (55%) для преодоления сетевого периметра без использования методов социальной инженерии требовалась средняя либо низкая квалификация, либо вовсе тривиальные действия нарушителя. В среднем для получения доступа к ресурсам внутренней сети, как и в 2014 году, требовалась эксплуатация двух различных уязвимостей.
+ При преодолении сетевого периметра в 47% случаев вектор атаки основывался на эксплуатации уязвимостей веб-приложений. В целом уязвимости различного уровня риска в коде веб-приложений были обнаружены в 69% исследованных систем. Например, уязвимость «Загрузка произвольных файлов» была выявлена в 56% проектов, а «Внедрение операторов SQL» оказалось возможно в 44%.
+ Другие 53% атак, в результате которых был получен доступ к ресурсам внутренней сети, пришлись на использование словарных учетных данных. Данная уязвимость была наиболее распространенной в 2014 году, а в 2015 году выявлена на сетевом периметре 78% систем. Во всех этих системах были обнаружены простые пароли привилегированных пользователей. В 44% компаний словарные учетные данные использовались для доступа к общедоступным веб-приложениям.
+ Во всех исследованных системах были выявлены недостатки, связанные с использованием на сетевом периметре уязвимых версий ПО; главным образом это устаревшие версии веб-серверов (78%).
+ По сравнению с 2014 годом общий уровень защищенности сетевого периметра повысился — в рамках почти половины проектов, где проводились работы, не было выявлено недостатков, которые позволили бы получить доступ к критически важным ресурсам из внешних сетей. Сложность осуществления атак также возросла: для получения доступа к ресурсам внутренней сети внешнему нарушителю лишь в 46% случаев достаточно обладать низкой квалификацией (против 61% в 2014 году).

Недостатки защиты внутренней сети:

- Для всех исследуемых систем, для которых проводилось тестирование от лица внутреннего злоумышленника (например, из пользовательского сегмента сети), удалось повысить привилегии и получить максимальные привилегии в критически важных системах. При этом в 71% случаев был получен полный контроль над корпоративной инфраструктурой.
- В среднем при наличии доступа во внутреннюю сеть для контроля над критически важными ресурсами злоумышленнику требуется эксплуатация четырех различных уязвимостей, что на один шаг больше, чем в предыдущем году, и на один шаг меньше, чем в 2013 году. Однако сложность реализации атак существенно снизилась — в 82% случаев для доступа к критически важным ресурсам нарушителю достаточно было обладать квалификацией низкого уровня; аналогичный показатель в 2014 году составлял лишь 56%.
- Самой распространенной уязвимостью ресурсов внутренней сети остается использование словарных паролей. Данный недостаток обнаружен в рамках всех без исключения проектов. При этом в 91% случаев было выявлено использование слабых паролей для привилегированных учетных записей. Во всех системах также были выявлены недостатки защиты служебных протоколов, которые могут привести к перехвату и перенаправлению сетевого трафика. Недостаточный уровень защиты привилегированных учетных записей и недостатки антивирусной защиты по-прежнему распространены во внутренней сети компаний: уязвимости каждой из этих категорий были обнаружены в 91% систем.
- Уровень защищенности внутренних сетей по-прежнему остается крайне низким. Несмотря на отдельные улучшения (например, повысился средний уровень криптографической защиты, повысилась осведомленность пользователей в вопросах информационной безопасности), применяемых мер защиты все так же недостаточно для противодействия злоумышленникам. Наиболее распространенный сценарий развития атаки во внутренней сети практически не изменился с 2014 года и по-прежнему состоит всего из трех основных этапов. Как и прежде, для успешной атаки достаточно использовать широко распространенные и давно известные типы уязвимостей.

Недостатки осведомленности сотрудников в вопросах ИБ:

- При оценке осведомленности пользователей в вопросах информационной безопасности с использованием методов социальной инженерии были обнаружены те или иные недостатки во всех исследованных системах. Лишь в 25% случаев уровень осведомленности был оценен выше среднего. При этом вдвое снизилась доля компаний, для которых уровень осведомленности сотрудников был оценен как крайне низкий (25% против 50% в 2014 году).
- Важно отметить, что в 2015 году в среднем 24% пользователей осуществили переход по поддельной ссылке (в 2014 году было 20%). Не изменилась доля испытуемых, которые ввели свои учетные данные в заведомо ложную форму аутентификации или загрузили исполняемый файл: показатель остался на уровне 15%.
- В целом уровень осведомленности сотрудников в вопросах информационной безопасности оценивается выше, чем в 2014 году, но по-прежнему остается достаточно низким: ни в одной из протестированных систем он не был оценен как приемлемый.

Недостатки защиты беспроводных сетей:

+ В рамках всех проведенных работ по анализу защищенности беспроводных сетей были выявлены те или иные недостатки безопасности. Тем не менее для 33% систем уровень защищенности беспроводных сетей был оценен как приемлемый.
+ Наиболее распространенными недостатками оказались «Использование несанкционированных точек доступа», «Использование механизма WPS», в ряде случаев выявлено отсутствие защиты беспроводной сети, использование стандартных учетных записей на беспроводном сетевом оборудовании и доступность ряда беспроводных сетей из-за пределов контролируемой зоны.
+ Общий уровень защищенности беспроводных сетей в 2015 году можно оценить как средний. Выявленные недостатки организации беспроводного доступа в общем случае не позволяли получить доступ к ресурсам внутренней сети компаний. Однако в рамках одного из проектов было показано, что недостатки защиты беспроводных сетей в совокупности с уязвимостями ресурсов сетевого периметра позволяют любому внешнему нарушителю в два шага получить доступ к контроллеру корпоративного домена — даже из-за пределов контролируемой зоны.

2. Исходные данные

В рамках исследования были проанализированы результаты тестов на проникновение для 17 информационных систем крупных российских и зарубежных компаний. Как и в предыдущие годы, в их число вошли компании из различных секторов экономики, в том числе банки и финансовые организации, крупные промышленные компании, лидеры в области телекоммуникаций и информационных технологий; представлены одна транспортная компания и одна государственная организация. Наибольшую долю составляют компании банковского и финансового сектора (35%). В равных долях в исследовании представлены промышленные, телекоммуникационные и IT-компании (по 18%).

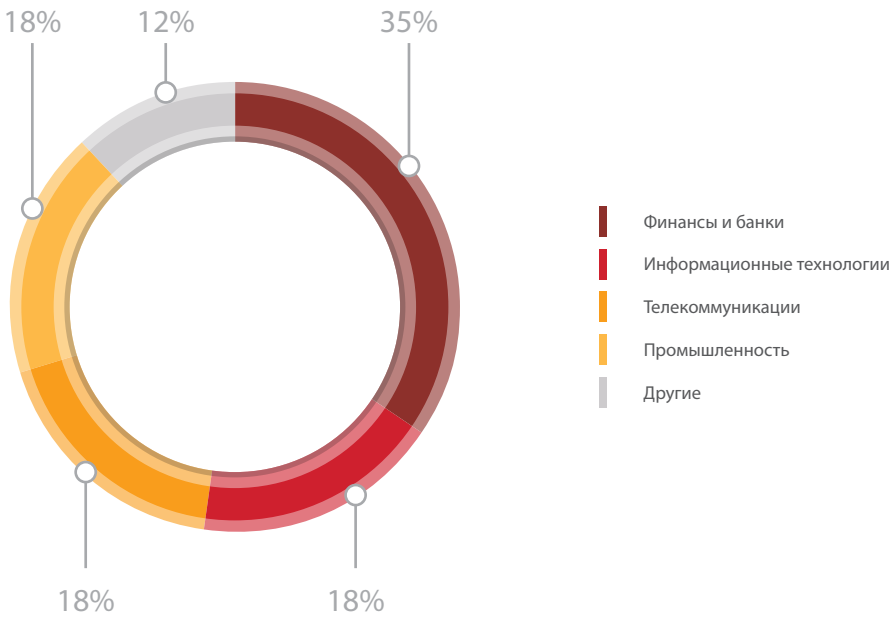

Рис. 1. Распределение исследованных систем по отраслям

Большинство 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 тестов на проникновение в ряде случаев становились сети автоматизированных систем управления технологическими процессами. Важность проведения анализа защищенности подобных систем и своевременного устранения выявленных уязвимостей подтверждают результаты исследования «Безопасность АСУ ТП в цифрах», проведенного Positive Technologies.

В состав оказанных услуг для рассматриваемых систем входили различные виды тестирования на проникновение — внешнее, внутреннее и комплексное тестирование (последнее включает в себя как внешнее, так и внутреннее).

