Агентство Активного Аудита
Мы знаем ВСЕ об информационной безопасности

Всеукраинский форум «ДНИ ИНТЕРНЕТ – МАРКЕТИНГА»

Информационная безопасность компании - как не подарить кибермошенникам Ваш бизнес

Владимир Ткаченко
Директор ООО «Агентство активного аудита»

ТОП 10 киберугроз применительно к Украине:

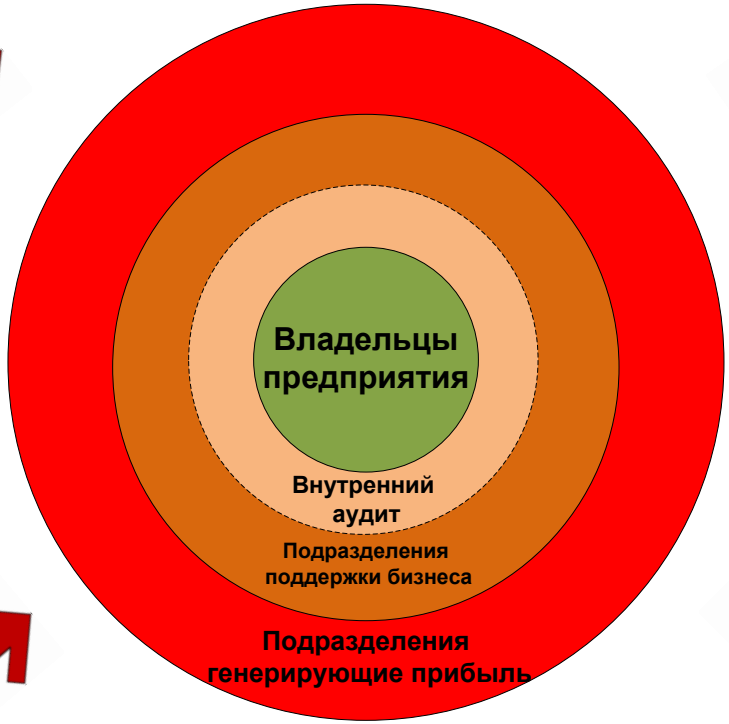
- Мошенничество с помощью систем ДБО;
- Высокая степень уязвимости к приемам социальной инженерии;
- ПО на стороне клиента продолжает оставаться необновленным даже после выпуска патчей;
- Слабая организация управления ИБ;
- Отсутствие риск менеджмента в отношении информационных активов (1С и др. БД);
- Уязвимости WEB-сайтов и WEB-приложений использующихся через Internet;
- Уязвимости беспроводных сетей предприятия (Wi-Fi, CDMA, GSM, IP Telephony)
- Рост количества и сложности DDoS как способа конкурентной борьбы;
- Рост количества 0-day уязвимостей;
- Несоблюдение рекомендаций производителей ПО и оборудования по настройке параметров безопасности

SOPHOS
SANS
Trustwave
GROUP-IB
pwc
verizon
Національний банк України
Active Audit Agency

Идеальный подход к защите бизнеса

Государство
(законы, налоги, A1H1…)

Партнеры
(поставщики, посредники…)



Конкуренты
(целенаправленные злонамеренные действия)

Клиенты

Практическая реализация защиты бизнеса и ИТ инфраструктуры предприятия

Факты по картам

- В своем письме банкам от 15.04.2010 № 25-312/943-5139 НБУ отмечает что «Кількість шахрайських операцій з використанням платіжних карток … становила 6 304 тис. грн.», т.е. 6 млн. 304 тыс. грн. (Fake ATM – в Караване, fake Internet shop, phishing, vishing, skimming, trojan horses, SMS phishing, кражи карточных данных в торговых точках, АЗС и т.п.)

Факты по ДБО

- Мировая тенденция уже в Украине (25% наших клиентов пострадали от подобных операций);
- В основном угрозы через вирусы (троянские кони) и собственный персонал (небрежное хранение ключевых данных к ДБО). Примеры: ZeuS, Trojan.PWS.OSMP, Trojan.Tatanarg и др. ;
- «Черкасское дело» (март-апрель 2011г) – 7 млн. грн.

Как избежать рисков?

- ✓ **Процедуры хранения и применения ключей и паролей ДБО**
- ✓ **Фильтрация по IP-адресу и другим признакам**
- ✓ **Элементарные меры защиты (антивирус, сканер уязвимостей, осведомленность)**

Как определить потребность в продуктах ИБ?

