Обеспечивает ли защищенность наличие сертификата соответствия требованиям международных стандартов по ИБ

2016

EY

Совершенствуя бизнес,
улучшаем мир

Результаты исследования EY GISS 2015

Укрепляя доверие в цифровом мире

18ое Ежегодное Международное Исследование ЭЯ по вопросам информационной безопасности за 2015 год

- **Собственные сотрудники** (71%), **криминальные синдикаты** (53%) и **хакеры-одиночки** (41%) входят в список основных источников кибератак в России.
- По мнению респондентов **наименее** вероятным источником кибератаки являются бизнес-партнеры.
- 29% респондентов отмечает использование средств обнаружения кибератак на внешнем периметре корпоративной сети, и **только 6% респондентов отмечает использование комплексных систем** по управлению событиями и инцидентами информационной безопасности в совокупности с системами обнаружения и предотвращения кибератак.
- ***Наиболее распространенным недостатком в системе внутренних контролей, повлекшем за собой реализацию киберриска, отмечается слабый уровень осведомленности пользователей в вопросах реагирования на фишинговые атаки.***

Эволюция кибератак

Простые атаки (Скрипт-кидди)
Атака происходит по причине того, что Вы подключены к Интернет и присутствует уязвимость

Сложные атаки (Хакеры)
Атака происходит по причине того, что Вы подключены к Интернет и обладаете ценной информацией

Корпоративный шпионаж (Инсайдеры)
Ваши текущие или бывшие сотрудники пытаются получить финансовую выгоду за счет продажи вашей интеллектуальной собственности

Целевые атаки (киберпреступные группировки)
Атака происходит по причине того, что Вы используете конкретную технологию, атака на которую может обеспечить высокую степень монетизации

Атаки с использованием продвинутых методов обеспечения постоянного присутствия (APT)
Вы являетесь целью потому что:
- Вы тот, кем являетесь;
- Делаете то, что делаете;
- Высокая стоимость Вашей интеллектуальной собственности.

Высококвалифицированная группа киберпреступников

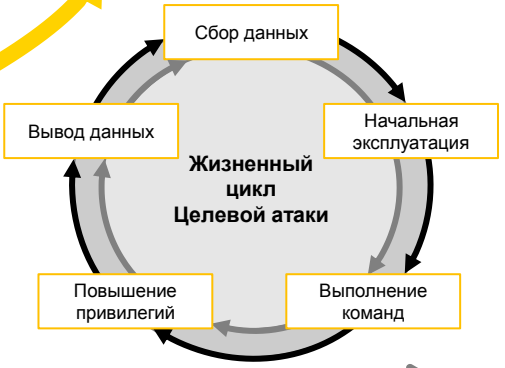
Риск

Эксперимент/
Развлечение

Монетизация

Корпоративный
шпионаж

Монетизация /
остановка бизнес-процессов



Источник атаки и ее сложность

1980s/1990s — 2016

- BrainBoom/Morris Worm
- Polymorphic viruses
- Michelangelo
- Concept Marco viruses
- Melissa
- 'I love you'
- Anna Kournikova
- Sircam
- Code Red and Nimada
- SQL Slammer
- Blaster
- Fizzer
- MyDoom
- NetSky
- Sasser
- Zeus
- Koobface
- Conflicer
- Stuxnet
- Aurora
- Anonymous
- Carbanak
- BlackEnergy
- Corkow/Metel

Распространенные заблуждения

Использование передовых технических решений по защите информации

Наиболее популярные и традиционные средства защиты	Используемые методы обхода при целевых атаках и APT
Контроль трафика на пограничных маршрутизаторах	Использование SSL, защищенных контейнеров/файлов
Пограничное межсетевое экранирование и оценка метаданных трафика	Использование для коммуникаций разрешенных протоколов (HTTP, SMPT, DNS и т.д.)
Межсетевой экран на рабочей станции и оценка метаданных трафика	При начальной эксплуатации проводится изменение локальных правил
Системы обнаружения и предотвращения вторжений	Для коммуникаций используются стандартные протоколы, порты и скрытые каналы
Антивирусное обеспечение на серверах и рабочих станциях	Компиляция перед атакой, проверка на популярных антивирусах с последними обновлениями
Ежемесячная/ежеквартальная оценка уязвимостей	Используются неизвестные уязвимости, а также методы социальной инженерии
Использование двухфакторной аутентификации	Заражение происходит с правами аутентифицированного пользователя