Стоит обратить внимание, что в 2015 году актуальность приобрели отдельные услуги по тестированию на проникновение (либо только внешнее, либо только внутреннее). Лишь одной компании, включенной в данное исследование, была оказана комплексная услуга.

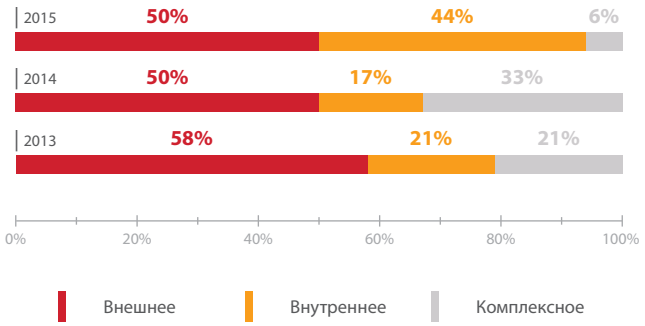

Рис. 2. Виды тестирования на проникновение (доли систем)

В 24% проектов была включена услуга по оценке осведомленности сотрудников в вопросах информационной безопасности. Подобные работы включают в себя ряд проверок, моделирующих наиболее распространенные атаки, основанные на методах социальной инженерии (например, фишинговые рассылки). Подробная статистика и анализ приводятся в разделе 6.

3. Статистика за 2015 год и сравнение ее с результатами 2014 и 2013 годов

3.1. Общие результаты тестов на проникновение

При проведении работ в 2015 году в 76% тестируемых систем специалисты Positive Technologies получили полный контроль над отдельными критически важными ресурсами. В 35% исследованных систем такой уровень привилегий может быть получен от лица любого внешнего нарушителя и еще в 41% систем — со стороны внутреннего нарушителя из пользовательских либо технологических сегментов локальной вычислительной сети. В 24% проектов в 2015 году не удалось получить контроль над какими-либо критически важными ресурсами в рамках установленных границ проведения работ. В целом эти показатели отражают тенденцию к повышению общего уровня защищенности критически важных ресурсов по сравнению с результатами 2013 и 2014 годов.

Рис. 3. Минимальный уровень доступа, необходимый нарушителю для получения полного контроля над отдельными критически важными ресурсами (доля систем)

Для половины исследованных компаний возможно получение полного контроля над всей IT-инфраструктурой, при этом в 19% случаев такой уровень привилегий возможно получить от лица внешнего атакующего. В 31% всех исследованных организаций для получения такого контроля достаточно иметь доступ к внутренней сети.

В 2014 году получение полного контроля над инфраструктурой от лица внешнего нарушителя было возможно в 44% случаев, и в 39% случаев — от лица внутреннего нарушителя. Однако стоит отметить, что в 2015 году в рамках работ по внешнему тестированию на проникновение в ряде проектов по просьбе заказчика не проводилось развитие атаки во внутреннюю сеть компании. Максимальными полученными привилегиями в рамках таких проектов могли стать административные привилегии на серверах сетевого периметра, с которых возможно развитие атаки на ресурсы внутренней сети.

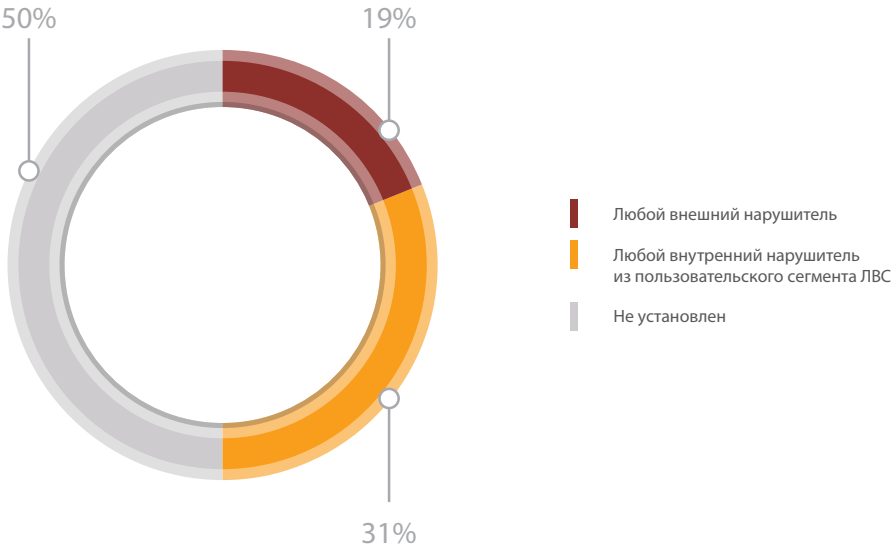

Рис. 4. Минимальный уровень доступа, необходимый нарушителю для получения полного контроля над всей инфраструктурой (доля систем)

Как и в предыдущие годы, практически в каждой корпоративной инфраструктуре были обнаружены уязвимости высокой степени риска. Лишь в одной из систем не было выявлено критически опасных уязвимостей, но были обнаружены уязвимости средней степени риска.

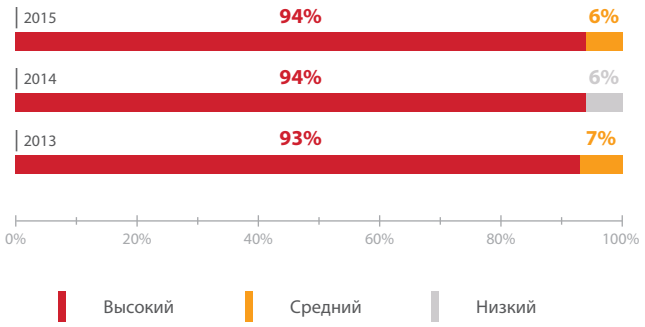

Рис. 5. Доля систем по максимальному уровню опасности уязвимостей

С 2013 года сохраняется тенденция к росту доли организаций, корпоративная инфраструктура которых подвержена критически опасным уязвимостям, связанным с использованием устаревших версий ПО и с отсутствием актуальных обновлений безопасности. Средний возраст наиболее устаревших неустановленных обновлений по системам, где такие уязвимости были обнаружены, составляет 73 месяца (более шести лет). Такой же показатель был выявлен и в 2014 году. Информация о самой старой из обнаруженных уязвимостей была опубликована 14 лет назад (CVE-2002-0083). Данная уязвимость в OpenSSH позволяет авторизованному нарушителю повысить привилегии в системе.

В 13% систем, в отношении которых проводилось тестирование в 2015 году, не было обнаружено уязвимостей, связанных с отсутствием актуальных обновлений. 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 и в этих системах.

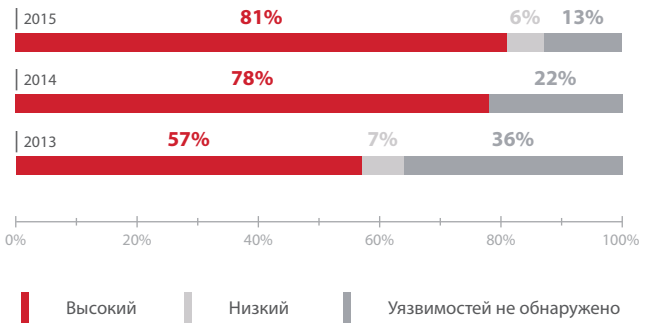

Рис. 6. Максимальный уровень риска уязвимостей, связанных с отсутствием обновлений безопасности (доля уязвимых систем)

Несколько снизилась доля корпоративных систем, содержащих критически опасные уязвимости, связанные с недостатками конфигурации: она составила 81%. Практически в каждой пятой системе (19% от общего числа) были выявлены недостатки конфигурации с уровнем риска не выше среднего.

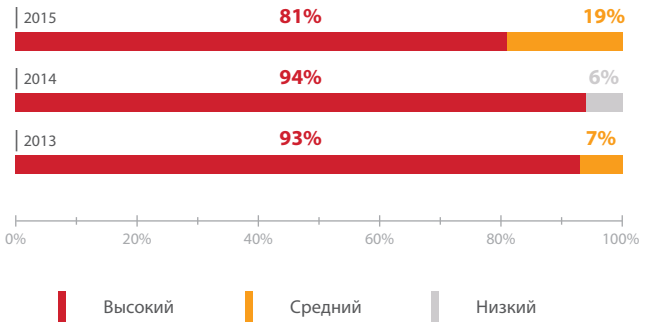

Рис. 7. Максимальный уровень опасности уязвимостей, связанных с недостатками конфигурации (доли систем)

В 68% систем, исследованных в ходе тестов на проникновение, обнаружились уязвимости, связанные с ошибками в коде веб-приложений. В каждой второй организации (57% от общего числа) были выявлены уязвимости высокой степени риска, например «Внедрение операторов SQL», «Внедрение внешних сущностей XML» или «Загрузка произвольных файлов». В 2014 году уровень защищенности веб-приложений был ниже, тогда практически в каждой исследованной системе (89%) были обнаружены уязвимости веб-приложений различного уровня риска. Стоит отметить, что и теперь, и в прежние годы уязвимости в веб-приложениях могли присутствовать *во всех* исследованных корпоративных системах, однако в связи с тем, что тестирование на проникновение проводится методом черного ящика, эти недостатки могли остаться невыявленными.