Данные для принятия решения	Описание
Анализ ИТ рисков	Позволяет определить наиболее критичные ресурсы подверженные наиболее вероятному перечню угроз + возможность оптимально резервировать ресурсы для решения задач ИБ, возможность измерить риск в бизнес терминах - процесс, требующий ресурсов (квалификация и методология)
Статистика инцидентов ИТ (ИБ)	Объективная совокупность фактов, позволяющая проводить статистический анализ характера и особенностей инцидентов, а также их природы
Внутренний или внешний аудит ИТ	Оценить, а, где это возможно, сравнить выполнение процессов с политикой СУИБ (требованиями стандартов и/или регуляторов), целями и практическим опытом и доложить результаты менеджменту (руководству) для анализа.
Тест на проникновение	Достаточно быстрый способ определить РЕАЛЬНЫЕ уязвимые места в инфраструктуре и определить процессы ИТ, требующие улучшения. + относительно быстро (до 1-2 мес), возможно охватить большинство критичных ресурсов и процессов (в том числе аспекты физической безопасности) - ограниченный финансовый ресурс ☺

Стандарты ИБ

- ✓ ISO 27001 – открытие для ИТ директоров предприятий
- ✓ ISO 18044 – откровение для ИТ и бизнеса
- ✓ CoBIT – это что-то только у «них там на западе» и «у нас не работает»
- ✓ Купим Антивирус, WEB-фильтр, IDS/IPS, DLP (нужное подчеркнуть) и все будет ок
- ✓ PCI DSS и PA-DSS – для тех кто собирается принимать платежи пластиковыми карточками, но по прежнему надеется что-как нибудь само решится…
- ✓ Закон Украины №2297-17 от 01.06.2010 «О защите персональных данных» - один для всех?
- ✓ Другие идеи и инициативы в Украине о защите информации (регуляторы ГССЗЗИ, НБУ, ГСПЗПД и другие сложные аббревиатуры)

0,5 слова о защите ПДн

Агентство Активного Аудита
Мы знаем ВСЕ об информационной безопасности

1 Инвентаризация и подготовительные действия к внедрению СУОПДн

- Подготовительные действия
- Инвентаризация баз ПДн
- Описание баз ПДн

- Приказ об организации работ по проекту
- Приказ о назначении ответственных лиц за СОУПДн
- Внесение изменений в должностные обязанности ответственных лиц.
- Реестр баз персональных данных предприятия
- Приложение к Реестру с описанием баз ПДн
- Реестр владельцев баз персональных данных

2 Определение текущего состояния СУОПДн (аудит)

- Сбор и анализ информации
- Определение критичности баз ПДн
- Подготовка отчета


Отчет по результатам аудита


Презентация результатов аудита руководству

3 Определение мероприятий защиты в отношении баз ПДн

- Определение мероприятий по защите
- Создание политик и процедур
- Определение порядка обработки ПДн

- План мероприятий защиты
- «Порядок обработки ПДн на предприятии»
- Процедуры и политики по обработке и хранению баз ПДн

4 Внедрение СОУПДн

- Устранение недостатков
- Уведомление субъектов ПДн
- Постановка необходимых процессов.
- Регистрация баз в Гос. реестре
- Согласование «Кодекса» со Службой

- Процессы обновления, хранения и утилизации баз ПДн
- Процесс уведомления субъектов персональных данных + формы уведомлений
- Зарегистрированные в ГРБПДн базы ПДн
- Согласованный со службой «Порядок обработки ПДн»

Тест на проникновение

Основные цели тестирования систем(ы) или приложения на устойчивость ко взлому:

- **Снизить потенциальный (финансовый и репутационный) ущерб от реализации угроз;**
- **Определить эффективность принятых мер безопасности для защиты от внешних угроз (из сети Интернет);**
- **Оценить устойчивость систем(ы) или приложения к наиболее распространенным видам внешних атак;**
- **Защитить потенциальных пользователей систем(ы) или приложения от компрометации их данных или других мошеннических действий;**
- **Получить оценку независимых экспертов о степени защищенности системы**

Из жизни …

Из обнаруженных уязвимостей:

1) Межсайтовое выполнение сценариев (Cross-Site Scripting) на странице http://fart.com.ua/search.php.

2) Использование простых паролей позволило аудиторам развить атаку и получить полный доступ к серверу.

3) Обнаружены сторонние PHP скрипты, вероятней всего сайт уже был взломан или скрипт был оставлен сотрудниками компании с неизвестной целью.