Наличие сертификатов соответствия стандартам по информационной безопасности

- **Сертификация не покрывает все бизнес-процессы компании**
- **Не защищают от уязвимостей нулевого дня/технических закладок**
- **Эффективность контрольной среды за отдельный период времени**

Сертификат соответствия стандарту говорит о том, что сертификационный орган (проверяющая сторона) получил резонную и достаточную уверенность в выполнении формальных требований объектом проверки

Ключевые замечания о целевых атаках

Необязательно использование 0-day

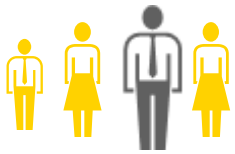
Практика показывает, что для успешного проникновения в корпоративную сеть, кибер-преступники используют зарекомендовавшие себя методы. Использование уязвимостей 0-day (уязвимости, для которых еще не выпущено бюллетеней безопасности) является дорогостоящим мероприятием. Например, 0-day exploit для Apple iOS стоит $1 млн.

Атака может быть через внешний /неконтролируемый периметр

Наш опыт подсказывает, что в некоторых случаях атака выполняется через внешний периметр: внешний сайт Компании, атака на поставщиков услуг или поставщика оборудования. Например, производится закупка оборудования с предустановленным зловредным программным обеспечением (из-за скомпрометированной сети поставщика/производителя оборудования).

Атака может быть выполнена через средства защиты

Внедрение новых средств защиты не означает повышение уровня безопасности. Так, в одном из продуктов антивирусной компании с мировым именем было раскрыто несколько 0-day уязвимостей. Также следует помнить о человеческом факторе: хранение файлов конфигураций в открытом виде, незашифрованные пароли и т.д.

