СЕРВИСЫ POSITIVE TECHNOLOGIES ПО ОЦЕНКЕ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ

Тестирование на проникновение

Анализ защищенности веб-приложений

Анализ защищенности мобильных приложений

Специализированные сервисы по оценке защищенности бизнес-приложений

POSITIVE TECHNOLOGIES

ОДНА ОШИБКА — И ТЫ ОШИБСЯ

Цифровая трансформация бизнеса — настоящий подарок для хакеров и головная боль для ИБ-специалистов. Злоумышленникам для успешной атаки достаточно одной уязвимости, тогда как компании должны закрывать абсолютно все бреши безопасности для предотвращения инцидентов.

Хотелось бы, чтобы защита веб-приложений была разовой задачей, но это невозможно. Обеспечение безопасности приложений — критически важный процесс, который должен работать непрерывно. Только так корпоративная инфраструктура, включая мобильные и веб-приложения, будет максимально защищена от кибератак.

Всегда необходим взгляд со стороны

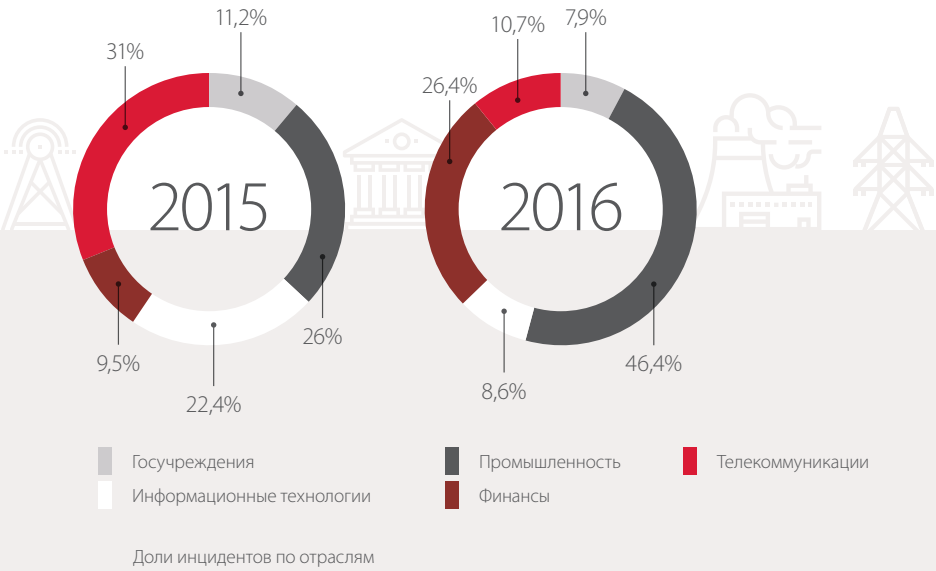
Недавно мы проводили анализ защищенности в крупном банке. Руководство банка постоянно инвестирует в безопасность: среди прочего у них используется межсетевой экран уровня веб-приложений и проводится регулярное тестирование на проникновение. Осознавая необходимость экспертной оценки своей защиты, специалисты банка регулярно обращаются к разным командам пентестеров. К моменту, когда они обратились к нам, в банке уже был проведен ряд сторонних проверок. В ходе исследования наши эксперты обнаружили:

+ пять векторов атак — каждый мог быть использован для проникновения;
+ в четырех из пяти векторов использовались уязвимости веб-приложений;
+ в двух системах были обнаружены действующие веб-шеллы — скрипты, позволяющие получить удаленный доступ. Это потребовало отдельного расследования.

Опыт подтвердил, что регулярная независимая оценка защищенности необходима: жертвой хакеров могут стать даже те компании, в которых уже внедрены межсетевые экраны уровня приложений и проводится собственное тестирование. В результате аудита банк получил наглядную картину рисков безопасности, угрожавших его операциям, клиентам и репутации. Благодаря рекомендациям наших экспертов специалисты заказчика незамедлительно приступили к закрытию уязвимостей и оперативно устранили угрозы.

