Как ИБ-компании обманывают своих клиентов

Алексей Лукацкий

Бизнес-консультант по безопасности

Цель ИБ-компании – безопасность

- Вам говорят

  Свою миссию компания X видит в том, чтобы обеспечить своим клиентам безопасное ведение бизнеса при использовании современных информационных технологий…

- Что на самом деле

  Надо добавить «и заработать на этом деньги!»

  Цель коммерческой компании – увеличение своей доходности за счет роста числа клиентов, роста стоимости услуг, снижения их себестоимости…

Обнаружение неизвестных вирусов

- Вам говорят

  Эвристический анализатор X обнаруживает неизвестные вирусы

- Что на самом деле

  Обнаружение неизвестных вирусов… по характерным для вирусов действиям

  «*Эвристическое сканирование является во многом вероятностным методом поиска вирусов*» – Е.Касперский

  «*Антивирусные компании практически мгновенно выпустили вакцины, однако сразу возникла проблема: червь начал мутировать*»

Обнаружение неизвестных вирусов

- Что на самом деле

  «*Защита от данной вредоносной программы уже добавлена в базу данных*»

  «*К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие антивирусного программирования идёт в сторону увеличения количества обнаруживаемых вирусов, а не в сторону улучшения их детектирования*» - ВМиК МГУ и ИСП РАН

  Если бы антивирус мог обнаруживать неизвестные вирусы, то их не надо было бы обновлять и выпускать новые версии!

Обнаружение 100% вирусов

- Вам говорят

  Антивирусы X обеспечивают высочайший уровень защиты, неоднократно подтвержденный сертификатом VirusBulletin 100% Detection

- Что на самом деле

  Теоремы Райса и Успенского (50-е годы) – «*распознавание любого нетривиального свойства алгоритма является неразрешимой проблемой*»

  Фред Коэн в 1987 г. демонстрирует, что не существует алгоритма, который в полной мере может обнаруживать все вирусы

  Исследовательский центр IBM им.Томаса Ватсона (2000 г.) опубликовал исследование «An Undetectable Computer Virus», в котором доказал, что возможно существование компьютерных вирусов, которые не может обнаружить никакой алгоритм

Обнаружение 100% вирусов

- Что на самом деле

  Исследовательская лаборатория компании Hewlett-Packard в Бристоле (2004 г.) проводила исследования сигнатурных подходов – «*Сигнатурная модель имеет фундаментальные недостатки*»

  Можно попытаться приблизиться к заветному числу в 100%, но потребуется сложный математический аппарат → система будет работать медленнее → продукт будет вызывать раздражение пользователей

Сертификат ФСТЭК и защищенность

- Вам говорят

  Сертификат ФСТЭК гарантирует защищенность

- Что на самом деле

  Гарантия защищенности возможна в двух случаях – кто-то проверил защищенность на 100% и несет ответственность за это

  Можно ли проверить не комбинации, но хотя бы просто все ветвления, параметры и настройки для миллионов строк кода?

  Что насчет компилятора, который может внести закладки?

  Несет ли ФСТЭК ответственность за взлом сертифицированной системы?

  Теоремы Райса и Успенского (50-е годы) – «*распознавание любого нетривиального свойства алгоритма является неразрешимой проблемой*»

Защита персональных данных

- Вам говорят

  Вы обязаны выполнять требования ФСТЭК по защите персональных данных и мы вам в этом поможем

- Что на самом деле

  Постановление Правительства РФ от 13 августа 1997 года № 1009 «Об утверждении Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации»

  НПА должен быть подписан только руководителем федерального органа исполнительной власти (п.9)

  НПА должен быть зарегистрирована в Министерстве Юстиции (п.10-11)

  НПА должен быть опубликован в открытой печати (п.17)

Оценка рисков

- Вам говорят

  Мы оценим для вас риски и на основе этой оценки вы сможете обосновать финансирование проектов по ИБ

- Что на самом деле

  Риск = f(вероятность риска, сумма ущерба)

  Для оценки вероятности мы должны иметь статистику по конкретной компании за длительный интервал времени

  Можете ли вы оценить стоимость защищаемой информации?

