Teach Me Skills

Введение в кибербезопасность

Общая информация и знакомство

Teach
Me
Skills

Собираемся и отмечаемся

Teach
Me
Skills

Познакомимся?

Белугин Никита

Security Engeneer (Reverse/Analytic)
В крупнейшем SOC в РБ.

4 Года опыта работы в корпоративном секторе.
Sertified in cybersecurity
Sertified with Kaspersky/Avsoft products

Расскажите о себе?

1. **Как вас зовут?**
2. **Какие у вас знания в CS, курсы/самообучение/уч заведения?**
3. **Есть ли у вас опыт в ИТ/ИБ? Если есть, то в какой области?**
4. **Учитесь или работает в связанных с ИТ/ИБ областях?**
5. **Какой ЯП знаете или хотите узнать?**
6. **Расскажите ваше видение работы в ИБ. Что вы ожидаете от ИБ?**

Mini-quize по текущей теме:

1. **Что такое ИБ?**
2. **Какие направления в ИБ вы знаете?**
3. **Какие основные типы атак вы знаете?**
4. **Кто такие «Белые Хакеры»?**
5. **Какие ОС вы знаете?**
6. **Что такое троян, сниффер, vpn, пентест, фишинг, 0-day**
7. **Какие команды есть в КиберБезе?**

Teach Me Skills

План занятия

1. Разберемся какие основные существуют направления в ИБ.
2. Изучим историю первых вирусов, и веб-атак.
3. Познакомимся с CIA, AAA.
4. Изучим кто такие WhiteHat, BlackHat и Red/BlueTeam.
5. Изучим основые тенденции и пути развития направления.

Направления в ИБ

Информационная безопасность – комплекс мер по обеспечению КЦД данных и систем.

1) Уход вендоров
2) Создание SOC-ов
3) Предотвращение кибератак
4) КВОИ
5) Переход на отечественные компоненты

1) Сетевая безопасность
2) Безопасность приложений
3) Безопасность данных
4) Облачная безопасность
5) Обучение и развитие
6) Реагирование на инциденты
7) Безопасность конечных устройств
8) Кибербразведка
9) Управление рисками

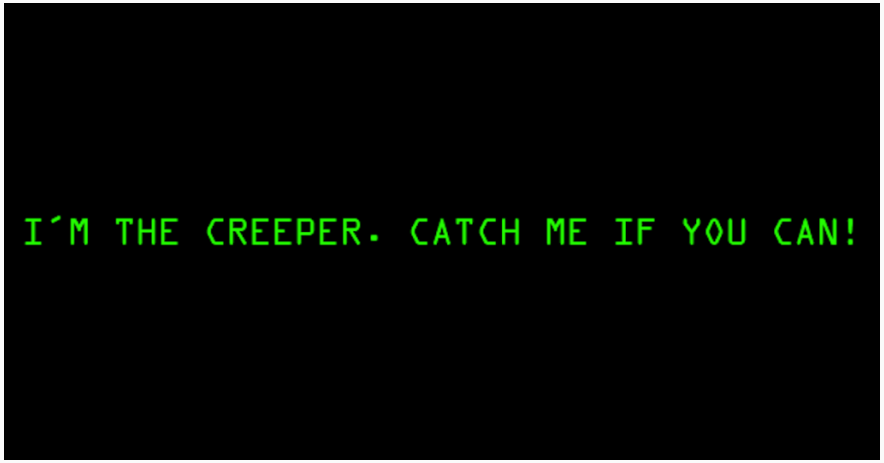
Компьютерные вирусы

Вредоносная программа, вредонос, **зловред** — любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого ПК или к информации, хранимой на ПК.

Компью́терный ви́рус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи

Джон Фон Нейман - заложил основы теории самовоспроизводящихся механизмов.