Безопасность для галочки — не наш подход

Наша миссия заключается в выстраивании долгосрочных отношений с клиентами, которые нам доверяют. Команда экспертов Positive Technologies уже проверила сотни сетей по всему миру. Если вы доверите нам оценку защищенности вашей компании, мы тщательно протестируем системы безопасности, выявим истинный уровень риска и обеспечим наилучший результат от ваших инвестиций в защиту веб-приложений.



Доли инцидентов по отраслям

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ: УВИДЕТЬ ВСЮ КАРТИНУ

Тестирование на проникновение (пентест) — это взгляд на инфраструктуру с точки зрения хакера и поиск уязвимостей, которыми может воспользоваться реальный злоумышленник. Ежегодно мы проводим десятки пентестов в крупных международных организациях. Вот как выглядят результаты пентестов, проведенных за последние три года:

Семь из 10 попыток взлома были успешными, хотя большинство компаний регулярно проводили тестирование.

В 80% случаев злоумышленники могли бы получить **полный контроль над инфраструктурой компании** (в 2016 году этот показатель достигал 100%).

В каждой протестированной системе были обнаружены уязвимости. В некоторых случаях **было выявлено до десяти отдельных векторов атак**, способных в совокупности привести к успешному проникновению.

В нескольких случаях нашим экспертам удалось **выявить и пресечь целевые атаки (APT)**, которые все еще велись на момент проверки.

Что мы делаем: передовые сервисы от экспертов в анализе защищенности

+ **Инвентаризация доступных извне и внутренних ресурсов.** Инфраструктура крупной компании — это изменчивая среда, состоящая из множества компонентов. Для обеспечения полноценной защиты инфраструктуры необходимо понимать, какие ресурсы в нее входят и какая их часть доступна через внешние сети.
+ **Обнаружение слабых мест в инфраструктуре и демонстрация потенциальных атак.** Наши эксперты играют роль внешних злоумышленников, стараясь обойти защитные механизмы и проникнуть в корпоративную сеть.
+ **Непрерывная поддержка и консультация экспертов.** Результаты тестирования включают подробные рекомендации экспертов для оперативного устранения уязвимостей.
+ **Повторное тестирование для проверки корректности устранения угроз.** Через некоторое время наши эксперты проведут повторное тестирование, помогут вам проверить успешность устранения уязвимостей и при необходимости дадут дальнейшие рекомендации.

Как мы это делаем: приемы белых хакеров

Как и хакеры-злоумышленники, эксперты Positive Technologies используют различные техники, позволяющие проверить вашу безопасность на прочность:

+ **Внешнее тестирование на проникновение** выявляет уязвимости, которые могут использовать злоумышленники без знаний о вашей инфраструктуре и прав доступа.
+ **Внутреннее тестирование на проникновение** выявляет способы проведения успешной атаки со стороны внутреннего нарушителя.

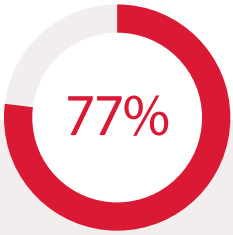
Объем услуг может быть дополнен оценкой защищенности беспроводных сетей и социотехническим пентестом (имитацией атак с приемами социальной инженерии).

ОЦЕНКА ЗАЩИЩЕННОСТИ ВЕБ-ПРИЛОЖЕНИЙ

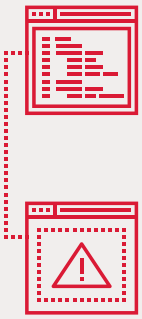
Уязвимости есть практически во всех веб-приложениях. Даже если в приложении нет критически опасных уязвимостей (хотя по нашему опыту это редкость), сочетание уязвимостей средней и низкой степени опасности может привести ко взлому.

Веб-приложения с критически опасными уязвимостями

Веб-приложения с уязвимостями средней степени опасности



Успешные попытки проникновения через уязвимости в веб-приложениях (пентест)



Сводные результаты проектов по тестированию на проникновение, проведенных экспертами Positive Research в 2016 году.

Даже если вам кажется, что ваши веб-приложения не являются ценной добычей, помните: для злоумышленников плохо защищенное приложение — это ключ ко всей инфраструктуре. В ходе исследований нашим экспертам в 77% случаев удалось проникнуть за периметр через веб-уязвимости.

