Монитор безопасности

Обеспечение информационной безопасности

ПРОФИЛЬ КОМПАНИИ

ЗАО «Монитор безопасности» – основано в 2012г.

Основной фокус услуг компании – анализ защищенности корпоративных сетей.

✓ Мы получили высокую степень экспертизы в данной сфере благодаря участию в многочисленных проектах по всему миру (на международном рынке мы работаем в партнерстве с SEC Consult) Наши сотрудники проводят более 350 аудитов в год.

✓Все специалисты компании проходили обучение в Австрии, Германии, Сингапуре и Литве, что позволило перенять лучший мировой опыт и ноу-хау как в проведении кибератак так и в противодействии их проведению.

✓Специалисты компании обладают международными сертификатами и являются членами международных профессиональных сообществ.

✓Собственная лаборатория выявления уязвимостей в России.

ОСНОВНЫЕ УСЛУГИ КОМПАНИИ

- Анализ защищенности web-приложений;
- Внешний и внутренний аудит (анализ защищенности):
  - мобильных устройств;
  - VoIP;
  - WLAN;
  - DMZ ;
  - Интернет-банкинг;
  - Банкоматы;
  - ERP и т.д.;
- Обеспечение безопасности при разработке ПО;
- Аудит безопасности исходных кодов;
- Анализ вредоносного кода;
- Расследование компьютерных инцидентов;
- Симуляция DoS-атаки (уровни L3-L7);
- Социальная инженерия.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ И ПРЕИМУЩЕСТВА

- ✓ Применяем те же технологии, что и реальные хакеры;
- ✓ Воспроизводим атаки внешних злоумышленников или внутренних нарушителей;
- ✓ Выявляем уязвимости, недоступные для сканеров безопасности и прочих автоматизированных технических решений;
- ✓ Акцентируем свое внимание не на широко распространенных ошибках в программном обеспечении и стандартных уязвимостях, а на реальных угрозах, способных нанести урон ИТ-инфраструктуре или привести к финансовым или репутационным потерям;
- ✓ Обладаем международной экспертизой в выявлении уязвимостей сети.

Монитор безопасности

УГРОЗЫ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОТОРЫЕ МЫ РЕШАЕМ

Угрозы безопасности в информационных системах общественно значимых структур

Дискредитация компании путем замены официальной информации на ложную или компрометирующую.

Похищение конфиденциальной информации или персональных данных граждан.

Похищение секретной информации, в том числе, содержащей коммерческую тайну.

Нарушение работоспособности информационных систем. Финансовые потери по причине простоя.

Мошеннические действия на основе услуг, предоставляемых в электронном виде.

Злоупотребления при оплате государственных услуг и сервисов, а также услуг критически значимой инфраструктуры – транспорта и ЖКХ.

Монитор безопасности

ЧТО МЫ ПРЕДЛАГАЕМ?

Противодействие кибератакам: автоматические сканеры vs. моделирование атаки

ХАКЕРСКАЯ АТАКА:
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ + ЧЕЛОВЕЧЕСКИЙ ИНТЕЛЛЕКТ

Автоматические сканеры выявляют только публично ИЗВЕСТНЫЕ уязвимости в безопасности.

Автоматические сканеры практически не выявляют ошибки бизнес-логики приложений.

Автоматические сканеры плохо идентифицируют уязвимости на стыке нескольких систем.

Автоматические сканеры не способны выявлять новые, ранее неизвестные уязвимости.

ТОЛЬКО МОДЕЛИРОВАНИЕ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА МОЖЕТ ПОКАЗАТЬ РЕАЛЬНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ СИСТЕМЫ

Наша специализация – проведение аудита информационной безопасности в ручном режиме

1. МОДЕЛИРОВАНИЕ ДЕЙСТВИЙ РЕАЛЬНЫХ ЗЛОУМЫШЛЕННИКОВ

Наши специалисты проводят аудит информационных систем в ручном режиме. Технические средства позволяют выявить только публично известные уязвимости. В ходе аудита проводится не только сканирование и тестирование используемого ПО, но и моделируются сценарии наиболее критически противоправных действий внешних и внутренних злоумышленников.

2. АКЦЕНТ НА КРИТИЧНЫХ НАПРАВЛЕНИЯХ АТАКИ

Аудит производится с учетом критерия целесообразности использования сценария для злоумышленника и степенью критичности выбранного вектора атаки.

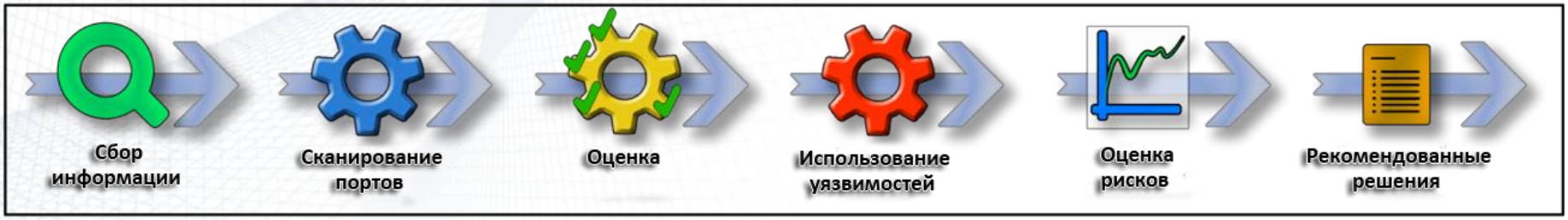
3. ПРОВЕДЕНИЕ АУДИТА В РУЧНОМ РЕЖИМЕ

Моделирование атак и анализ кода производятся в «ручном режиме», технические средства используются как основа для принятия решений по построению атаки или оценки критичности уязвимости для бизнеса.