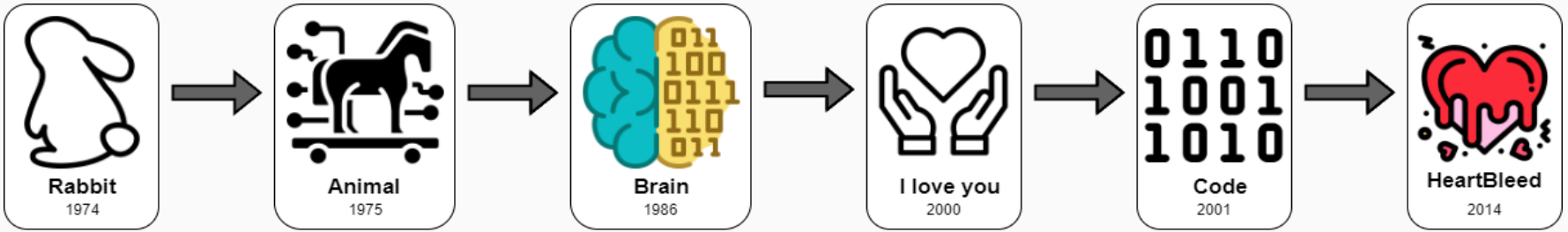
История первых вирусов



Creeper, создан в 1971 году сотрудником компании BBN Бобом Томасом. По факту, Creeper был создан как тестовая программа, чтобы проверить, возможно ли создать самовоспроизводящуюся программу.

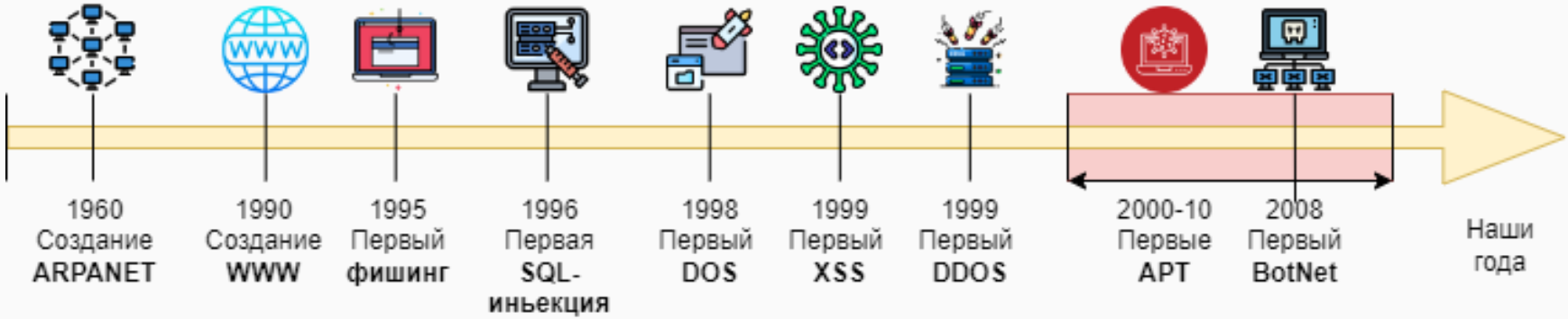
Заразив новый жесткий диск, Creeper пытался удалить себя с предыдущего компьютера. Creeper **не совершал никаких вредоносных действий**!

Следом был первый **Зловред «**Кролик», и первый троянец ANIMAL, первый вирус BOOT - сектора.



История первых веб-атак

Таймлайн событий ИнфоБеза в ретроперспективе

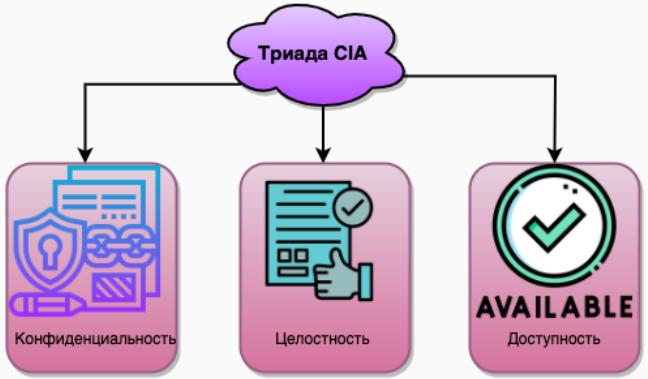


Триада CIA(КЦД)

1.Конфиденциальность: Гарантирует, что информация доступна только тем, кто имеет право ее видеть. Направлена на предотвращение несанкционированного доступа к конфиденциальным данным.

2.Целостность: Обеспечивает точность и неприкосновенность информации. Контроль целостности может осуществляться с помощью методов хеширования, цифровых подписей и других технологий, которые обнаруживают изменения в данных.

3.Доступность: Гарантирует, что системы и данные доступны для тех, кто имеет к ним законный доступ, в нужное время. Это включает в себя меры по предотвращению отказов в обслуживании, а также обеспечение резервирования и восстановления данных.

