Кибербразведка и поверхность атаки

Алексей Томилов

Технический директор FINDLER

Современные киберугрозы

Киберугрозы, с которыми компании сталкиваются в реальной жизни.

- **Шифрование инфраструктуры**
- **Кража/слив персональных данных**
- **Финансовые убытки**
- **Репутационные потери**
- **Штрафы от регуляторов**

Кибербразведка

— это процесс получения информации о возможных уязвимостях компании через ее поверхность атаки.

Кибербразведка, первый шаг для дальнейшей атаки на компанию.

Поверхность атаки

Это все точки, через которые возможен доступ к системе компании.

- **Внешние IP-адреса**
- **Веб-сайты и приложения**
- **Публичные базы данных**
- **Уязвимости в программном обеспечении**

Периметр компании

Это совокупность всех IT-ресурсов и сетей, доступных извне.

Плюсы для атакующего:

Актуальность информации

Атакующий получает данные в реальном времени.

Возможность эксплуатировать уязвимости на лету

Как только обнаружена уязвимость, ее можно использовать мгновенно, прежде чем компания успеет ее исправить.

Минусы для атакующего:

Могут обнаружить

При активном мониторинге трафика, компания обнаруживает подозрительную активность и может блокировать атакующего.

Подрядчики

Риски, связанные при работе с подрядчиками.

Плюсы для атакующего:

Невидим для средств защиты

Часто подрядчики не соблюдают высокие стандарты информационной безопасности, что упрощает доступ к их инфраструктуре.

Больше целей для атаки

Подрядчики могут работать с множеством клиентов, открывая доступ к более широкому кругу целей через одну успешную атаку.

Минусы для атакующего:

Больше работы

Взломать подрядчика, а затем продвинуться к основной цели — процесс требует больше усилий.

Неактуальные данные о цели

У подрядчиков может не быть самой свежей информации о защищаемой системе.

Сотрудники

Проблемы безопасности — человеческий фактор.

Плюсы для атакующего:

Остается незаметным

Атаки могут маскироваться под действия сотрудников, что затрудняет расследование.

Минусы для атакующего:

Навыки соц.инжиниринга

Для успеха злоумышленнику нужно обладать определенными Soft Skills.

Больше работы

Взлом сотрудника может не дать моментального доступа к целям, что усложняет атаку.

Как выжить?

Рекомендации для бизнеса по защите.

- **Регулярные аудиты безопасности**
- **Обучение сотрудников основам информационной безопасности**
- **Меры по контролю и мониторингу**

Контроль утечек через личные устройства сотрудников

Проблема:

Сотрудники используют личные устройства и личные почтовые ящики для работы. Это создает дополнительные риски утечек.

Решение:

Внешние CRM и задачники могут хранить чувствительную информацию, а доступ к ним осуществляется через личные аккаунты.

Обсудите, как облачные решения могут увеличивать риски и как их контролировать.

«Работа» с подрядчиками

Важно осознавать, что подрядчики могут стать слабым звеном.

Риски при взломе подрядчика

Главное понимать: Что произойдет, если подрядчик взломан? Какие данные может получить атакующий?

Ограничения по законодательству

Сканировать подрядчиков нельзя, но можно мониторить учетные записи, которые используются для взаимодействия с вашей компанией.

Разработчики и тестовые контуры

Подрядчики, особенно разработчики, могут небрежно хранить тестовые системы, что может стать источником утечек.

Всегда знать актуальную информацию о своих активах

Доменные имена/IP-адреса

Важно постоянно обновлять список своих активов и понимать, какие из них подвержены рискам.

Открытые порты и уязвимости

Регулярный мониторинг и закрытие неиспользуемых портов.

Пароли, которые утекли

Проверять и изменять уязвимые пароли, которые были скомпрометированы в результате утечек.

Киберразведка и поверхность атаки

Алексей Томилов

Технический директор FINDLER

Findler
by RebrandyCo