  Любой финансист захочет, чтобы методология расчета была понятной и проверяемой

  Количественная оценка рисков в ИБ (конвертация трех градаций «высокий/средний/низкий» в числа - не количественная оценка) - миф

Предотвращение утечек информации

- Вам говорят

  Мы предлагаем систему контроля и предотвращения утечек информации

- Что на самом деле

  Утечка может произойти по любому из существующих каналов – электронная почта, USB, IrDA, Bluetooth, Wi-Fi, COM, Web… а также 65535 TCP-портов, ICMP (Loki), экран монитора, ЭМИН, акустика, бумага и многое другое

  Не существует DLP-систем, которые контролировали бы все эти каналы

  Квалифицированный злоумышленник всегда найдет способ унести информацию

  А еще есть проблемы с законодательством…

Токены

- Вам говорят

  Токены решают многие проблемы с безопасностью

- Что на самом деле

  И создают новые…

  В офисных организациях преимущественный контингент – женщины

  Куда женщина должна положить токен, если у нее обычно нет карманов на одежде? А если есть, то они носят декоративный характер и она не будет ничего туда запихивать, как мужчина ;-)

  В итоге токен остается на столе ;-(

Аутсорсинг безопасности

- Вам говорят

  За счет аутсорсинга безопасности мы снимаем с вас проблемы по управлению средствами защиты и вы еще и экономите

  «*Содержать штат сотрудников, которые в круглосуточном режиме будут заниматься мониторингом и отражением атак, может позволить себе далеко не каждая компания*»

  «*…имеющий в своём штате сертифицированных и высококвалифицированных аналитиков и инженеров*»

- Что на самом деле

  Управление при отсутствии хороших и резервируемых каналов связи за пределами Москвы

Аутсорсинг безопасности

- Что на самом деле

  «*Специалисты компании <имярек> выполнят следующие работы: Предоставление рекомендаций по выявленным инцидентам безопасности*» - т.е. реагировать вам придется самим

  Квалифицированный специалист по ИБ не будет заниматься рутинной работой по «просиживанию штанов за консолью»

  Если у аутсорсера работает CCIE или CISSP, а у вас его нет, то неужели его услуги будут стоит дешевле?

  Аутсорсер не дает гарантий и не несет ответственности

  Отдав ИБ на аутсорсинг, разве вы сократите свой персонал, которого и так не хватает? О какой экономии тогда идет речь?

Системы корреляции

- Вам говорят

  Наша система корреляции позволяет подключать любые системы защиты, даже отечественного производства

- Что на самом деле

  У многих систем корреляции (SIEM) действительно существует «универсальный агент», который позволяет собирать сигналы тревоги от различных средств защиты

  Но смысл системы корреляции в корреляции (поиске взаимозависимостей) атак и уязвимостей, а не просто сборе и хранении событий

  Корреляция реализуется за счет правил, которых для неизвестных систем нет

  Вам придется самостоятельно писать эти правила, что является нетривиальной задачей или… заплатить деньги продавцу системы

Средства подавления DDoS-атак

- Вам говорят

  Купите средства подавления DDoS-атак и вы будете спасены

- Что на самом деле

  Установив средства подавления DDoS-атак вы не защитите Интернет-канал от себя до оператора связи – он будет все равно забит

Сертификат по «Общим критериям»

- Вам говорят

  Наша система сертифицирована по «Общим критериям»

- Что на самом деле

  В отличие от сертификатов ФСТЭК по РД, сертификация ОК проводится на соответствие заданию по безопасности, которое помимо требований по защите (а-ля РД) содержит конкретную модель угроз