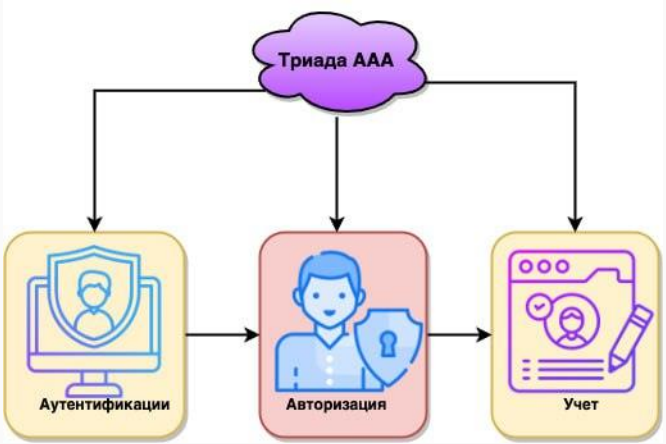


Триада AAA

1.Аутентификация: направлена на проверку личности пользователя или устройства, чтобы удостовериться, что оно является тем, за что себя выдает. Происходит с использованием учетных записей (логинов) и паролей.

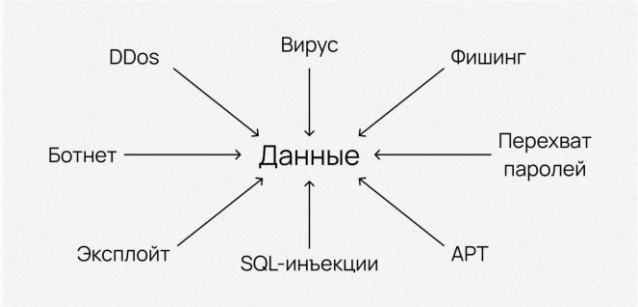
2.Авторизация: Этот принцип определяет, какие ресурсы и действия пользователь или устройство могут выполнять после успешной аутентификации.

3.Аудит: Мониторинг и регистрация событий безопасности, происходящих в системе. Сбор данных о действиях пользователей, изменениях в системе, попытках неудачной аутентификации и других событиях.



Угрозы

Угрозы информационной безопасности (ИБ) представляют собой действия, события или обстоятельства, которые могут привести к несанкционированному доступу, использованию, раскрытию, разрушению или изменению информации.



Основные виды угроз ИБ
1. Кибератаки
ВПО
Фишинг
DDoS-атаки
SQL-инъекции

2. Внутренние угрозы
Инсайдеры
Случайные инциденты

3. Физические угрозы
Кража оборудования
Природные катастрофы

Уязвимости

Уязвимости — это слабые места в программном обеспечении, аппаратном обеспечении, сетях или процессах, которые могут быть использованы злоумышленниками для компрометации системы.

Уязвимости могут возникать из-за ошибок в коде, неправильной конфигурации систем, слабых паролей и других причин.

OWASP(Open Web Application Security Project) – общедоступный проект по обеспечению веб-безопасности.

POC – proof of concept, доказательство концепта
CVE – common vulnerabilities and exposures, база общедоступных уязвимостей

White & black hat

White Hat (Белая шляпа)
White hat хакеры – это специалисты по кибербезопасности, которые используют свои навыки и знания для обеспечения безопасности систем. Они работают в рамках закона и этических норм, часто нанимаются организациями для проведения тестирования на проникновение и оценки уязвимостей.

Black Hat (Черная шляпа)
Black hat хакеры – это злоумышленники, которые используют свои навыки для незаконного доступа к системам с целью кражи данных, нанесения ущерба или получения финансовой выгоды. Они нарушают законы и этические нормы, их деятельность считается криминальной.

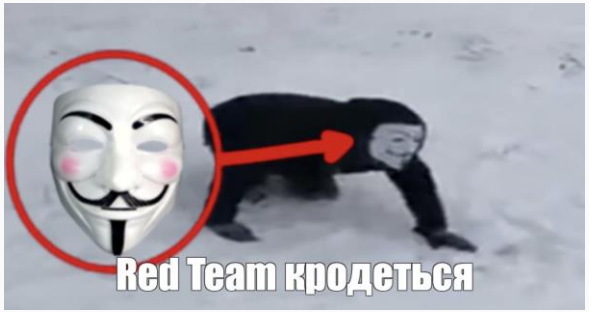
White hat

Gray Hat (Серая шляпа)
Кроме white hat и black hat хакеров, существуют также gray hat. Эти хакеры находятся между этими двумя крайностями. Они могут взламывать системы без разрешения, но не с целью нанесения вреда, а чтобы указать на уязвимости и предложить их исправление. Их деятельность все равно считается незаконной, но мотивы часто менее злонамеренные, чем у black hat.