Также было обнаружено:

- лицензия на ПО управления сайтом истекла, и в дальнейшем сайты не смогут получать обновления;
- протоколирование действий в системе средствами сайта отключено, что позволяет потенциальному злоумышленнику остаться необнаруженным;
- ПО сервера обновляется не постоянно;
- пользователь www имеет доступ к файлам и папкам за пределами своей домашней директории;
- разграничение прав доступа к файлам на WEB- сервере не настроено;
- учет изменений на сервере не ведется.

DDoS – метод конкурентной борьбы

- 25 % наших клиентов сталкивались с DoS
- Тенденция – ботнеты состоят не только из ПК, но серверов и сетевого оборудования
- Стоимость DDoS 300-500 USD в зависимости от задачи и требуемых ресурсов
- Украина создает 12% Ddos трафика в мире (2 е место) 2012 г!!!!

Громкие DDoS в Украине:

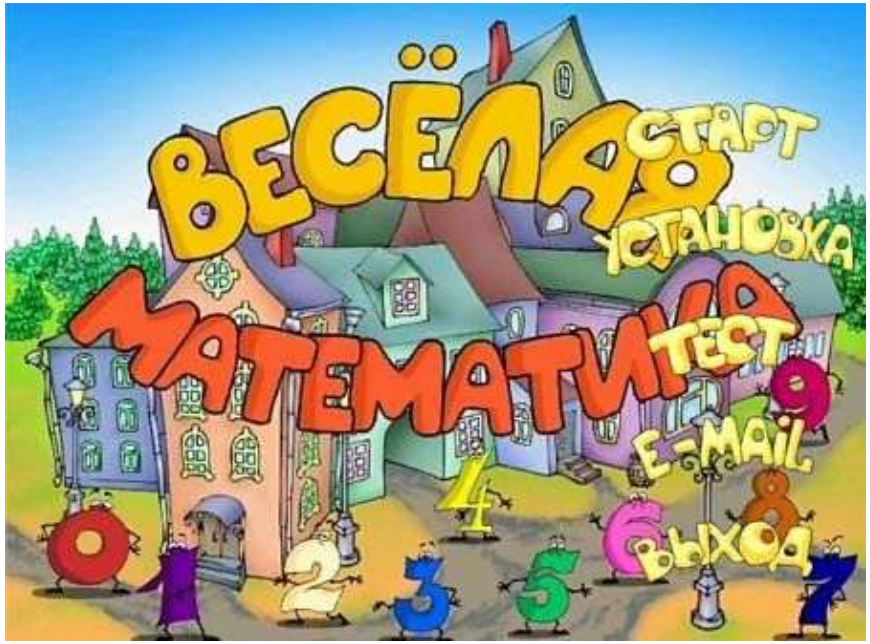
1) 29.01.2010 – DDoS на сайт security.ua, 23.03.2010 – UA-Reporter.com;
2) Конец августа 2010 г – imena.ua/mirohost.net (2Гбит/с, ZeuS, 3 млн. компьютеров ботнет);
3) 8 октября 2010 г. – Укртелеком (ухудшение качества доступа в Internet);
4) Конец января –начало февраля 2012 – атаки на сайты органов власти - (EX.UA);
5) На этой неделе – 19.03.2012 – сайт РБК-Украина

Александр Ольшанский (президент Imena.ua) сообщил: *«К сожалению, у нас DDOS-атаки стали привычным инструментом **политической** и **конкурентной борьбы**, который используют для воздействия на неугодные сайты или шантажа электронных магазинов. Зло это общемировое, и Украина здесь далеко не впереди планеты всей. Тем не менее и в нашей стране в течение ближайших 2-3 лет проблема DDOS-атак приобретет серьезную актуальность и будет требовать соответствующих решений как от владельцев интернет-ресурсов, так и от хостинг-провайдеров».*

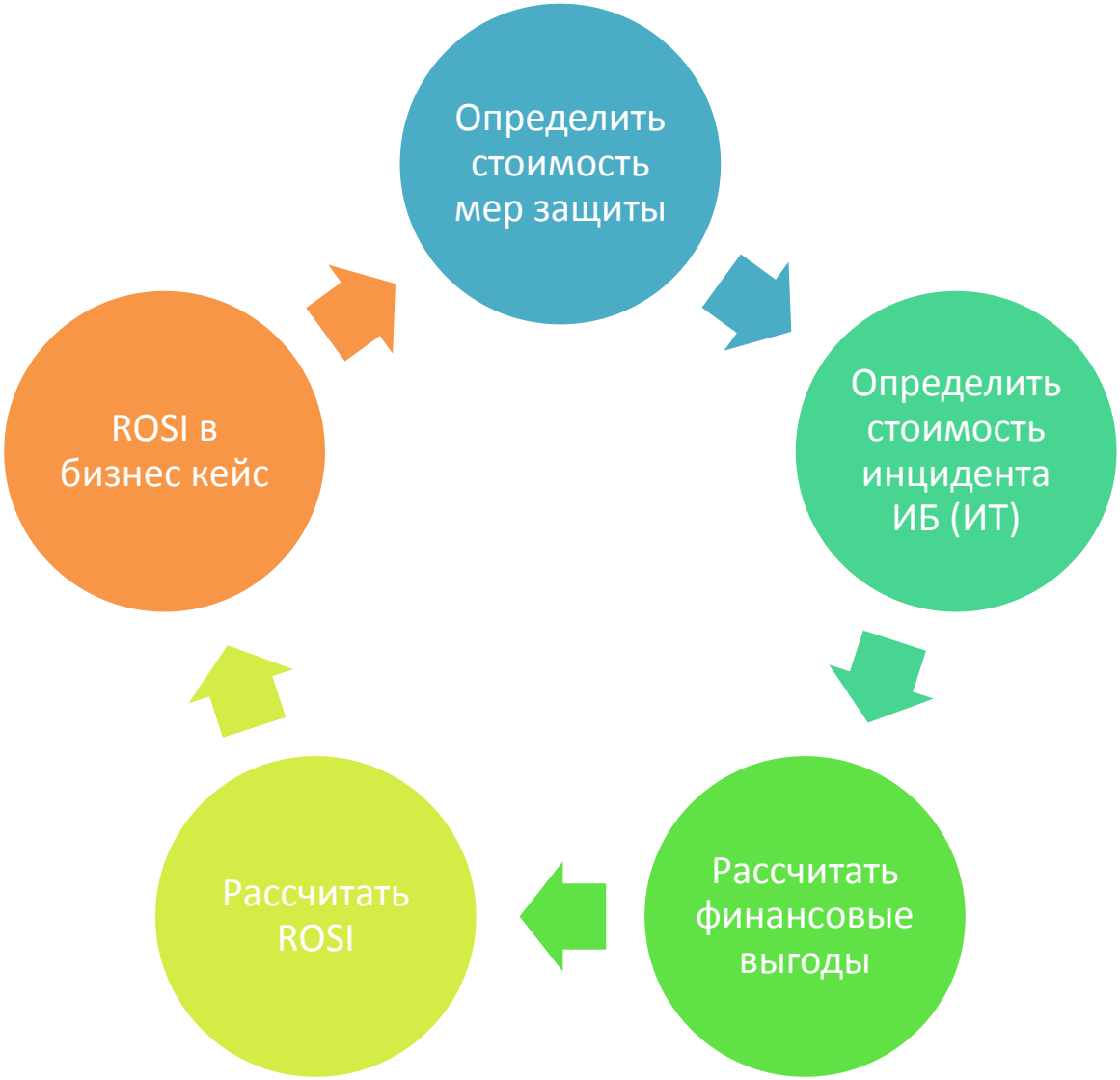
Затраты на ИБ

Затраты на ИБ –

- ✓ Стоимость квалифицированных специалистов
- ✓ Стоимость мероприятий по обеспечению безопасности и их поддержка
- ✓ Накладные расходы
- ✓ Обучение и повышение квалификации (или осведомленности) сотрудников
- ✓ Затраты на реакцию на инциденты



Как с этой фигней взлететь?



Выводы

Перед началом проекта

- ✓ Оценить риски (в т. ч. информационные)
- ✓ Выделить бюджет на оценку защищенности
- ✓ Разработать мероприятия по обеспечению безопасности и их поддержке

Во время проекта

- ✓ Разграничение среды разработки, тестирования и производственной
- ✓ Выявлять риски по мере возможности
- ✓ Подерживать мероприятия по безопасности
- ✓ Провести опытную (тестовую) эксплуатацию

После ввода в эксплуатацию

- ✓ Мониторинг событий
- ✓ Анализ рисков (пересмотр) периодически
- ✓ Регистрировать изменения в системе (системах)
- ✓ Периодически проводить оценку защищенности

Вопросы

Агентство Активного Аудита
Мы знаем ВСЕ об информационной безопасности

v.tkachenko@auditagency.com.ua

www.auditagency.com.ua

044 2281588