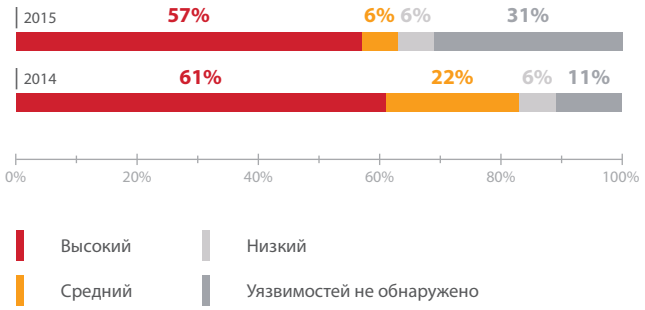

Рис. 8. Максимальный уровень риска уязвимостей, связанных с ошибками в коде веб-приложений (доля уязвимых систем)

3.2. Результаты анализа защищенности сетевого периметра

В 82% исследованных корпоративных информационных систем была выявлена возможность преодолеть сетевой периметр и получить несанкционированный доступ к ресурсам локальной вычислительной сети из внешних сетей. При этом более чем в половине проектов (55%) получить доступ к ресурсам внутренней сети было возможно со стороны любого внешнего нарушителя, не использующего методы социальной инженерии. Этот результат существенно ниже показателей 2013 и 2014 годов.

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

В сравнении с 2014 годом возросла, по оценке специалистов Positive Technologies, сложность преодоления периметра. В 46% случаев для преодоления периметра требуется низкая квалификация либо вовсе тривиальные действия со стороны нарушителя (в 2014 году был 61%). Для 27% систем преодоление периметра было возможно лишь при использовании методов социальной инженерии в отношении сотрудников компании.

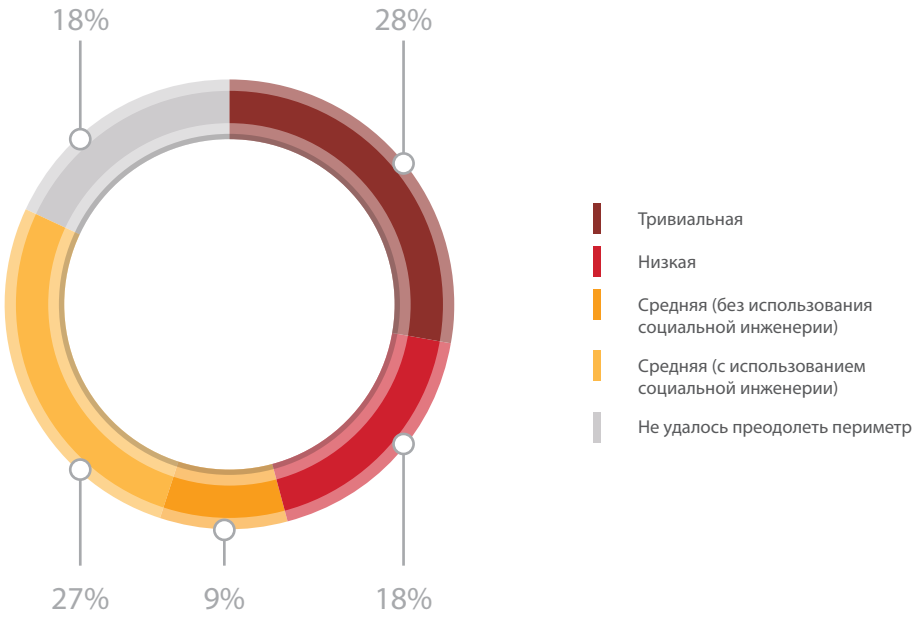

Рис. 10. Сложность преодоления периметра

Согласно полученным данным, для преодоления периметра необходима, как и в предыдущие годы, эксплуатация в среднем двух различных уязвимостей. Практически для каждой из систем было выявлено по несколько векторов атаки для получения несанкционированного доступа к ресурсам ЛВС. При этом в 80% тех случаев, когда периметр удалось преодолеть, был обнаружен по крайней мере один вектор развития атаки, при котором необходима эксплуатация всего одной уязвимости.

Немногим менее половины успешных векторов атак с целью преодоления сетевого периметра в 2015 году были основаны на эксплуатации уязвимостей веб-приложений (47%), а большая часть — на использовании словарных учетных данных (53%). В отличие от атак, реализованных в 2014 году, не были использованы уязвимости устаревших версий ПО, — которые, впрочем, и в 2015 году оказались широко распространены на узлах сетевого периметра.

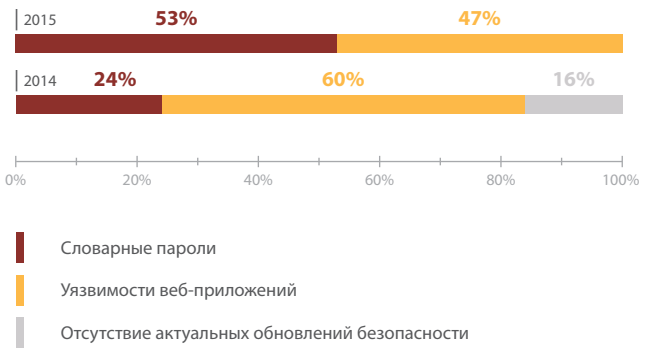

Рис. 11. Векторы атак для преодоления сетевого периметра

Наиболее распространенные уязвимости, выявленные в 2015 году на сетевом периметре:

- уязвимые версии ПО на узлах периметра, недостатки которых нарушитель может использовать для проведения атак;
- использование открытых протоколов передачи данных (Telnet, FTP, HTTP и др.);
- наличие доступных из внешних сетей интерфейсов удаленного доступа и управления сетевым оборудованием и серверами, которые должны быть доступны только ограниченному числу администраторов.

Каждая из этих проблем встретилась более чем в 89% исследованных систем.

Перечисленные уязвимости были распространены и в предыдущие годы. На 33% выросла доля систем, в которых было обнаружено использование уязвимых версий ПО на сетевом периметре. Данный недостаток актуален для всех систем в 2015 году. На 9% участилось использование открытых протоколов передачи данных. Эта уязвимость занимает вторую строчку рейтинга (см. рис. 12). Несколько снизилась (до 89%) доля систем, в которых были выявлены доступные любому пользователю внешней сети интерфейсы управления серверами и сетевым оборудованием; этот недостаток замыкает тройку самых распространенных уязвимостей на сетевом периметре.

