Информационная безопасность. Мировые тренды и направления развития

Информационная безопасность

Для выступления на заседании Круглого стола «О законодательных мерах обеспечения информационной безопасности в экономической сфере при использовании программного обеспечения и оборудования на объектах критической информационной инфраструктуры»

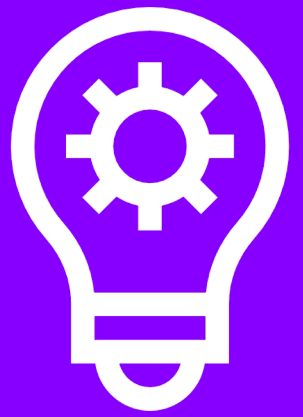
8 февраля 2021 года

Анна Надобных

- Соучредитель ИТ-компании «BizApps»
- Основатель стартапа «Galochka» (SaaS-решение)
- Владелец «r.Bot» (российское RPA-решение)
- Финансовый директор
- Эксперт в управленческом и проектном учете
- ChicagoBooth EMBA
- Член Генерального совета «Деловой России»

Раздел 1

Предпосылки и причины возникновения



Историческая справка

2000

Информационная безопасность не воспринималась всерьез (не существовала в потребительском секторе) до начала 00-х гг.

ИБ существовала в военном секторе

Толчком стало повсеместное развитие Интернета

2003

Начало развития направления в корпоративном секторе с 2003 года

2005

Профессиональная специализация ИБ начала формироваться с 2005 года

Причины возникновения ИБ

Любые системы/компьютеры («железо» и ПО) унаследовали много старых компонент.

Например, MS Windows до сих пор использует код из версий ПО Windows 95-98. В MS Windows 2003 40 млн строк кода.

«Старый» код используется повсеместно и он небезопасный.

Программное обеспечение можно сравнить с археологией, так как оно пишется и обновляется на протяжении многих лет и обновляется, как правило, только на «современном слое» — слое, где реализованы современные и востребованные функции, а на глубинном, «древнем слое» все остается практически в неизменном виде.

Как следствие, мы имеем две большие задачи:

Задача 1. Понять в каких компонентах такого ПО могут возникнуть проблемы с ИБ

Задача 2. Что может привести к возможности применения взломов (хакерству).

Справка: Хакерство возможно из-за наличия даже незначительных ошибок, «багов» в ПО и железе. Каждая система имеет тысячи таких багов/проблем, которые могут привести, в результате, к взлому

Раздел 2

Базовые идеи Информационной безопасности

Существует «три кита», на которых строится информационная безопасность

Конфиденциальность (privacy)

Целостность данных (integrity)

Защита данных от модификации или удаления неавторизованными сторонами. Обеспечение возможности восстановления информации, некорректно измененной или удаленной уполномоченными лицами.

Доступность данных (availability)

Системы, каналы доступа и механизмы аутентификации должны работать должным образом, чтобы информация, которую они предоставляют и защищают, была доступна пользователям, в соответствии с политикой безопасности компании

Виды обеспечения безопасности

Принцип «глубокой защиты» (defense in depth)

Самая популярная современная концепция на текущий момент. Опирается на построение «многослойной» защиты. Ее также называют тактикой «наслаивания». Включает три основных уровня защиты:

Физическая:
контроль того, что физически попадает в организацию (люди и оборудование)

Техническая :
архитектура: firewall и network connection
клиентская часть (point protection): антивирусы, логирование

Административная:
корпоративные правила, позволяющие избежать основных ошибок. Например, обязанность зашифровывать пароли и правила их шифрования

Принцип наименьших привилегий (principle of least privilege)

Опирается на идею строгих ограничений с целью предоставления минимального доступа для выполнения поставленной задачи

Раздел 3

Основные проблемы ИБ

Перечень основных проблем

Финансовые

Так как сложно оценить затраты на ИБ, - сложно аргументировать их необходимость. ИБ защищает от событий с низкой вероятностью, но возможным большим ущербом. Не получая достаточных аргументов по финансовой эффективности, при ухудшении экономической ситуации в стране руководители, зачастую, урезают бюджеты именно на ИБ.

Кадровые

- Мало квалифицированных специалистов по ИБ, разбирающихся во всех аспектах ИТ (программирование, техническая архитектура, networking), так как в университетах обучают специалистов по каждому аспекту отдельно.
- Проблема координации между ИТ командой и командой по ИБ (пример: необходимость постоянных обновлений для удаления системных багов)

Постоянно совершенствующиеся вирусы и инструменты хакеров

Ежедневно регистрируются десятки миллионов попыток взлома. Кибератаки происходят на международном уровне. Buffer overflow - один из распространенных багов, используемых хакерами для атак. Ежегодно возникают миллионы новых вирусов

Законодательные

Иногда законы устанавливают правила по ИБ, которые сложно или практически невозможно реализовать. Но при этом, они не решают проблемы ИБ.
Пример: требование по удалению персональных данных

Раздел 4

Тренды ИБ

Основные тренды в ИБ

Развитие новых систем защиты

Пример: Развитие Firewall. От простых межсетевых экранов до инструментов анализа контента (Paloalto fiwewalls). Добавляется возможность анализа контента и применяется AI
Каждая программа имеет свой паттерн: если можно определить этот паттерн, например, есть паттерн, который используют отдельные группы хакеров, то можно его заблокировать

Zero trust

Тщательный контроль прав для выполнения задач. Изначально все заблокировано, невозможно даже попробовать подключиться к любой системе, к которой не выдан доступ. Например, только бухгалтеры могут иметь доступ в учетную систему. Очень обсуждаемая идея, но сложно реализуемая. Нужно иметь сильную ИТ-команду, которая управляет всеми системами и процессами

Копирования и анализ всего поступающего контента

Возникло из-за последствий действий Сноудена. Крупные компании размещают в собственной сети сервер, через который пропускают весь входящий трафик и записывают его. Если появляется новая угроза (новый механизм атаки), всегда можно найти, как она была применена и какие части систем были атакованы

Раздел 5

Перспективы в ИБ

Что если

- продолжать сокращать бюджеты на ИТ и ИБ
- не прорабатывать проблему безопасности на законодательном уровне

В случае информационной войны большая часть данных будет заблокирована

Что делать

В идеале необходимо пересматривать всю ИБ, потому что сейчас даже небольшой баг может привести к атаке

Сложные системы, такие как Windows, часто содержат небольшие ошибки, но и это может привести к атаке

Как мыслить

Чаще задавайте себе вопрос: «Есть ли небезопасные компоненты в hardware и software моей компании?»

Раздел 6

Несколько слов в конце

Ключевая идея

Если не уделять информационной безопасности должного внимания, пострадать можете не только вы, но и третья сторона.

Когда из-за проблем с безопасностью какой-то компании затраты/ущерб несет третья сторона, это называется «негативный внешний эффект» (negative externality)

Пример: Загрязнение окружающей среды. Есть прямые затраты, которые несут компании, а есть затраты, которые перекладываются на все общество.

Прямо сейчас существует много ненужного избыточного риска, по аналогии с безопасностью труда на первых фабриках. В те времена рабочим было небезопасно выполнять свои обязанности.
Что касается информационной безопасности, сейчас опасность больше грозит потребителям товаров и услуг, чем компаниям, которые эти товары и услуги производят.

Спасибо за внимание

Контакты

Москва, Варшавское шоссе д. 1,
стр. 6, “W-plaza 2”, офис B-307

+ 7 495 150 31 07
+ 7 926 562 18 88

info@biz-apps.ru
biz-apps.ru