Ныряем глубже: получение полной картины безопасности

Почему уязвимости не всегда удается выявить с помощью стандартных инструментов и процедур? Дело в том, что успешность поиска зависит от глубины анализа. В рамках услуги по оценке защищенности веб-приложений наши эксперты анализируют как само приложение, так и постоянно изменяющуюся среду, в которой оно работает.

Комплексная оценка защищенности веб-приложений.
Мы проводим всесторонний анализ приложений как вручную, так и с использованием автоматизированных средств. Методы черного, серого и белого ящика комбинируются с инструментальным анализом с помощью PT Application Inspector.

Максимальная точность и наглядность.
Наши эксперты производят оценку того, с какой вероятностью злоумышленники воспользуются теми или иными уязвимостями. Процедура оценки проводится параллельно с практической демонстрацией эксплуатации уязвимостей.

Рекомендации по устранению выявленных недостатков.
Результат тестирования — подробный отчет с рекомендациями по устранению выявленных уязвимостей и повышению защищенности как приложений, так и всего периметра в целом.

Проверка корректности устранения уязвимостей.
Через установленный промежуток времени проводится повторный анализ защищенности, позволяющий оценить эффективность работ по устранению уязвимостей.

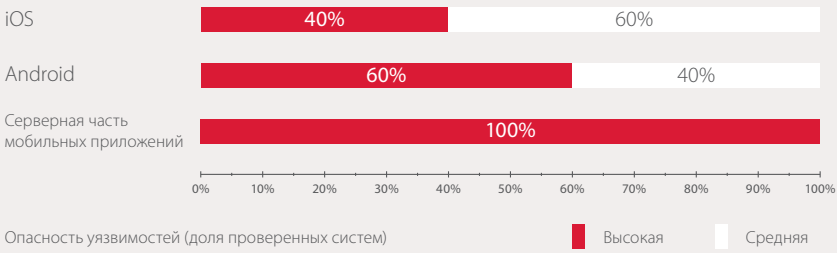
ЗАЩИТА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ: БАЛАНС МЕЖДУ БЕЗОПАСНОСТЬЮ И УДОБСТВОМ ИСПОЛЬЗОВАНИЯ

Пользователи все больше доверяют мобильным сервисам. Уровень потребления растет — а с ним и аппетит пользователей к функциональности приложений. В свою очередь хакеры спешат воспользоваться открывающимися возможностями и низким уровнем осведомленности пользователей в вопросах безопасности. Поскольку мобильные платформы постепенно становятся даже не основным, а единственным средством обслуживания во многих банках, в электронной коммерции и других отраслях, защиту клиентов и собственной инфраструктуры необходимо сделать приоритетной.

Революция в мобильном банкинге

Уже 54% клиентов сегодня пользуются мобильными банковскими приложениями, и этот показатель вырос по сравнению с 2015 годом (48%). Среди пользователей поколения двухтысячных рост популярности мобильных банков еще заметнее: сейчас ими пользуются 75% клиентов по сравнению с 59% в 2015 году.

(Bank of America, Trends in Consumer Mobility Report, 2016 год)



Сбои в обслуживании, утечка конфиденциальных данных и прямые атаки на пользователей мобильных приложений заставляют разочарованных клиентов уходить к конкурентам. Долговременный ущерб бренду и репутации компании в результате хакерской атаки может быть катастрофическим.

Серверная инфраструктура: иллюзия безопасности

Несмотря на то что большинство компаний придают большое значение проблеме безопасности, вопрос защиты мобильных устройств остается в тени. В результате пользователи подвергаются повышенной опасности, а серверная инфраструктура остается незащищенной. Концентрируясь на защите веб-приложений, организации часто забывают, что на стороне сервера мобильные приложения используют веб-технологии и подвержены тем же рискам.