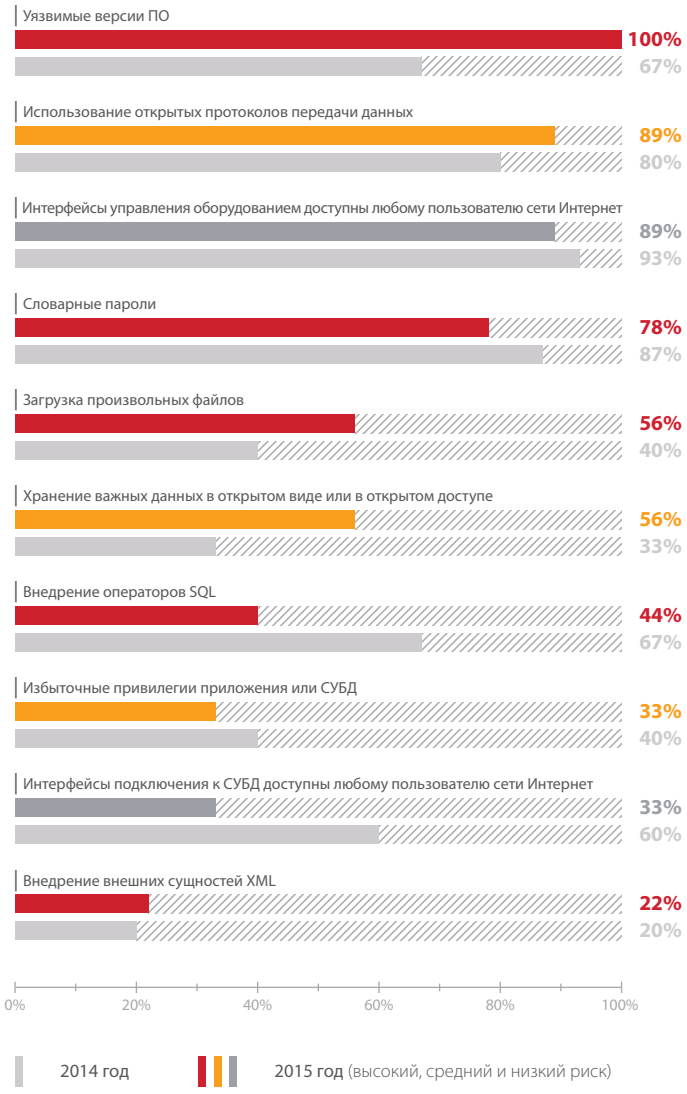

Рис. 12. Наиболее распространенные уязвимости на сетевом периметре

В отличие от предыдущих лет, в топ-5 не вошла критически опасная уязвимость «Внедрение операторов SQL», связанная с ошибками в коде веб-приложения и позволяющая получить несанкционированный доступ к системе управления базами данных в обход логики работы приложения, но она по-прежнему занимает высокую позицию в рейтинге и была выявлена в 44% организаций. Следует отметить, что общий уровень защищенности веб-приложений по-прежнему остается низким, что подтверждается результатами соответствующего исследования «Статистика уязвимостей веб-приложений (2015 г.)», проведенного специалистами Positive Technologies.

3.2.1. Уязвимые версии ПО (1)

При преодолении периметра во всех системах были выявлены недостатки, связанные с использованием уязвимых версий ПО. Это существенно хуже показателей 2014 года, когда подобные уязвимости встретились на периметре 67% компаний.

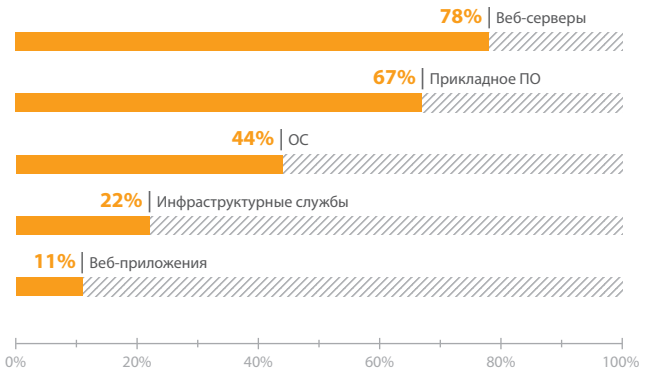

Рис. 13. Устаревшие версии ПО на сетевом периметре

Лидером рейтинга уязвимостей сетевого периметра, как и в предыдущие годы, остаются уязвимые версии веб-серверов. Такое ПО обнаружено на периметре 78% исследованных систем. Например, критически опасные уязвимости на сервере, связанные с использованием Apache HTTP Server версии 1.3.33, поддержка которой прекращена вендором. Возросла доля компаний, на сетевом периметре которых были выявлены уязвимые версии прикладного ПО (с 40% в 2014 году до 67% в 2015-м), например использование устаревшей версии OpenSSH Server с критически опасной уязвимостью «Выполнение произвольного кода». Также возросла доля систем, в которых выявлено использование уязвимых версий ОС (с 33 до 40%), например использование устаревших версий Windows, подверженных критически опасной уязвимости «Удаленное выполнение произвольных команд ОС» (MS08-067). При этом наблюдается снижение доли компаний, на периметре которых были выявлены уязвимые версии приложений, поставляемых из коробки.

3.2.2. Использование открытых протоколов (2, 3)

По-прежнему актуальна проблема использования открытых протоколов передачи данных. Данный недостаток был выявлен в 89% систем и поднялся на вторую строчку рейтинга. Во всех таких системах обнаружено использование протокола FTP. Широко используются и такие протоколы, как Telnet и HTTP, — для доступа к интерфейсам управления. Используя отсутствие защиты данных, передаваемых по этим протоколам, злоумышленник может перехватить чувствительную информацию, в том числе учетные данные привилегированных пользователей, и получить несанкционированный доступ к ресурсам.

3.2.3. Интерфейсы управления оборудованием (2, 3)

Проблема доступности из внешних сетей интерфейсов сетевых служб на сетевом периметре по-прежнему актуальна и входит в тройку наиболее распространенных недостатков.

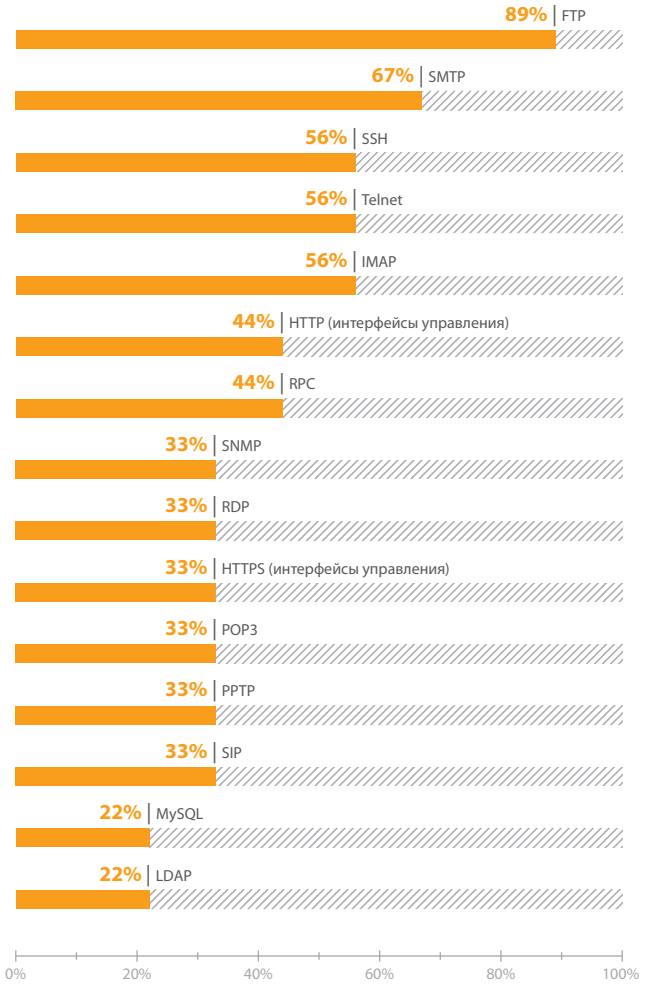

Рис. 14. Протоколы на сетевом периметре (доли систем)

Как и прежде, сохраняется высокая доля систем, где были выявлены доступные для подключения из сети Интернет интерфейсы управления оборудованием по протоколам SSH (56%) и Telnet (56%). В 44% систем для подключения из внешних сетей к интерфейсам управления оборудованием использовался открытый протокол HTTP.

Значительно снизилась (с 80 до 33%) доля организаций, на сетевом периметре которых доступна для подключения любому пользователю внешней сети служба SNMP. При этом на сетевом периметре одной из систем было выявлено использование стандартного значения SNMP Community String с правами на чтение (public).

3.2.4. Словарные идентификаторы и пароли (4)

Использование словарных паролей остается одной из главных проблем безопасности организаций.

В ходе тестирования на проникновение получение паролей пользователей может осуществляться различными способами. Это 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 хеш-значений; восстановление учетных данных из зашифрованных значений и другие методы. В данном исследовании рассматривались все пароли, полученные в ходе тестирования на проникновение тем или иным способом, при этом словарными признавались пароли, которые могут быть в короткие сроки подобраны злоумышленником путем перебора по распространенным словарям.

По сравнению с 2014 годом доля компаний, на сетевом периметре которых выявлен данный недостаток, снизилась незначительно (с 87 до 78%), при этом уязвимость не вошла в тройку наиболее распространенных. Словарные пароли для доступа к приложениям (например, admin) остаются самой распространенной проблемой в данной категории (44%). Доля систем, содержащих словарные пароли для домена и электронной почты (например, 12345678), почти в два раза снизилась в сравнении с 2014 годом (с 40 до 22%). Доля систем, содержащих словарные пароли для СУБД (например, sa) значительно возросла за прошедший год (с 13 до 33%).