  Это значит, что ЗБ для одного заказчика не может быть использовано для другого (модели угроз будут разные)

  На практике модель угроз в ЗБ прописывается минимальная

  Сертификация Windows XP Professional Service Pack 1a «*на соответствие реализованных в операционной системе функций защиты и задекларированных в задании по безопасности*»

Сертификат по «Общим критериям»

- Что на самом деле

  ЗБ на Windows 2000 содержит всего 9 (!) угроз, а для Windows XP всего 5 угроз

  В ЗБ на Windows 2000 написано, что Microsoft не несет ответственности за все, что творится за пределами Windows 2000. Перехват трафика? Пожалуйста. Утечка через инфракрасный порт, Bluetooth-, WiFi-адаптер или Flash-диск? Последние три периферийных устройства вообще не указаны в списке разрешенных на сертифицированных машинах Windows 2000

  Проверке подвергается не только ОС Windows 2000, но и компьютер, на которую она устанавливается. В сертификате четко прописаны модели компьютеров - Compaq Proliant ML570 и ML330, Compaq Professional Workstation AP550, Dell Optiplex GX400, Dell PE 2500, 6450, 2550 и 1550

Защищенный компьютер

- Вам говорят

  ОС Windows - незащищенная. Мы предлагаем вам СЗИ от НСД по 3-му классу СВТ + электронный замок, который будет контролировать целостность до загрузки ОС

- Что на самом деле

  В 1995 году на симпозиуме IEEE прозвучал доклад трех американских исследователей (Олин Сайберт, Филлип Поррас и Роберт Линделл) «An Analysis of the Intel 80x86 Security Architecture and Implementations»

  Обнаружено множество недокументированных узлов и каналов, скрытых каналов и т.п.

  Intel 8086, 80286, 80386, 80486, Pentium, AMD, Cyrix и т.д.

Проверки регуляторов

- Вам говорят

  Если вы не купите наши системы защиты, имеющие сертификат, то когда к вам придут с проверкой, то накажут. А проверить вас могут когда захотят

- Что на самом деле

  Любой орган государственного надзора и контроля (ФСТЭК, ФСБ или Роскомнадзор) должен проводить свои проверки в строгом соответствии с ФЗ от 14.07.2001 №134 «О защите прав юридических лиц и индивидуальных предпринимателей при проведении государственного контроля (надзора)»

  Презумпция добросовестности – вы невиновны, пока не доказано обратное

Проверки регуляторов

- Что на самом деле

  «…*открытость и доступность для юридических лиц и индивидуальных предпринимателей нормативных правовых актов, устанавливающих обязательные требования, выполнение которых проверяется при проведении государственного контроля (надзора)*»

  Ревизор должен представить правовые основания проведения проверки

  «*Плановое мероприятие по контролю может быть проведено не более чем один раз в два года*» (для малого бизнеса – раз в три года)

  «*Нормативные правовые акты, принятые органами государственного контроля (надзора) в нарушение законодательства Российской Федерации, признаются недействительными полностью или частично в порядке, установленном законодательством Российской Федерации*»

Проверки регуляторов

- Что на самом деле

  Внеплановая проверка осуществляется для контроля исполнения выданных ранее предписаний или при «*обращении граждан, юридических лиц и индивидуальных предпринимателей с жалобами на нарушения их прав и законных интересов*»

  «*Обращения, не позволяющие установить лицо, обратившееся в орган государственного контроля (надзора), не могут служить основанием для проведения внепланового мероприятия по контролю*»

ГОСТ 28147-89 и другие ГОСТы

- Вам говорят

  Наше решение использует ГОСТ шифрования, а значит мы легитимны перед законом

- Что на самом деле

  С точки зрения закона в России есть сертифицированные решения, несертифицированные и выпадающие из системы сертификации (мобильники, шифрование менее 56 бит, Wi-Fi с диапазоном до 400 метров и т.д.)

  Постановление Правительства 957

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410