Устраняя риски во всей среде мобильных приложений

В ходе оценки защищенности мобильных приложений эксперты Positive Technologies помогут выявить уязвимости и на стороне клиента приложения, и на стороне серверной инфраструктуры, а также выполнят объективную и независимую оценку общего уровня защищенности. В объем работ входят:

+ **Оценка защищенности серверной стороны мобильного приложения.** Используются те же методы белого, серого и черного ящика, что и при тестировании веб-приложений, а также анализ кода приложений при помощи PT Application Inspector.
+ **Анализ защищенности клиентской части мобильного приложения.** Эксперты выявляют уязвимости клиентского приложения: хранение конфиденциальной информации в виде незашифрованного текста, возможность получения несанкционированного доступа к критически важным функциям приложения (например, финансовым транзакциям) и др.

СПЕЦИАЛИЗИРОВАННЫЕ УСЛУГИ ПО ОЦЕНКЕ ЗАЩИЩЕННОСТИ БИЗНЕС-ПРИЛОЖЕНИЙ

Онлайн- и мобильный банкинг, электронная коммерция, порталы и ERP-системы — практически в каждой отрасли критически важные для бизнеса приложения автоматизируют ежедневные операции и позволяют эффективнее взаимодействовать с клиентами.

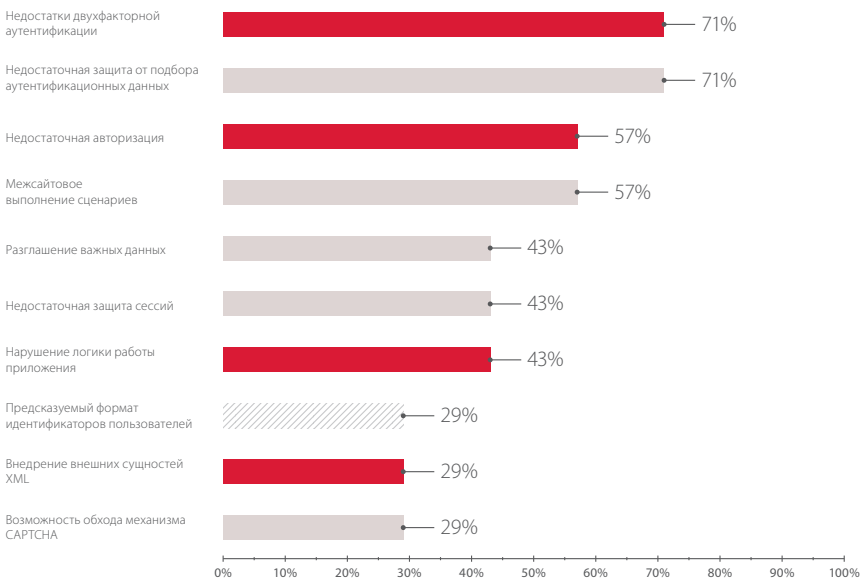
Все эти приложения важны для непрерывности бизнес-процессов, несмотря на разницу в бизнес-логике, сложности и степени конфиденциальности используемых данных. Многие из них функционируют через интернет частично, некоторые — так называемые тонкие клиенты — полностью работают через браузеры, что делает их уязвимыми к веб-угрозам. Другие (толстые клиенты) хоть и не подвержены интернет-угрозам, но уязвимы к иным видам атак.

Защита бизнес-приложений осложняется тем, что многие из них были разработаны до того, как появилось понимание рисков, связанных с защищенностью приложений. Организации продолжают пользоваться унаследованным ПО и не желают вносить изменения в критически важные процессы, боясь нарушить ход производства.

Благодаря нашим сервисам клиенты получают комплексную оценку рисков, связанных с критически важными для бизнеса приложениями, а также подробные рекомендации по устранению выявленных недостатков. Услуги включают в себя:

+ проверку механизмов идентификации, аутентификации, двухфакторной аутентификации и авторизации;
+ проверку бизнес-логики;
+ анализ защищенности веб-приложения;
+ обратную разработку толстого клиента.

На диаграмме представлены результаты наших проектов по оценке защищенности бизнес-приложений на предмет рисков, с которыми регулярно сталкивается банковская сфера*.



Топ-10 веб-уязвимостей онлайн-банков

* Positive Research 2017.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах 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 телеком-операторов.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com