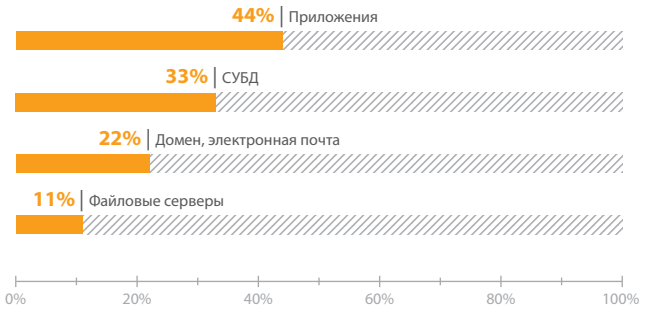

Рис. 15. Словарные пароли на сетевом периметре (доля систем)

Стоит отметить, что словарные пароли для привилегированных учетных записей встретились в 78% исследованных систем, что на 11% больше, чем в 2014 году. Использование словарных идентификаторов и паролей привилегированных пользователей зачастую становится ключевым этапом получения доступа к ЛВС.

3.2.5. Загрузка произвольных файлов (5, 6)

Доля систем с уязвимостями, которые позволяют загрузку произвольных файлов, составила 56%. В сравнении с 2014 годом данная критически опасная уязвимость веб-приложений встречалась на 16% чаще и в большинстве случаев позволяла не только получить возможность выполнения команд на серверах сетевого периметра, но и осуществить доступ к ресурсам ЛВС.

В рамках одного из проектов специалисты компании Positive Technologies получили возможность выполнять загрузку произвольных файлов, используя уязвимую конфигурацию ПО в комбинации с конкретным типом используемой ОС. Была выявлена возможность обойти установленные ограничения на загрузку файлов с расширением .php и загрузить на сервер веб-интерпретатор командной строки.

3.2.6. Хранение важных данных в открытом виде (5, 6)

Был выявлен значительный рост доли систем, содержащих такой недостаток безопасности, как хранение важных данных в открытом виде (с 33 до 56%). При этом в 44% систем обнаружились факты хранения важных данных в открытом виде на общедоступных ресурсах. На страницах публичных веб-ресурсов компаний в 2015 году можно было обнаружить доменные учетные данные, учетные данные для доступа к СУБД, а также персональные данные пользователей.

3.3. Анализ защищенности ресурсов внутренней сети

После получения доступа к внутренней сети внешний злоумышленник имеет возможности для развития атаки и получения полного контроля над критически важными системами. В рамках каждого второго проекта, где проводились такие работы, был получен полный контроль над критически важными ресурсами (системой Active Directory, СУБД, банковской или ERP-системой и другими). При этом в 28% случаев был получен полный контроль над корпоративной инфраструктурой. Данный показатель существенно снизился относительно результатов 2013 и 2014 годов, когда примерно в 80% проведенных тестов были получены максимальные привилегии в критически важных системах. Стоит отметить, что в рамках несколько проектов в 2015 году стояла задача получения контроля над конкретными целевыми ресурсами, без получения максимальных привилегий во всей инфраструктуре (в каждом из таких проектов поставленная цель была достигнута).

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

Как и в предыдущие годы, в рамках всех проектов удалось получить максимальные привилегии в критически важных системах при тестировании от лица внутреннего злоумышленника (например, рядового сотрудника, находящегося в пользовательском

сегменте сети). При этом полный контроль над инфраструктурой был получен в 71% случаев. Полученные результаты совпадают с показателями 2013 года.

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

По оценке специалистов Positive Technologies, для получения доступа к важнейшим ресурсам злоумышленнику достаточно обладать квалификацией низкого уровня. Лишь в 18% случаев сложность реализации атак была оценена как средняя. В 2014 году сложность таких атак оценивалась как средняя практически в половине проектов (44%).

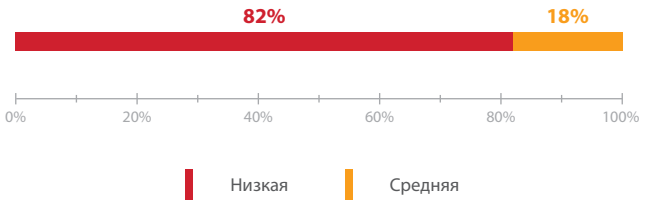

Рис. 18. Сложность получения доступа к критически важным ресурсам со стороны внутреннего нарушителя

В среднем при наличии доступа во внутреннюю сеть для контроля над критически важными ресурсами злоумышленнику требуется эксплуатация четырех уязвимостей, что на один шаг больше, чем в предыдущем 2014 году, и на один шаг меньше, чем в 2013 году. Самая сложная атака в 2015 году насчитывала 6 этапов.

Наиболее распространенный сценарий развития атаки во внутренней сети по-прежнему состоит всего из трех основных этапов и близок к сценарию 2014 года:

1. Получение доступа к ресурсам домена Active Directory с привилегиями пользователя в результате подбора либо перехвата учетных данных.
2. Получение максимальных локальных привилегий на рабочих станциях пользователей в результате подбора пароля либо получения пароля в открытом виде на ресурсах системы.
3. Загрузка на рабочие станции специализированного ПО и получение с его помощью учетных данных администратора домена, сессия которого активна на узле.

Использование словарных учетных данных по-прежнему сохраняет лидерство в рейтинге наиболее распространенных уязвимостей. Во всех исследованных системах был выявлен этот недостаток. В 91% случаев словарные учетные данные использовались и для привилегированных пользователей. На самом верху рейтинга оказались также недостатки защиты протоколов сетевого и канального уровней, приводящие к перенаправлению трафика и перехвату информации о конфигурации сети.

В 91% систем встретились такие уязвимости, как недостаточная защита привилегированных учетных записей и недостаточно эффективная реализация антивирусной. Пятую строчку рейтинга разделили «Использование уязвимых версий ПО» и «Хранение важной информации в открытом виде» (по 82%).

Полученные результаты в целом повторяют картину предыдущего года. При этом доля систем, в которых выявлены «Использование уязвимых версий ПО», «Доступность интерфейсов управления оборудованием любому пользователю локальной сети» и «Использование незащищенных протоколов передачи данных», существенно возросла.

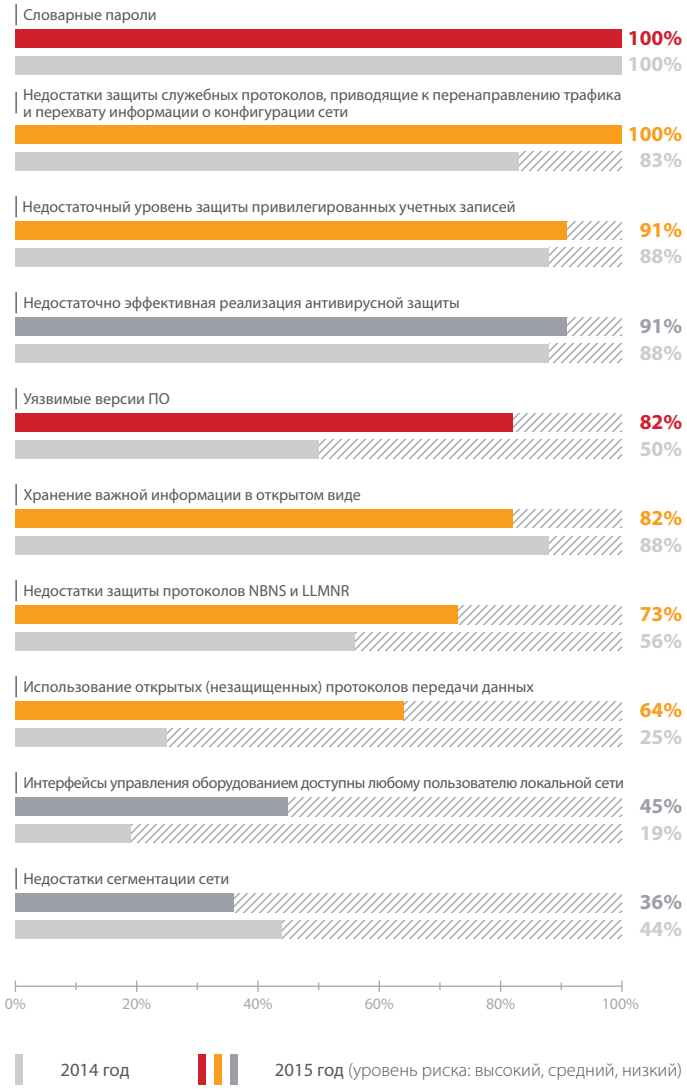

Рис. 19. Наиболее распространенные уязвимости внутренней сети

3.3.1. Словарные пароли (1, 2)

Использование словарных паролей было выявлено во внутренних сетях во всех исследованных системах. Более чем в половине проектов были выявлены словарные пароли для доступа к СУБД и сетевому оборудованию. Словарные пароли для доступа к приложениям также встречались почти в каждой второй системе.