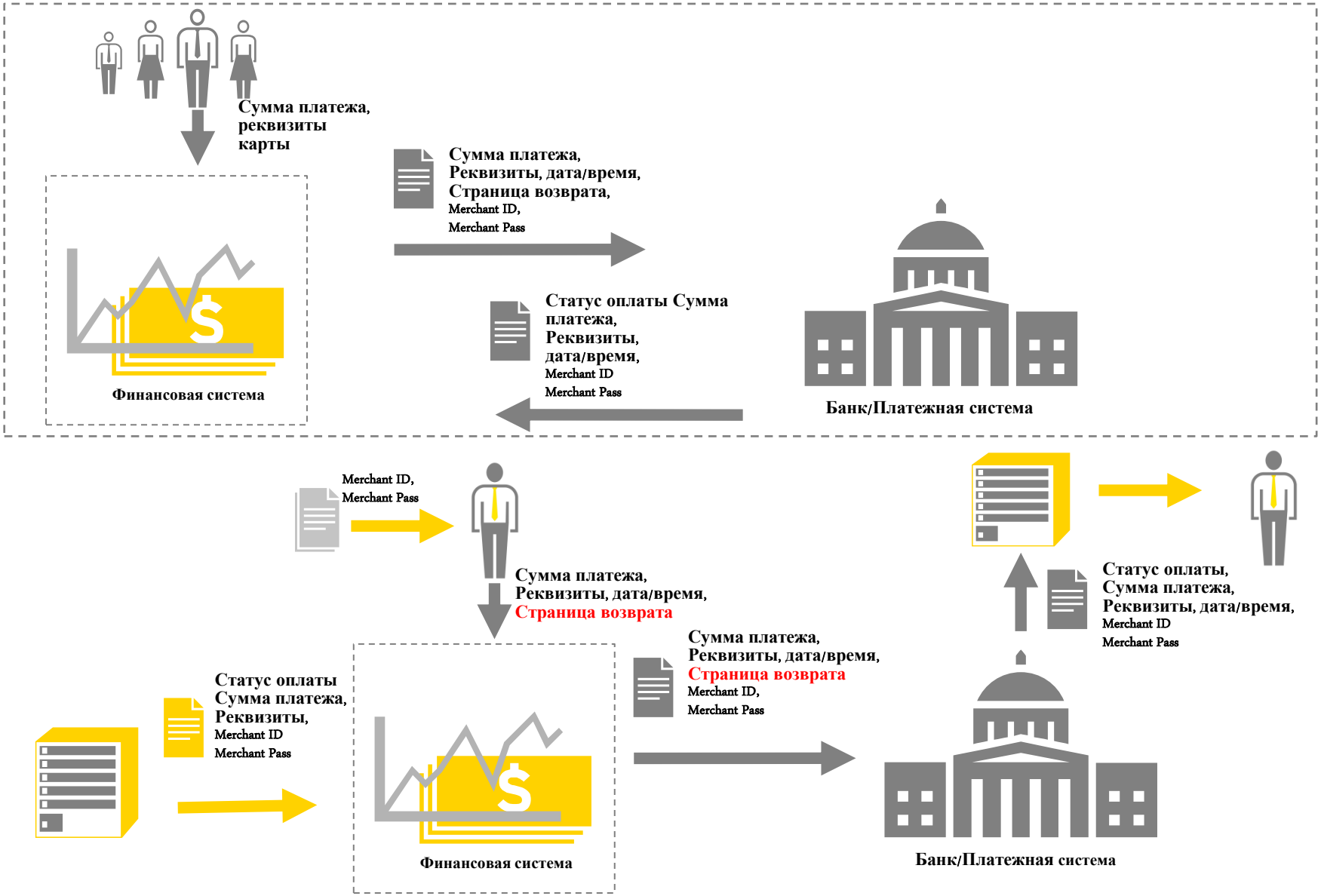


Самый простой способ проникновения в сеть – человеческий фактор

По статистике, наиболее успешным методом проникновения является атака на сотрудников Компании.

APT, Advanced Persistent Threat – Угроза с продвинутыми методами обеспечения постоянного присутствия. Данная история вовсе не о том, как выбирается цель, является ли атака спонсируемой, какова квалификация киберпреступников, какие методы проникновения используются т.п., а о том, каким образом киберпреступникам удается оставаться незамеченным в корпоративной системе на протяжении длительного времени.

Демонстрация возможного финансового ущерба



Почему сложно противостоять угрозам ИБ

 Чрезмерно уверенный в своих силах ИТ- и ИБ-персонал компании	► Отсутствие зарегистрированного инцидента не означает, что инцидента не было ► Вход в сеть может быть осуществлен через неконтролируемый периметр
 Неэффективный ситуационный центр информационной безопасности (SOC)	► Выполняются только функции мониторинга ► Подключена не вся инфраструктура компании ► Устаревшие технологии (SOC 1.0/SOC 2.0)
 Растянутые во времени действия злоумышленников	Атака выполняется в нефиксированные промежутки времени, хаотично, непредсказуемо, с использованием сложных механизмов сокрытия присутствия
 Бесконтрольное использование разнородных технологий	Атака осуществляется с использованием «маловероятных» векторов, например, IoT (принтеры)
 Неэффективное управление бюджетом	► Инвестиции в необоснованные решения защиты ► Сокращение штата ИТ/ИБ ► Непонимание всех последствий угроз
 Непонимание службой ИТ/ИБ принципов построения контрольной среды и процессов управления ИБ	За границами Проекта остаются процессы, связанные, например: с управлением изменениями, управление активами/лицензиями, разделение полномочий, управление операционными рисками, управление поставщиками

Для построения эффективной программы управления кибербезопасностью должен использоваться комплексный подход, включающий в себя организационно-технические меры и механизмы активной защиты

Контакты:

Андрей Абашев

Старший Менеджер

Тел: +7 (495) 641-2991

Andrey.Abashev@ru.ey.com

EY

Совершенствуя бизнес,
улучшаем мир