Информзащита
Системный интегратор

Расслоение рынка ИБ в России

Характерные проблемы для каждого уровня зрелости

WWW.INFOSEC.RU

О нас

Команда анализа защищенности ГК Информзащита это:

- 14 экспертов в области анализа защищенности;
- более 100 проектов по тестированию безопасности за последние 2 года;
- успешное проникновение и демонстрация возможности нанесения вреда в 8 случаев из 10.

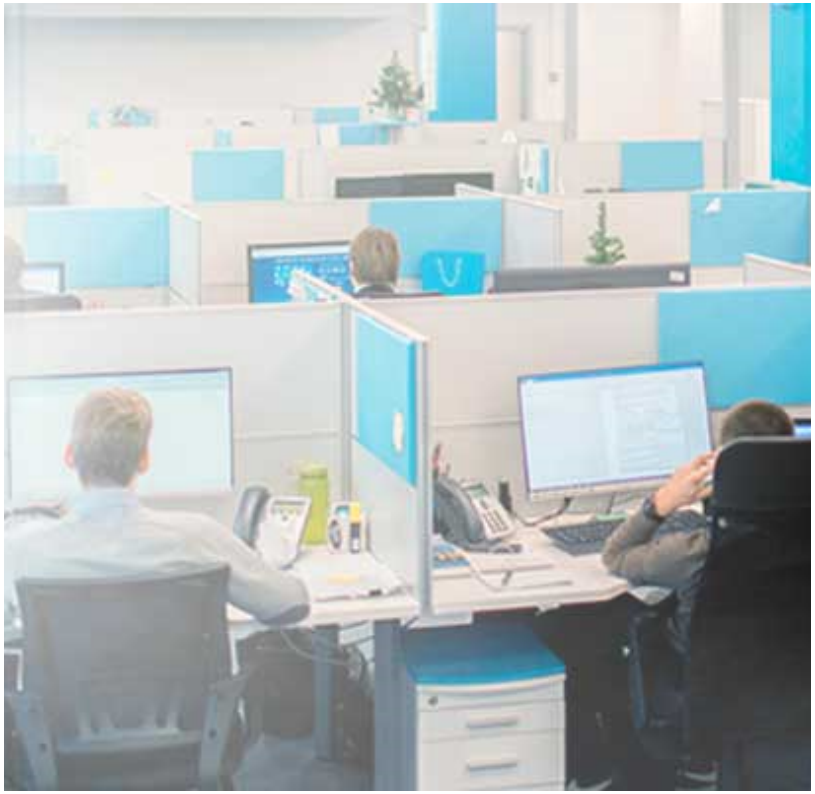
Аналитика для исследования

В качестве базиса для исследования мы использовали следующие источники:

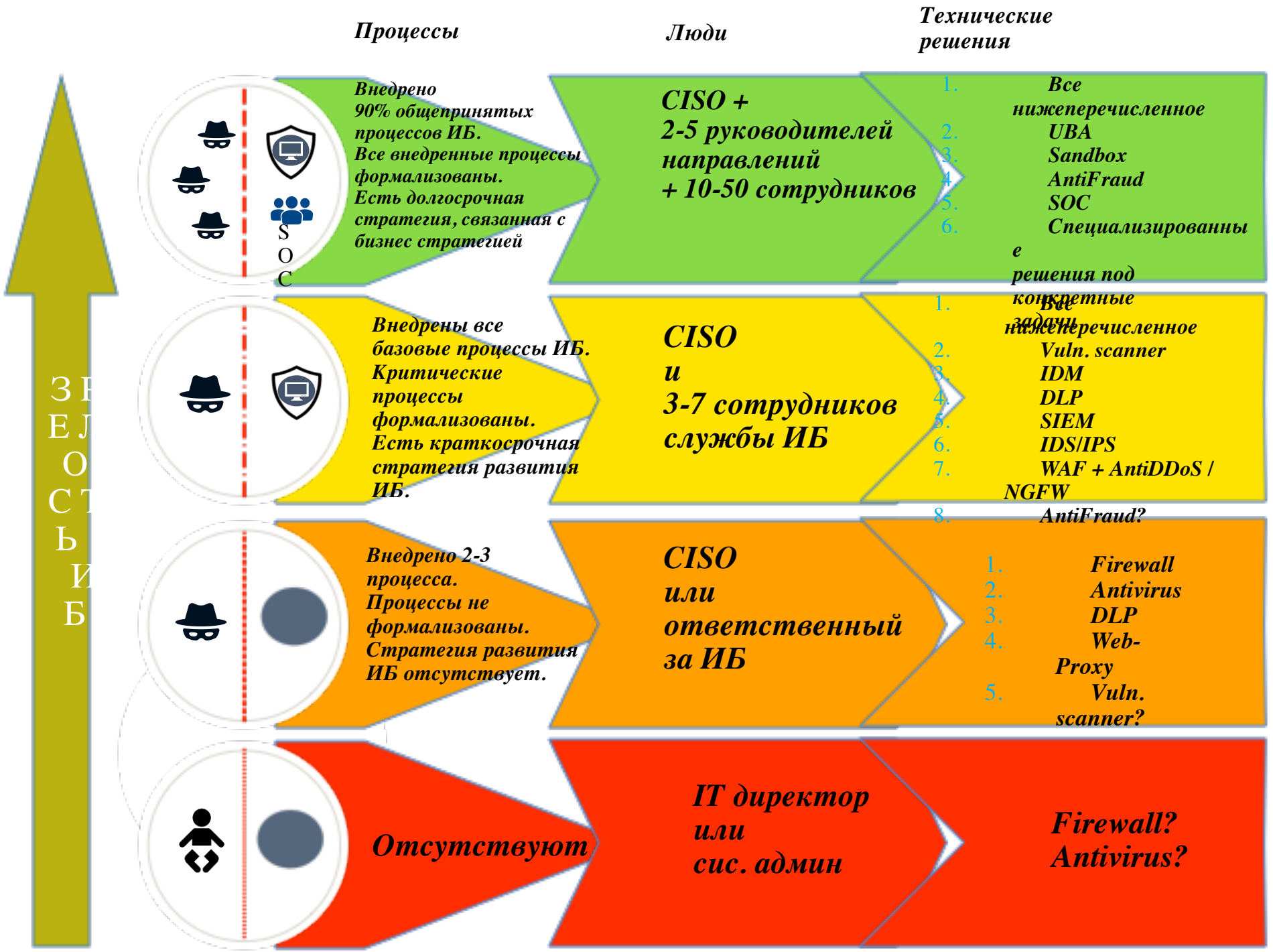
1. *Аналитика результатов выполнения проектов за последние 2 года;*