Рис. 20. Словарные пароли (доли систем)

Наиболее распространенными в 2015 году паролями стали комбинации до 7 строчных букв (44% проектов). В 38% случаев в качестве пароля использовались сочетания до 7 символов: цифры и строчные буквы; близкие сочетания клавиш на клавиатуре (например, 1qaz2wsx); пустой пароль.

Пароли admin и 123456 стабильно входят в рейтинг самых частых и встречаются почти в каждой третьей системе.

Пароль admin оказался столь же распространенным и среди привилегированных пользователей. Первую строчку соответствующего рейтинга с ним делит комбинация из не более чем 7 строчных букв (то же в 2014 году).

3.3.2. Недостатки защиты служебных протоколов (1, 2)

Каждая исследуемая система содержала различные недостатки защиты служебных протоколов, таких как ARP, STP, NBNS, LLMNR. В каждом из проектов, где проводился анализ сетевого трафика ЛВС, было выявлено отсутствие механизмов защиты от атак ARP Cache Poisoning. В 73% случаев в системах отсутствовала защита протокола NBNS, и в 36% систем — протокола LLMNR; оба по умолчанию используются в системах на базе Windows для разрешения имен при недоступности DNS-серверов. В целом в 2015 году доля систем с уязвимостями служебных протоколов возросла, внутренние сети компаний по-прежнему недостаточно защищены от атак на протоколы канального и сетевого уровней.

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

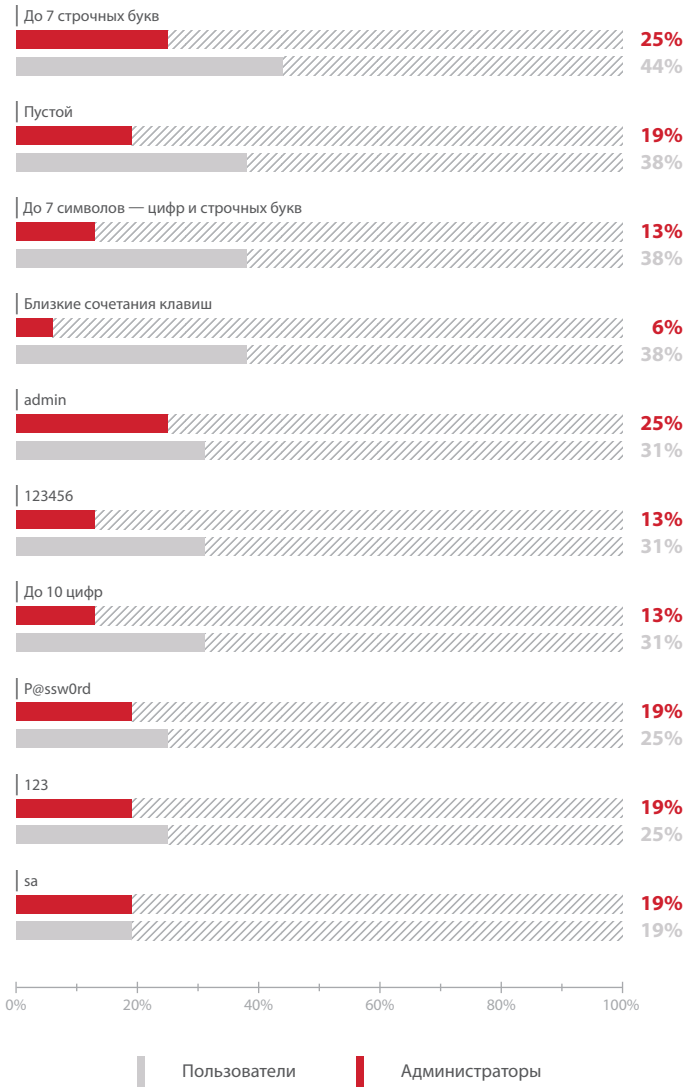

Рис. 21. Словарные пароли во внутренней сети

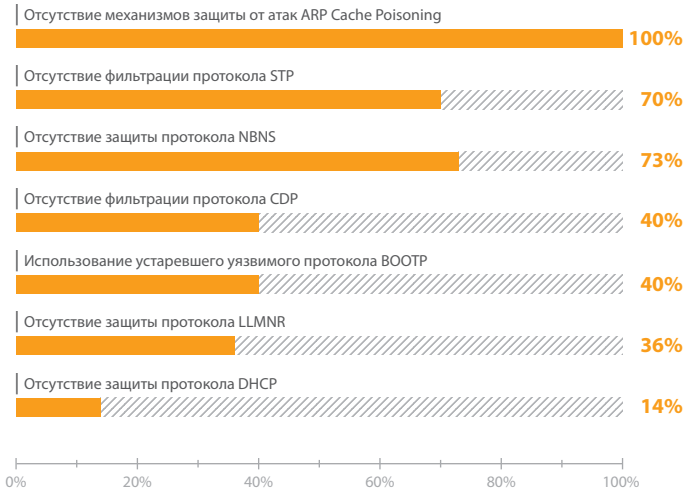

Рис. 22. Недостатки защиты служебных протоколов (доля уязвимых систем)

3.3.3. Недостаточный уровень защиты привилегированных учетных записей (3, 4)

Недостаточный уровень защиты привилегированных учетных записей остается одним из самых распространенных недостатков безопасности корпоративных инфраструктур (91%). Привилегированные учетные записи плохо защищены от атак со стороны злоумышленника, обладающего привилегиями локального администратора. В результате такой нарушитель способен расширить свои привилегии вплоть до получения полного контроля над доменной инфраструктурой. Важно отметить, что подобный недостаток был выявлен во всех корпоративных системах, которые построены на основе доменной архитектуры. Для защиты привилегированных учетных записей критически важных систем рекомендуется использовать двухфакторную аутентификацию.

3.3.4. Недостаточно эффективная реализация антивирусной защиты (3, 4)

Столь же высока доля систем, в которых выявлены недостатки антивирусной защиты. Используемые средства антивирусной защиты имеют недостаточно эффективную реализацию, что позволяет злоумышленнику осуществить запуск вредоносного ПО, в частности специализированных утилит для взлома.

На тех узлах, где антивирус выявлял действия нарушителя и блокировал запуск вредоносного ПО, привилегии локального администратора позволяли отключать антивирус, добавлять данное ПО в список исключений либо создавать копию памяти серверного процесса.

Эксплуатация данного недостатка часто позволяет злоумышленнику получить учетные данные пользователей Windows, в том числе администраторов доменов, в открытом виде.

3.3.5. Хранение важной информации в открытом виде (5, 6)

Остается распространенным хранение чувствительной информации в открытом виде; этот недостаток выявлен в 82% исследованных систем. Файлы с учетными записями для доступа к критически важным ресурсам, приватные ключи для доступа по протоколу SSH, данные для привилегированного доступа к СУБД, персональные данные пользователей, финансовая и другая чувствительная информация были обнаружена в ходе работ по анализу защищенности.

3.3.6. Уязвимые версии ПО (5, 6)

В сравнении с результатами 2014 года в корпоративных системах существенно чаще стали встречаться устаревшие версии ПО (82% исследованных систем).

В каждой второй системе (55% от общего числа) были выявлены уязвимые версии прикладного ПО. Широкое распространение получило использование устаревших версий ОС, на которых не установлены актуальные обновления безопасности (45% выполненных проектов).

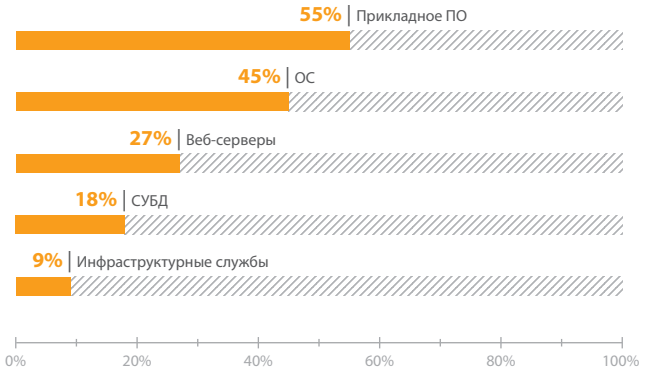

Рис. 23. Устаревшие версии ПО во внутренней сети

4. Векторы атак

В данном разделе приведена оценка среднего уровня защищенности информационных систем по различным векторам атак. Векторы были классифицированы в зависимости от компонентов системы, уязвимости в которых позволяли 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 позволяют напрямую получить доступ к критически важным ресурсам либо присутствует множество критически опасных уязвимостей), а оценка 5 соответствует приемлемому уровню защищенности (уязвимостей не обнаружено, средства защиты реализованы корректно).