Black hat

Red team

Red Team — это группа специалистов по кибербезопасности, которая проводит атакующие действия с целью тестирования защиты организации (пентеста).
Основная задача Red Team — выявить уязвимости и слабые места в системе безопасности компании, моделируя действия реальных злоумышленников.



ВАЖНО!
В отличие пентеста, Red Team действует более комплексно и часто в рамках долгосрочной кампании.

Казалось, при чем тут RED ALERT?

Концепция красных и синих команд появилась 60-ых. В аналитическом центре **RAND Corporation**, который проводил моделирование для вооруженных сил США во время холодной войны.
«**Красная команда**» использовались для представления СССР, а «**синяя команда**» и синий цвет использовались для представления США.

Blue Team

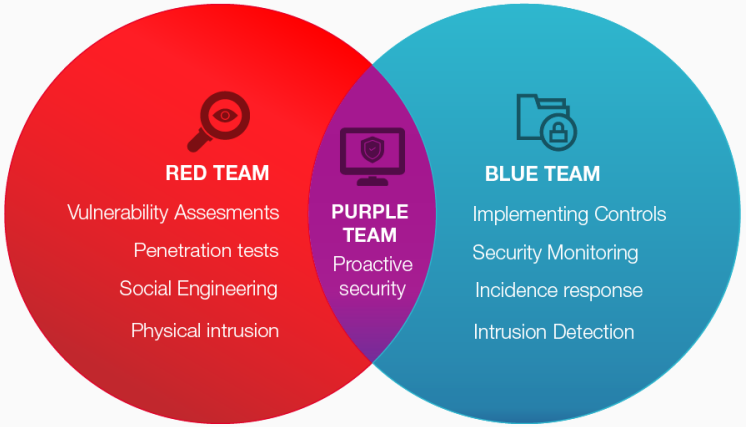
Blue Team (Синяя команда) — это группа специалистов по кибербезопасности, отвечающая за защиту информационных систем организации от кибератак и других угроз. Blue Team играет ключевую роль в защите информационных ресурсов, обеспечивая мониторинг, обнаружение и реагирование на инциденты безопасности.

Базово blue team-овцы владеют:

•знаниями и пониманиями основных векторов возможных атак, инфраструктуры компании с учетом бизнес-процессов;
•знают и применяют на деле международные и национальные стандарты ИБ (ISO 27001, GDPR, NIST);
•умеют анализировать огромные потоки данных и находить подозрительные закономерности;
•умеют администрировать СрЗИ и внедрять их;
•понимают принципы основных тактик и техник MITRE ATT&CK и OWASP TOP 10;
•Частично понимают логику злоумышленников, вектора.

Красный + Синий = ...

Purple Team (Фиолетовая команда) — это концепция в кибербезопасности, которая объединяет усилия Red Team и Blue для улучшения общей безопасности организации. Purple Team обеспечивает сотрудничество и обмен знаниями между этими двумя группами, создавая более скоординированный и эффективный подход к защите и атаке.



Основная их задача - обучение, обмен знаниями и опытом между командами защиты и нападения в режиме реального времени. Этот подход направлен на устранение разрыва между наступательными и оборонительными практиками кибербезопасности и повышение общей киберустойчивости ИТ-инфраструктуры организации.

Инфографика по инцидентам

Инцидент (**ИБ**) — это событие, которое угрожает конфиденциальности, целостности или доступности информационных систем и данных. Инциденты могут быть вызваны различными причинами, такими как кибератаки, человеческие ошибки, сбои оборудования или программного обеспечения, и природные катастрофы.

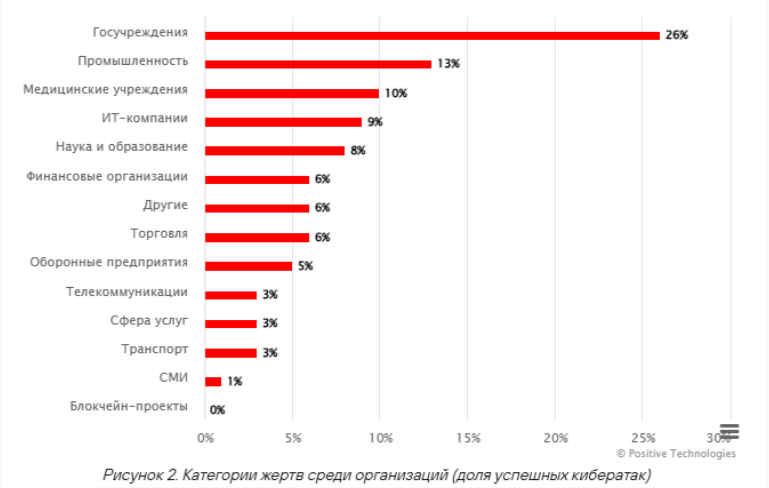


Рисунок 2. Категории жертв среди организаций (доля успешных кибератак)

Годовой отчет **Kaspersky** 2023

https://content.kaspersky-labs.com/se/media/ru/data-leaks-report-2023.pdf -

Годовой отчет **Positive Technologies** 2023

https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/

Поговорим о сливах...

Сливы данных, происходят, когда конфиденциальная информация попадает в публичный доступ без разрешения владельца. Это может быть результатом хакерских атак, внутренних нарушений безопасности или небрежности в обращении с данными.

Причины утечек данных
Кибератаки: Хакеры могут использовать различные методы для получения доступа к конфиденциальной информации.

Внутренние угрозы: Сотрудники могут случайно или умышленно «сливать» данные. Это может быть связано с небрежным обращением с информацией или с целью навредить компании.

Ошибки в конфигурации: Неправильные настройки могут открыть доступ к информации для неавторизованных пользователей.

Физическая кража: Устройства, содержащие данные, такие как ноутбуки, смартфоны или внешние жесткие диски, могут быть украдены.

Сливы данных

Последствия утечек данных:

Финансовые убытки: Компании несут значительные финансовые потери из-за штрафов, компенсаций клиентам и расходов на восстановление системы безопасности.

Ущерб репутации: Утечки данных подрывают доверие клиентов и партнеров.

Юридические последствия: Компании привлекаются к ответственности за несоблюдение законов и НПА по защите данных.

Потеря конфиденциальной информации: Утечка данных может привести к раскрытию коммерческих тайн, личной информации клиентов и сотрудников.

Примеры крупных утечек данных:

1)Equifax (2017): Утечка данных, затронувшая личную информацию более 147 миллионов человек, включая номера социального страхования, даты рождения и адреса.
2)Yahoo (2013-2014): Две крупные утечки, в результате которых были скомпрометированы данные более 3 миллиардов учетных записей.
3)Marriott (2018): Утечка данных, затронувшая около 500 миллионов гостей, включая информацию о номерах кредитных карт и паспортные данные.

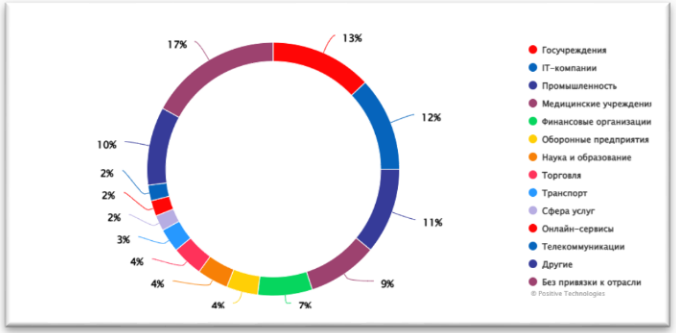
Меры по предотвращению утечек данных:

1) Шифрование
2) Обучение сотрудников
3) Системы обнаружения вторжений
4) DLP
5) Регулярные аудиты безопасности

Статистика о сливах

По статистике F.A.C.C.T.:
За первые шесть месяцев 2024 года в открытый доступ выложили **150 (уникальных) баз данных** российских компаний.

За 6 месяцев 2023-его всего:
119 скомпрометированных баз, а за весь год - **246** БД.



Распределение утечек по **направлениям**

А что у соседей?(май-июнь 2024):

1) Бангладешский поставщик ИТ-услуг **Tappware**. (95 тысяч адресов электронной почты и персональные данные сотркдников);
2) Новостной сайт **The Post Millennial**. (Данные сотни авторов и редакторов, десятки тысяч подписчиков)
3) Французский бренда **Zadig & Voltaire**. (Имена, электронные и физические адреса, номера телефонов и пол);
4) **Advance Auto Parts** стала жертвой утечки данных (79 миллионов уникальных адресов электронной почты, а также имена, номера телефонов, адреса и другие данны, сотрудников компании);

ДЗ

1) Установить **VirtualBox**
2) Загрузить образ *.iso **Kali Linux**
3) Загрузить образ *.iso **Windows10**

Teach
Me
Skills

Спасибо за внимание!