Аудит информационной безопасности в ручном режиме

Метод	Знания исполнителей	Степень охвата
Метод «черного ящика» (blackbox)	• Отсутствие детальной информации о целевой системе. • Равнозначность внешней атаке хакеров.	• Могут быть обнаружены около 30% всех уязвимостей.
Метод «прозрачного ящика» (glassbox)	• Знания о целевой системе и (или) административный доступ к целевой системе и, следовательно, доступ к логам и внутренней системной информации. • Информация о целевой архитектуре. • Частичный анализ исходного кода (или обратное проектирование через бинарный анализ).	• Могут быть обнаружены около 70% всех уязвимостей.
Анализ исходного кода (source code review)	• Ручной анализ исходного кода и проверка уязвимостей, обнаруженных в тестовой среде.	• Могут быть найдены практически все уязвимости , для которых существует возможность осуществления атаки

Процедура и результаты (методы «стеклянного ящика» и «черного ящика»)



1. Сбор информации

Мероприятие	Результат
Установление имен доменов и IP-адресов	Имена доменов и IP-адреса
Анализ веб-сайта компании	Различная информация
Поиск с помощью поисковых машин	Различная информация

2. Сканирование портов

Мероприятие	Результат
Сканирование портов тестируемых объектов	Конфигурация брандмауэра и предлагаемые сервисы Существующие операционные системы Существующие сетевые компоненты

3. Оценка

Мероприятие	Результат
Автоматический анализ сервисов на наличие известных проблем в системе безопасности	Список уязвимостей
Ручная проверка сервисов, в особенности приложений	Список уязвимостей

4. Использование уязвимостей

Мероприятие	Результат
Использование обнаруженных уязвимостей (если это не угрожает текущим операциям)	Доказательство концепции материала (имена пользователей, пароли, скриншоты, секретные данные)

5. Оценка рисков

Мероприятие	Результат
Оценка рисков отдельных уязвимостей путем составления матрицы рисков	Оценка рисков для каждого слабого места в системе безопасности
Расстановка приоритетов выявленных слабых сторон в системе безопасности	Классификация слабых мест в системе безопасности
Просчет общих рисков	Общий риск системы
Оценка распределения рисков (собственные приложения, настройки, инфраструктура, стандартное программное обеспечение, статус патча)	Графическое распределение ИТ-рисков

6. Рекомендованные решения

Мероприятие	Результат
Разработка предложений по исправлению для обнаруженных уязвимостей	Список предлагаемых решений

Процедура и результаты (анализ исходного кода)

1. Подготовка

Мероприятие	Результат
Подготовка тестовой системы	Подготовленная тестовая система

2. Анализ исходного кода

Мероприятие	Результат
Автоматическая проверка	Список уязвимостей
Ручная проверка	Список уязвимостей
Использование выявленных уязвимостей	Доказательство концепции материала (имена пользователей, пароли, скриншоты, секретные данные)

3. Оценка рисков

Мероприятие	Результат
Оценка рисков отдельных уязвимостей путем составления матрицы рисков	Оценка рисков для каждого слабого места в системе безопасности
Расстановка приоритетов выявленных слабых сторон в системе безопасности	Классификация слабых мест в системе безопасности
Просчет глобального воздействия	Общий риск системы

4. Рекомендованные решения

Мероприятие	Результат
Разработка предложений для исправления обнаруженных уязвимостей	Список предлагаемых решений

Результат проведения аудита информационной безопасности в ручном режиме

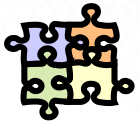
Обнаружение существующих уязвимостей в системе обеспечения безопасности информационных систем посредством целевых атак.

Оценка степени риска существующих уязвимостей в системе обеспечения безопасности информационных систем и их значение для внутренних и внешних процессов, в том числе – критически значимых.

Подготовка рекомендуемых решений для устранения обнаруженных уязвимостей.

Обнаружение подсистем с высоким уровнем риска для безопасности, требующих проведения дополнительных проверок.

Приоритезация мер по повышению уровня информационной безопасности, через акцентирование усилий на критически значимых направлениях.



Комплексная оценка уровня безопасности, в том числе с учетом возможности комбинаций уязвимостей взаимосвязанных систем.

Проверка эффективности внедренных инструментов обеспечения информационной безопасности.

Структура отчета по итогам аудита

КЛИЕНТЫ

В список клиентов «Монитор безопасности» входят лидирующие банки, государственные учреждения, публичные компании из: России, Германии, Австрии, Швейцарии, Сингапура и Восточной Европы.

За время своего существования компания «Монитор безопасности» провела более 700 тестов на проникновение, более 100 из них были проведены для систем ДБО.

«Монитор безопасности» использует очень строгие соглашения о неразглашении с своими Клиентами. Данные соглашения не позволяют предоставлять информацию по большинству проектов. Решение о предоставлении информации о клиентах принимается в каждом отдельном случае и учитывает действующие соглашения о неразглашении информации.

Монитор безопасности

Контактное лицо:
Ксения Варламова
Директор по работе с клиентами
Т: +7 (495) 984-08-34
М: +7(926)902-51-54
119334, Россия, Москва, 5-й Донской пр-д, д.15, стр. 11
E-mail: k.varlamova@securitymonitor.ru