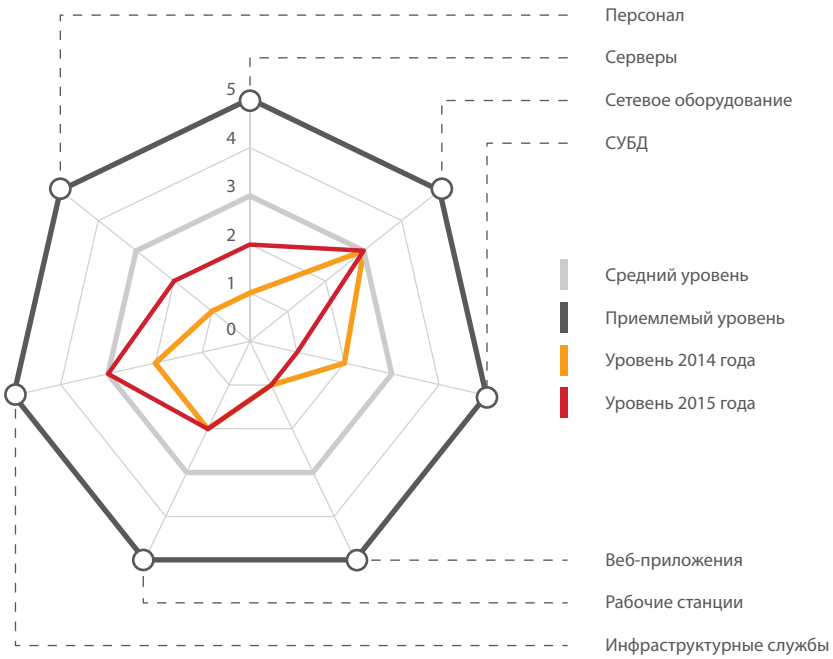

Рис. 24. Общие уровни защищенности отдельных компонентов систем

Общий уровень информационной безопасности повысился по сравнению с 2014 годом. Снижение уровня защищенности было зафиксировано только для СУБД: множество векторов атак в 2015 году было связано с недостатками именно этих систем. Для инфраструктурных служб и сетевого оборудования уровень защищенности оценивается как средний. Низкий уровень защищенности сохраняют веб-приложения, множественные уязвимости которых зачастую позволяли преодолеть сетевой периметр и получать контроль над критически важными ресурсами. Уровень защищенности в категориях «Персонал» и «Серверы» незначительно повысился, но все еще остается достаточно низким.

5. Оценка механизмов защиты

Оценки уровня защищенности для различных механизмов защиты повысились в категориях «Осведомленность пользователей в вопросах ИБ» и «Криптографическая защита». При этом наблюдается снижение уровня надежности антивирусной защиты, недостатки которой были выявлены почти в каждом проекте 2015 года.

Низкой остается оценка в категории «Обнаружение и предотвращение вторжений» — в 2015 году в рамках реализованных проектов не было зафиксировано действий со стороны администраторов систем, направленных на предотвращение атак. Автоматизированные системы, такие как межсетевые экраны уровня приложений, были выявлены на сетевых периметрах ряда компаний, однако недостаточная эффективность их реализации не позволила обеспечить необходимую защиту от атак.

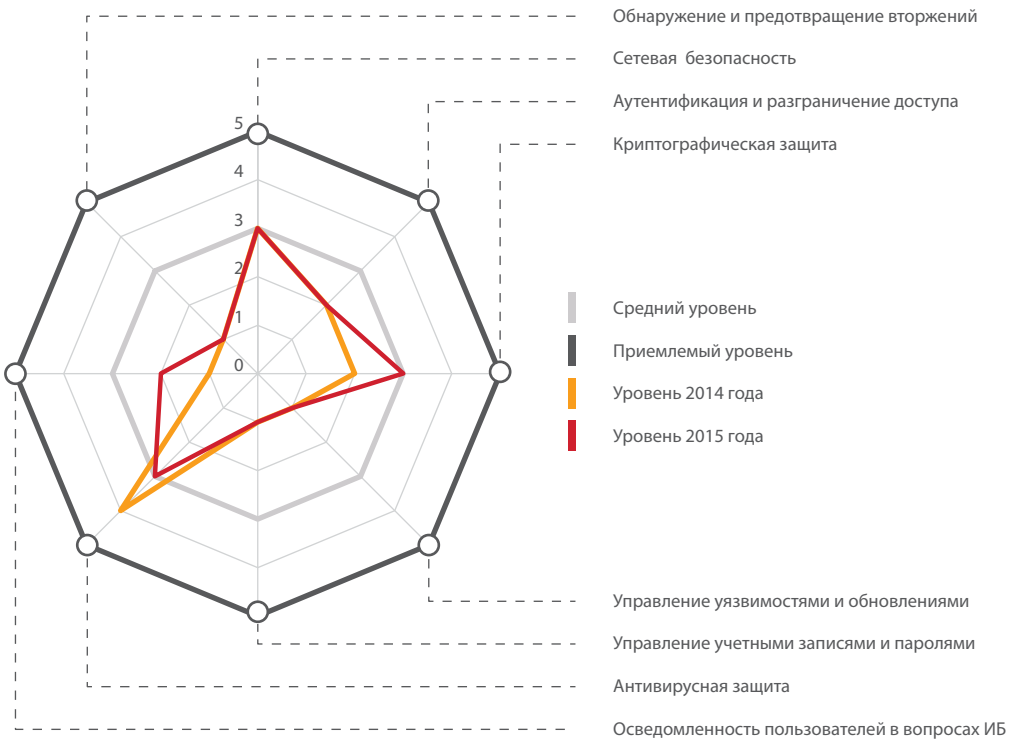

Рис. 25. Общие уровни защищенности систем в зависимости от механизма защиты

6. Результаты оценки осведомленности пользователей в вопросах ИБ

В рамках работ по тестированию на проникновение корпоративных информационных систем в 2015 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 по индивидуальным сценариям методом рассылки по электронной почте сообщений, содержащих вложения в виде файла либо 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 применялись также сценарии, при которых письма отправлялись от какого-либо стороннего лица или организации.

Оценка уровня осведомленности производилась на основании экспертного мнения специалистов Positive Technologies.

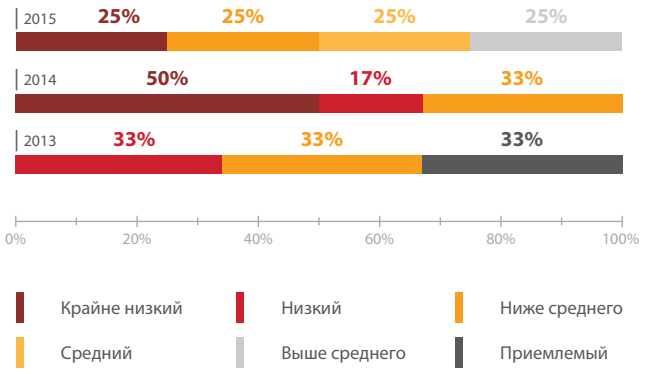

Рис. 26. Уровень осведомленности пользователей в вопросах ИБ (доли систем)

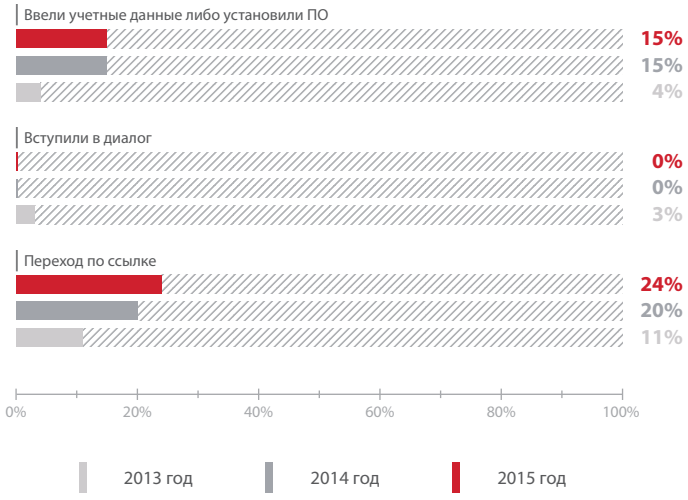

Рис. 27. Доля зафиксированных событий относительно общего количества отправленных сообщений

Полученные результаты в целом свидетельствуют о повышении среднего уровня осведомленности сотрудников компаний в вопросах ИБ. В два раза снизилась доля систем с крайне низким уровнем осведомленности. В каждой второй системе уровень осведомленности оказался не ниже среднего.