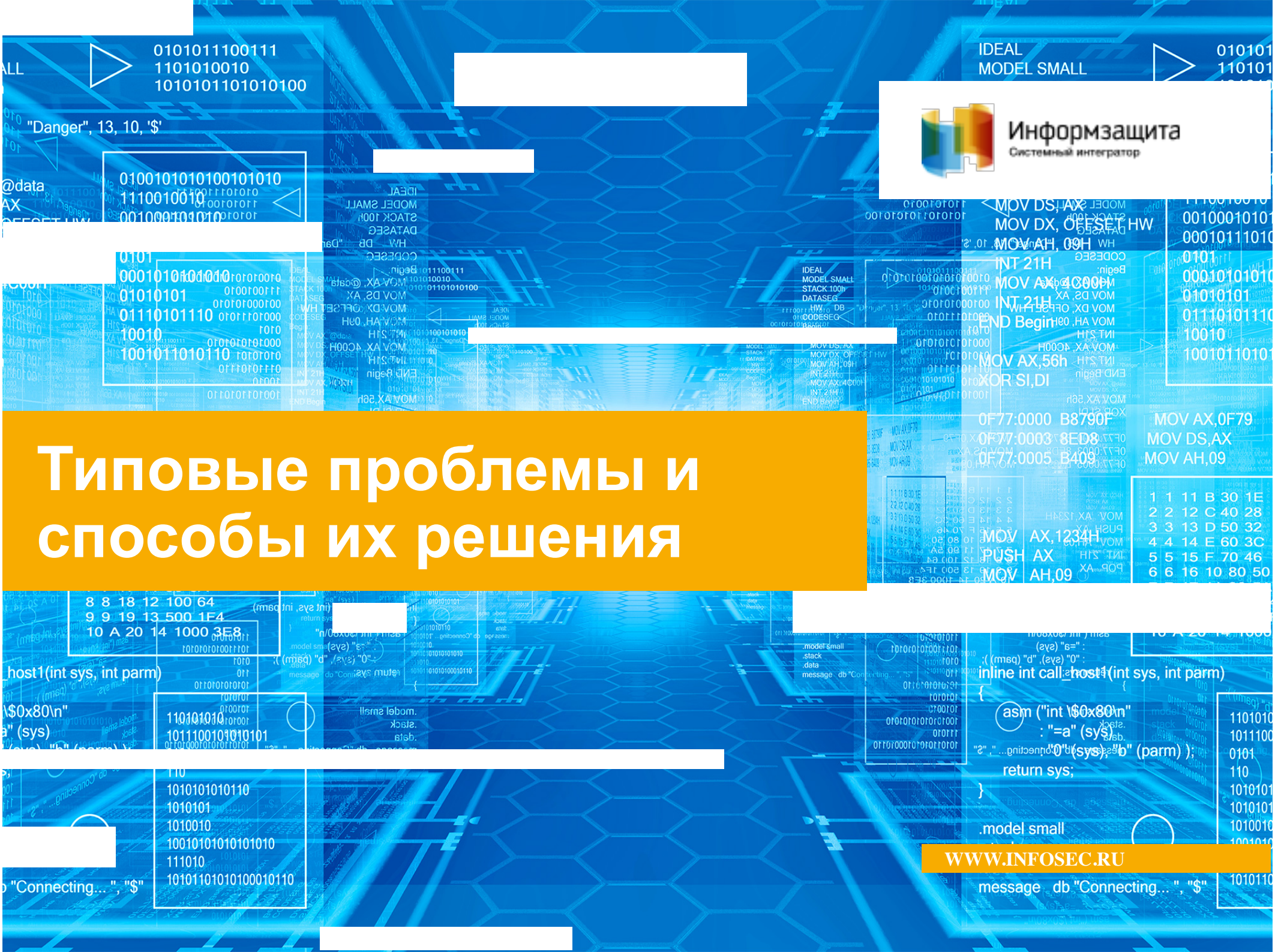
2. *отчеты исследовательского центра ГК Информзащита по таргетированным атакам;*

3. *тренды успешных кибератак за последние 2 года во всем мире.*



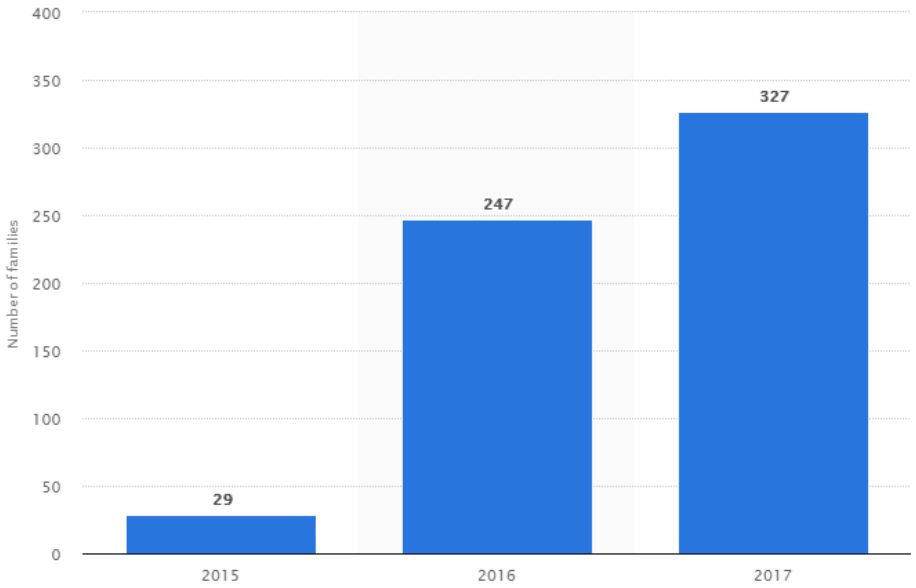
Расслоение рынка ИБ




Информзащита
Системный интегратор
Типовые проблемы и способы их решения
WWW.INFOSEC.RU

Актуальные угрозы для компаний с нулевым уровнем зрелости ИБ

Ransomware



Количество новых обнаруженных экземпляров Ransomware

Уязвимые веб-приложения

Quick Wins

1. *Осознать и принять тот факт, что злоумышленникам интересно все до чего они могут дотянуться.*

2. *Быть защищеннее соседа.*

3. *Использовать облачные решения ИБ и ИТ.*

Актуальные угрозы для компаний с низким уровнем зрелости ИБ

Устаревшие системы

82%

Процент компаний у которых за 2 года мы обнаружили уязвимости из семейства MS17-010. В 95% случаев это приводило к компрометации всей инфраструктуры

Слабые пароли

В среднем 1 пароль, длинною 8 символов без спецсимволов можно взломать за 1 час.

Существует облачный сервис которые взламывает пароль из 10 символов, за 15 минут. Стоит такая операция 10$.

Quick Wins

1. *Использовать сканеры уязвимостей для непрерывного мониторинга собственного состояния защищенности.*

2. *Провести аудит информационной безопасности, и на основании результатов разработать стратегию развития ИБ на ближайшие 3 года.*

3. *Быть защищеннее соседа*

Актуальные угрозы для компаний с средним уровнем зрелости ИБ

Забытые системы

67%

Компаний имеют один или несколько серверов за которые никто не отвечает. О них просто забывают.

Недостаточная осведомленность

В 2018 году только 3% вредоносного ПО эксплуатировала только технические уязвимости. 97% включала в себя атаки методом социальной инженерии.

Quick Wins

1. *Проанализировать наличие и эффективность таких процессов ИБ как:*
   управление активами;
   управление изменениями;
   управление уязвимостями.

2. *Уделить отдельное внимание процессу управления рисками.Для компаний среднего уровня зрелости, это один из самых критичных процессов ИБ.*

3. *Проводить регулярные упражнения по анализу защищенности инфраструктуры.*

Актуальные угрозы для компаний с средним уровнем зрелости ИБ

Недостаточный контроль
за действиями привилегированных
учетных записей

100%

захватов доменной инфраструктуры происходит из-за недостаточного контроля за действиями следующих групп пользователей:

- доменные администраторы;
- внутренняя разработка;
- служба поддержки.

Недостаточный контроль поставщиков

Юнистрим

MyFitnessPal **HackingTeam**

Equifax **Universal Music Group**

US DoD + Pentagon **Silence**

Stuxnet **US Democratic Party**

Все это компании/хакерские атаки, которые в основе своей содержали атаку через 3-х лиц.

Использование 0-day уязвимостей, на самом деле является частным случаем атаки через поставщиков.

Quick Wins

1. ***Принцип нулевого доверия***

2. *Введение дополнительных мер по обеспечению контроля за привилегированными сотрудниками.*

3. *Введение дополнительных требований ИБ к поставщикам и третьим лицам имеющим доступ к инфраструктуре.*

4. *Обеспечение физической и информационной безопасности первых лиц компании.*

Информзащита
Системный интегратор

Выводы

WWW.INFOSEC.RU

Выводы

- Безопасность это проблема любой компании, а не только тех которые у всех на виду.
- Для компаний с маленькими бюджетами, достаточно для начала быть защищённые своих соседей. В таком случае к ней придут в последнюю очередь и она успеет подготовиться.
- Четкое понимание рисков ИБ для вашей компании, это ключ к построению надежной инфраструктуры. Но нельзя забывать, что риски имеют тенденцию меняться с каждым изменением внутри компании.
- Принцип нулевого доверия. При интеграции сторонних компаний в свою инфраструктуру необходимо проводить анализ рисков, в идеале он должен включать независимый аудит ИБ поставщика.

Спасибо за внимание

Вопросы?