Важно отметить, что в среднем в рамках всех проектов зафиксированное количество переходов по ссылке на сторонний ресурс оказалось даже выше, чем в предыдущие годы, а факты загрузки и запуска файла остались на уровне 2014 года. Это объясняется тем, что большинство зафиксированных контролируемых событий приходится на проекты, где уровень осведомленности характеризуется как крайне низкий.

Таким образом, наблюдается тенденция к повышению общего уровня осведомленности пользователей в вопросах ИБ, однако он по-прежнему остается достаточно низким.

7. Результаты анализа защищенности беспроводных сетей

В 2015 году проводился ряд работ по анализу защищенности беспроводных сетей. В рамках данных работ проводится поиск недостатков в использовании точек доступа и клиентских устройств Wi-Fi для диапазонов 2,4 и 5 ГГц с использованием технологий 802.11a/b/g/n, а также недостатков в архитектуре и организации беспроводного доступа. В 67% систем уровень защищенности беспроводных сетей оценивается как средний или ниже среднего.

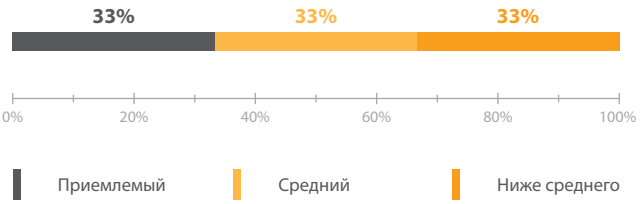

Рис. 28. Уровень защищенности беспроводных сетей (доли систем)

Среди выявленных недостатков стоит отметить использование механизма WPS для упрощения процесса настройки беспроводной сети. Для подключения к точке доступа используется специальный PIN-код, состоящий только из цифр. Нарушитель может подобрать PIN-код и подключиться к точке доступа.

Также выявлены факты использования несанкционированных точек доступа; в случае их подключения к локальной вычислительной сети злоумышленник имеет возможность получить доступ к внутренним сетям. В ряде систем было обнаружено отсутствие защиты отдельных беспроводных сетей. Отсутствие механизмов шифрования сетевого трафика может привести к его перехвату злоумышленником. Нарушитель может получить чувствительную информацию (например, учетные данные привилегированных пользователей). К распространенным уязвимостям можно также отнести использование стандартных учетных записей для доступа к веб-интерфейсу управления сетевым оборудованием.

В рамках одного из проектов было установлено, что почти все беспроводные сети компании доступны за пределами контролируемой зоны, при этом на общедоступных ресурсах сетевого периметра в открытом виде хранились учетные данные пользователя домена. Таким образом, любой внешний нарушитель, находящийся за пределами контролируемой зоны, может подключиться к беспроводной сети организации и осуществлять атаки на ресурсы ЛВС.

Заключение

Результаты исследования 2015 года показали, что информационные инфраструктуры компаний по-прежнему уязвимы для атак со стороны как внешнего, так и внутреннего нарушителя. Доля систем, для которых возможно преодоление периметра и получение несанкционированного доступа к важным ресурсам, снизилась по сравнению с предыдущим годом. Сложность проведения атак для внешнего атакующего оказалась выше. Тем не менее уровень защищенности от атак со стороны внешнего нарушителя, как и прежде, довольно низок. Уровень же защищенности систем от атак внутреннего нарушителя остается крайне низким. В большинстве случаев злоумышленник может с успехом использовать все те же уязвимости и атаки, которые были распространены в предыдущие годы.

Лидерами рейтинга распространенных уязвимостей на сетевом периметре стали «Уязвимые версии ПО», «Использование открытых протоколов передачи данных» и «Доступность интерфейсов управления оборудованием любому пользователю сети Интернет». Актуальной остается проблема использования словарных учетных данных, в том числе и для привилегированных пользователей.

Недостатки управления учетными записями и паролями, а также недостатки защиты служебных протоколов, оказались наиболее распространенными проблемами во внутренних сетях исследуемых систем. По-прежнему велика доля систем, в которых выявляются недостатки, связанные с защитой привилегированных записей, реализацией антивирусной защиты, хранением важных данных в открытом виде и использованием устаревших версий ПО.

Осведомленность пользователей в вопросах информационной безопасности в 2015 году была оценена выше, чем в 2014-м. Однако доля сотрудников, которые перешли по предлагаемой ссылке, увеличилась. Для четверти исследованных систем уровень осведомленности и вовсе оценивается как крайне низкий.

В ходе анализа защищенности беспроводных сетей во всех исследуемых системах были выявлены те или иные проблемы безопасности. С учетом уровня опасности выявленных недостатков общий уровень защищенности беспроводных сетей можно оценить как средний.

Подводя итоги, стоит отметить, что для обеспечения безопасности корпоративной системы необходим комплексный подход. Без учета всех компонентов функционирующей системы невозможно создать защищенную инфраструктуру. В 2015 году, как и в прежние годы, векторы атак на корпоративные инфраструктуры компаний со стороны внешних сетей и со стороны внутреннего нарушителя основывались на эксплуатации распространенных уязвимостей и недостатков, для устранения которых, как правило, достаточно применить самые общие принципы обеспечения информационной безопасности. Необходимо особое внимание уделять строгости парольной политики, защите привилегированных учетных записей, а также защите от атак на публичные веб-приложения. Необходимо обеспечить регулярное обновление используемого ПО и установку актуальных обновлений безопасности на автоматизированной основе.

Для снижения рисков компрометации критически важных систем со стороны внешних нарушителей рекомендуется особое внимание уделять ресурсам, доступным из внешних сетей. Как показывает практика, подавляющее большинство успешных атак, приводящих к получению доступа к критически важным ресурсам и преодолению сетевого периметра компании, основаны на эксплуатации уязвимостей не официальных сайтов организаций и их серверов, а каких-либо других ресурсов компании, которые не должны быть доступны на сетевом периметре (например, СУБД, неиспользуемых отладочных интерфейсов,

интерфейсов удаленного доступа или управления, интерфейсов инфраструктурных служб, таких как LDAP). Интерфейсы для доступа к таким ресурсам могут быть открыты для подключения по ошибке администраторов; зачастую представители крупных компаний, отвечающие за безопасность информационной инфраструктуры, не могут точно сказать — сколько и каких ресурсов организации доступны из внешних сетей. «Забытые» на сетевом периметре ресурсы наиболее уязвимы, так как их безопасности не уделяется никакого внимания, их ПО может не обновляться в течение нескольких лет, привилегии и учетные записи никем не администрируются. Атаки на эти ресурсы могут вовсе остаться незамеченными, если в компании не применяются эффективные средства обнаружения и предотвращения атак. В частности, для защиты от атак на веб-приложения рекомендуется применять межсетевые экраны уровня приложения с эффективными настройками правил корреляции. Для контроля за ресурсами на сетевом периметре рекомендуется обеспечить регулярное сканирование ресурсов, доступных из внешних сетей (к примеру, раз в месяц). Для своевременного выявления и устранения уязвимостей в коде критически важных веб-приложений необходимо регулярно проводить работы по анализу их защищенности, как методом черного или серого ящика, так и методом белого ящика с подробным анализом исходных кодов. Такие работы важно проводить не только на каждом этапе разработки приложения, но и в отношении систем, принятых в эксплуатацию (например, два раза в год), с последующим контролем устранения выявленных уязвимостей.

Что касается защиты корпоративных систем от атак со стороны внутреннего нарушителя, картина в данной области практически не изменяется с течением времени. Наиболее распространенный вектор атаки, позволяющий получить полный контроль над информационной инфраструктурой компании со стороны любого внутреннего нарушителя, основывается на тех же уязвимостях, что и год и два назад. Основные рекомендации в этом случае также неизменны. Необходимо следовать базовым принципам обеспечения информационной безопасности — ввести парольную политику, запрещающую использование простых паролей, предусматривающую обязательную двухфакторную аутентификацию для привилегированных пользователей критически важных систем, а также предусматривающую требования к регулярной смене паролей (например, раз в 60 дней) — и строго контролировать ее соблюдение; также необходимо обратить особое внимание на устаревшие версии ПО, на открытые протоколы передачи данных, на хранение важной информации в открытом виде на серверах и рабочих станциях сотрудников.

Кроме базовых мер защиты информации следует на регулярной основе проводить аудит безопасности информационных систем и тестирование на проникновение со стороны внешнего и внутреннего нарушителя. По оценке специалистов Positive Technologies, для снижения рисков компрометации корпоративных систем до приемлемого уровня такое тестирование должно проводиться не реже двух раз в год, с контролем исправления выявленных уязвимостей. Кроме того, рекомендуется проводить тренинги для сотрудников с целью повышения их уровня осведомленности в вопросах информационной безопасности, а также периодически оценивать эффективность этих тренингов.

О компании

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru