Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

«Организация и обеспечение аудита настроек средств защиты информации»

ОТЧЕТ ПО МОДУЛЮ №1

«Угрозы ИБ»

Выполнил:

Чу Ван Доан, студент группы N3347

(подпись)

Проверил:

Пенин Андрей Семенович

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

Содержание

Введение

Цель работы – Анализ инцидентов информационной безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

- Выбрать 5 случайных инцидентов (из списка 20 инцидентов информационной безопасности).
- Определить угрозы (связанные с каждым инцидентом), включая:
    - Вид угрозы.
    - Источник угрозы.
    - Способ реализации.
    - Цель угрозы.
- Предложить меры предотвращения (включая не менее 2 мер – техническую и организационную для каждой угрозы).

Задание

2. Атака с использованием фишинга

Сотрудник получил письмо, якобы от имени банка, с просьбой перейти по ссылке и ввести учетные данные. После выполнения действий злоумышленники получили доступ к внутренним системам компании.

7. DDoS-атака на корпоративный веб-сайт

Злоумышленники инициировали распределенную атаку (DDoS) на веб-ресурсы компании, что привело к нарушению их доступности для клиентов.

10. Взлом Wi-Fi-сети

Злоумышленники атаковали недостаточно защищенную корпоративную Wi-Fi-сеть, используя атаку злоумышленника "посередине" (MITM), и перехватили сетевой трафик, включая учетные данные для доступа к внутренним системам.

14. Разглашение информации в социальных сетях

Сотрудники непреднамеренно или намеренно разглашают корпоративную информацию или делятся конфиденциальными данными в соцсетях, что наносит ущерб компании.

20. Отсутствие регулярного резервного копирования

Компания не поддерживает регулярное создание резервных копий данных, что увеличивает риск их полной утраты в случае аварий или кибератак.

Ход работы

1. Атака с использованием фишинга

Сотрудник получил письмо, якобы от имени банка, с просьбой перейти по ссылке и ввести учетные данные. После выполнения действий злоумышленники получили доступ к внутренним системам компании.

1.1. Вид угрозы

Это фишинговая атака (Phishing Attack), а именно целевой фишинг (spear-phishing), когда электронное письмо персонализировано и нацелено на конкретного сотрудника компании, выдавая себя за доверенную организацию (банк).

1.2. Источник угрозы

Источник атаки может быть следующим:

- Поддельное электронное письмо, отправленное извне, использующее адрес, похожий на настоящий адрес банка (email spoofing).
- Фальшивый веб-сайт, созданный с целью имитации официального сайта банка для кражи учетных данных.
- Внешний злоумышленник может быть как независимым хакером, так и организованной киберпреступной группой с конкретной целью.

1.3. Способ реализации

- Отправка поддельного электронного письма – злоумышленник использует технику email spoofing или домен, схожий с официальным доменом банка, чтобы обмануть жертву и вызвать доверие.
- Вставка вредоносной ссылки – письмо содержит ссылку, ведущую на фальшивый веб-сайт, который визуально идентичен официальному сайту банка.
- Кража учетных данных – сотрудник вводит логин и пароль на поддельном сайте, после чего информация немедленно передается злоумышленнику.
- Доступ к внутренним системам – используя похищенные учетные данные, атакующий входит в критически важные системы компании.

- Эскалация привилегий (Privilege Escalation) – если украденный аккаунт обладает высокими правами доступа, злоумышленник может получить контроль над важными системами или установить вредоносное ПО для дальнейшего распространения атаки.

1.4. Цель

- Компрометация учетных данных – злоумышленник использует украденные логины и пароли для проникновения во внутреннюю систему компании.
- Кража критически важной информации – доступ к финансовым данным, информации о клиентах и другим конфиденциальным сведениям компании.
- Установка вредоносного ПО или ransomware – атакующий может зашифровать файлы компании и потребовать выкуп за их восстановление.
- Использование скомпрометированных учетных записей – проведение несанкционированных финансовых операций или организация внутренних атак (insider attack).

1.5. Меры предосторожности

1.5.1. Технические меры

- Настройка защиты электронной почты (Email Security)
- Внедрение DMARC, SPF, DKIM для предотвращения подделки писем.
- Использование фильтрации электронной почты для выявления писем с фишинговыми ссылками.
- Защита браузера и контроль доступа к веб-ресурсам
- Применение Web Filtering для блокировки доступа к фальшивым сайтам.
- Использование HTTPS Inspection для анализа и проверки содержимого веб-страниц.
- Двухфакторная аутентификация (Multi-Factor Authentication - MFA)
- Обязательное использование 2FA/MFA при входе во внутренние системы.
- Использование приложений OTP вместо SMS для снижения риска атак "человек посередине" (MITM).
- Мониторинг и обнаружение вторжений
- Внедрение SIEM (Security Information and Event Management) для отслеживания подозрительных попыток входа.

- Настройка оповещений при входе с неизвестного IP-адреса или устройства.

- Ограничение доступа и защита данных

- Применение принципа минимально необходимого доступа (Principle of Least Privilege - PoLP).
- Использование Data Loss Prevention (DLP) для предотвращения утечек критически важной информации.

- Шифрование и защита учетных данных

- Применение менеджеров паролей для безопасного хранения учетных записей.
- Шифрование конфиденциальных данных при передаче и хранении.

1.5.2. Организационные меры

- Обучение сотрудников кибербезопасности

- Проведение регулярных тренингов по распознаванию фишинговых писем.
- Имитация фишинговых атак для проверки реакции сотрудников.

- Процедуры аутентификации критически важных запросов

- Запрет выполнения финансовых операций или передачи конфиденциальных данных через электронную почту без подтверждения через официальный канал.
- Внедрение двойного подтверждения (dual approval) для критически важных транзакций.

- Политика реагирования на инциденты

- Разработка плана реагирования на фишинговые атаки.
- Внедрение процедуры быстрой отчетности о подозрительных письмах, чтобы сотрудники могли немедленно сообщать о выявленных угрозах.

- Периодические проверки безопасности

- Проведение тестов на проникновение (penetration testing) для оценки уязвимостей.
- Анализ логов доступа для выявления подозрительной активности.

2. DDoS-атака на корпоративный веб-сайт

Злоумышленники инициировали распределенную атаку (DDoS) на веб-ресурсы компании, что привело к нарушению их доступности для клиентов.

2.1. Вид угрозы

Это атака распределенного отказа в обслуживании (Distributed Denial-of-Service – DDoS Attack), при которой злоумышленник использует большую сеть скомпрометированных устройств (ботнет), чтобы отправить огромный объем поддельного трафика на веб-сайт компании, перегружая его и вызывая сбои в работе сервиса.

2.2. Источник угрозы

- Botnet – сеть компьютеров, зараженных вредоносным ПО и находящихся под контролем хакеров. Она может включать от тысяч до миллионов устройств по всему миру.
- Устройства IoT – слабо защищенные устройства Интернета вещей (IoT), которые злоумышленники используют для участия в атаке.
- Арендованные DDoS-атаки – некоторые хакерские группы предлагают DDoS-услуги на даркнете, позволяя злоумышленникам арендовать ботнет для проведения атак.
- Внутренние атаки (Insider Attack) – в некоторых случаях атака DDoS может исходить изнутри организации, например, по вине недовольного сотрудника.

2.3. Способ реализации

Атака может быть осуществлена различными методами:

Атаки, перегружающие полосу пропускания (Volume-based Attacks)

- UDP Flood – отправка большого количества поддельных UDP-пакетов на целевой сервер, чтобы занять доступную полосу пропускания.
- ICMP Flood (Ping Flood) – массовая отправка ICMP-запросов (ping) на сервер, что приводит к перегрузке системы.
- DNS Amplification – использование открытых DNS-серверов для отправки увеличенных ответов на жертву, перегружая сеть.

Атаки, истощающие ресурсы сервера (Protocol-based Attacks)

- SYN Flood – отправка множества TCP-запросов без завершения трехстороннего рукопожатия (3-way handshake), что потребляет ресурсы сервера и блокирует новые соединения.
- HTTP Flood – генерация большого количества поддельных HTTP-запросов к веб-сайту, истощая вычислительные ресурсы сервера.

Атаки на уровне приложений (Application Layer Attacks)

- Slowloris – удерживание HTTP-соединений открытыми как можно дольше, тем самым исчерпывая доступные ресурсы сервера.
- Атака на API – массовая отправка запросов к API веб-приложения с целью перегрузки системы.

2.4. Цель

- Нарушение работы сервиса – атака может привести к недоступности веб-сайта компании, что негативно сказывается на клиентах и доходах.
- Вымогательство (Ransom DDoS - RDoS) – злоумышленники требуют выкуп за прекращение атаки.
- Подрыв репутации – снижение доверия клиентов к компании из-за постоянных сбоев в работе.
- Отвлекающая атака – DDoS может использоваться как прикрытие для других атак, таких как взлом системы и кража данных.

2.5. Меры предосторожности

2.5.1. Технические меры

Использование специализированных систем защиты от DDoS

- Внедрение Web Application Firewall (WAF) для выявления и блокировки вредоносного трафика.
- Использование CDN (Content Delivery Network), таких как Cloudflare, Akamai, для распределения трафика и снижения нагрузки на сервер.
- Подключение DDoS Protection Services от провайдеров, таких как AWS Shield, Cloudflare, Imperva.

Фильтрация и ограничение сетевого трафика

- Настройка Rate Limiting для ограничения количества запросов с одного IP-адреса.
- Применение IP Reputation Filtering для блокировки IP-адресов, принадлежащих ботнетам.
- Использование Reverse Proxy для перераспределения нагрузки и защиты основного сервера.

Защита сетевой инфраструктуры

- Внедрение Network Intrusion Detection System (NIDS) для обнаружения подозрительных атак.
- Использование Anycast Routing для распределения вредоносного трафика между несколькими серверами.
- Применение Blackhole Routing для автоматического удаления вредоносного трафика до его попадания на сервер.

Защита уровня приложений

- Включение TLS/SSL для шифрования передаваемого трафика.
- Интеграция CAPTCHA в формы авторизации для предотвращения автоматизированных атак ботами.
- Использование Dynamic Rate Limiting для динамического регулирования лимитов запросов в зависимости от поведения пользователя.

2.5.2. Организационные меры

Разработка плана реагирования на инциденты

- Создание Incident Response Plan для оперативного устранения последствий атаки.
- Взаимодействие с провайдерами интернет-услуг (ISP) для снижения нагрузки на инфраструктуру.

Мониторинг и регулярные проверки

- Внедрение SIEM (Security Information and Event Management) для отслеживания сетевого трафика в реальном времени.
- Анализ логов доступа для выявления признаков атаки на ранних стадиях.

Обучение сотрудников

- Подготовка IT-отдела к выявлению и реагированию на DDoS-атаки.
- Повышение осведомленности о социальной инженерии, чтобы избежать установки вредоносного ПО.

Регулярные проверки безопасности

- Проведение penetration testing (пентестов) для оценки устойчивости системы к атакам.
- Проверка и обновление конфигурации межсетевых экранов (firewall) для повышения уровня защиты.

3. Взлом Wi-Fi-сети

Злоумышленники атаковали недостаточно защищенную корпоративную Wi-Fi-сеть, используя атаку злоумышленника "посередине" (MITM), и перехватили сетевой трафик, включая учетные данные для доступа к внутренним системам.

3.1. Вид угрозы

Это атака на Wi-Fi-сеть с использованием метода "человек посередине" (Man-in-the-Middle - MITM), при которой злоумышленник эксплуатирует уязвимости в корпоративной Wi-Fi-сети для перехвата и анализа сетевого трафика. Это может привести к утечке конфиденциальной информации, включая учетные данные для доступа к внутренним системам.

3.2. Источник угрозы

- Слабая защита Wi-Fi – использование устаревших и уязвимых протоколов шифрования, таких как WEP или WPA, которые легко взламываются.
- Некорректная или небезопасная конфигурация Wi-Fi – отсутствие защиты, например, фильтрации по MAC-адресам и сильной аутентификации.
- Компрометация устройств Wi-Fi – уязвимые роутеры и точки доступа (AP) могут быть взломаны, если их прошивка не обновляется.
- Атака "злой двойник" (Evil Twin Attack) – создание злоумышленником поддельной Wi-Fi-сети с таким же именем (SSID), чтобы жертвы подключились к ней.

- Внутренние угрозы – компрометированный сотрудник или зараженное устройство в сети может эксплуатировать уязвимости Wi-Fi для атак на корпоративные системы.

3.3. Способ реализации

Сбор информации о сети Wi-Fi

- Использование инструментов Aircrack-ng, Kismet для сканирования сети и сбора информации о целевом Wi-Fi.
- Определение SSID, типа шифрования, используемого канала и подключенных устройств.

Атака на Wi-Fi-сеть

- Brute-force атака на WPA/WPA2 – перехват handshake (процесс аутентификации между клиентом и точкой доступа) и перебор миллионов паролей.
- Взлом WEP/WPA – если сеть использует слабое шифрование, его можно взломать с помощью инструментов Reaver, Hashcat.

Атака Man-in-the-Middle (MITM)

- Evil Twin Attack – создание поддельной точки доступа с идентичным SSID, чтобы пользователи подключались к ней.
- ARP Spoofing – подмена MAC-адреса, чтобы перехватить трафик между роутером и устройством сотрудника.
- DNS Spoofing – перенаправление пользователей на фальшивые веб-сайты для кражи учетных данных.

Компрометация внутренних систем

- Мониторинг сетевого трафика и перехват паролей пользователей.
- Доступ к критически важным системам с украденными учетными записями.
- Установка вредоносного ПО или бэкдора для удаленного контроля над системой.

3.4. Цель

- Кража учетных данных – злоумышленник использует похищенные логины и пароли для доступа к внутренним системам компании.
- Перехват и блокировка данных – мониторинг и подслушивание важных корпоративных коммуникаций внутри сети.
- Изменение сетевого трафика – перенаправление пользователей на поддельные сайты для фишинга или установки вредоносного ПО.
- Эскалация привилегий – если атакующий получает доступ к учетной записи с высоким уровнем привилегий, он может захватить контроль над всей системой.

3.5. Меры предосторожности

3.5.1. Технические меры

Настройка безопасного Wi-Fi

- Использование WPA3 вместо WPA2/WEP для усиленной защиты.
- Отключение SSID broadcasting, чтобы снизить вероятность обнаружения сети злоумышленниками.
- Включение MAC Address Filtering для ограничения подключения только доверенных устройств.
- Настройка брандмауэра (Firewall) на точке доступа, чтобы блокировать несанкционированные соединения.

Шифрование и защита сетевых данных

- Использование VPN (Virtual Private Network) для шифрования всего сетевого трафика.
- Включение HTTPS Everywhere, чтобы все веб-транзакции проходили через защищенные соединения.
- Активация DNSSEC, чтобы защитить систему от атак DNS Spoofing.

Мониторинг и обнаружение вторжений

- Внедрение Intrusion Detection System (IDS) для выявления подозрительного трафика.

- Настройка WIDS (Wireless Intrusion Detection System) для обнаружения поддельных точек доступа.

Предотвращение атак Man-in-the-Middle (MITM)

- Включение Client Isolation в настройках Wi-Fi, чтобы запретить прямое взаимодействие между устройствами внутри сети.
- Использование ARP Spoofing Protection на маршрутизаторе для защиты от подмены ARP-адресов.
- Внедрение HSTS (HTTP Strict Transport Security) для предотвращения атак MITM через HTTP.

Защита конечных устройств

- Обязательное использование антивирусного ПО и endpoint protection на ноутбуках и мобильных устройствах сотрудников.
- Включение брандмауэра (firewall) на персональных компьютерах и мобильных устройствах для снижения риска атак.

3.5.2. Организационные меры

Обучение сотрудников по безопасности Wi-Fi

- Избегать подключения к публичным Wi-Fi-сетям или неизвестным точкам доступа.
- Всегда использовать VPN при работе удаленно.
- Проверять HTTPS в адресной строке браузера, чтобы избежать атак DNS Spoofing.

Разработка политики безопасности Wi-Fi

- Создание отдельных Wi-Fi-сетей для гостей и сотрудников, отделенных от внутренней корпоративной сети.
- Регулярная смена паролей Wi-Fi и использование сложных паролей.
- Требование обязательной регистрации устройств, подключаемых к корпоративному Wi-Fi.

Регулярные проверки и обновления безопасности

- Проведение Wi-Fi Pentesting для выявления уязвимостей в сети.

- Регулярное обновление прошивки роутеров и сетевого оборудования для устранения известных уязвимостей.
- Мониторинг логов доступа, чтобы обнаружить подозрительные подключения.

4. Разглашение информации в социальных сетях

Сотрудники непреднамеренно или намеренно разглашают корпоративную информацию или делятся конфиденциальными данными в соцсетях, что наносит ущерб компании.

4.1. Вид угрозы

Этот инцидент относится к категории утечки информации (Information Leakage), которая может произойти по следующим причинам:

- Неумышленное раскрытие (Unintentional Disclosure) – сотрудники случайно делятся корпоративной информацией, не осознавая ее конфиденциальность.
- Преднамеренное раскрытие (Intentional Disclosure) – сотрудник или инсайдер намеренно публикует или передает чувствительные данные.
- Техническая эксплуатация (Technical Exploitation) – хакеры используют социальные сети для сбора информации или обмана сотрудников с целью раскрытия данных.

4.2. Источник угрозы

- Сотрудники компании – публикация постов, изображений или документов, содержащих конфиденциальную информацию, без осознания серьезности ситуации.
- Официальные аккаунты компании в соцсетях – случайная публикация внутренних документов или неосторожные ответы клиентам, приводящие к утечке данных.
- Атаки социальной инженерии (Social Engineering) – хакеры используют методы обмана, чтобы заставить сотрудников раскрыть информацию.
- Связь личного и корпоративного аккаунта – сотрудники используют личные аккаунты, связанные с корпоративными данными, что может привести к утечке.
- Взлом аккаунта в соцсетях – компрометация учетной записи сотрудника или компании, что позволяет злоумышленникам распространять конфиденциальную информацию.

4.3. Способ реализации

Случайная утечка информации сотрудниками

- Публикация скриншотов электронной почты, документов или внутренних совещаний в соцсетях.
- Размещение фото рабочего места, на которых видны белые доски, печатные документы или пароли.
- Публичные комментарии в форумах и чатах без осознания рисков утечки данных.

Преднамеренная утечка информации сотрудниками

- Недовольные сотрудники намеренно сливают внутренние документы в сеть, чтобы подорвать репутацию компании.
- Передача конфиденциальных данных третьим лицам (конкурентам, СМИ).

Использование данных из соцсетей злоумышленниками

- OSINT (Open-Source Intelligence) – сбор открытой информации из соцсетей для составления детального профиля компании.
- Spear Phishing – использование собранных данных для таргетированных фишинговых атак на сотрудников.
- Мошенничество с поддельным наймом (Fake Recruitment Scam) – злоумышленники притворяются рекрутерами или партнерами, чтобы выманить корпоративную информацию.

4.4. Цель

- Сбор конфиденциальной информации о компании, сотрудниках и бизнес-стратегиях.
- Подрыв репутации за счет утечки негативных внутренних данных.
- Подготовка к дальнейшим атакам, таким как фишинг или социальная инженерия.
- Использование внутренних данных для кражи интеллектуальной собственности.

4.5. Меры предосторожности

4.5.1. Технические меры

Контроль и мониторинг публикаций

- Внедрение DLP (Data Loss Prevention) для обнаружения и блокировки утечки конфиденциальной информации.
- Настройка SIEM (Security Information and Event Management) для мониторинга аномальной активности в соцсетях.

Защита корпоративных аккаунтов в соцсетях

- Обязательное включение двухфакторной аутентификации (2FA) на всех корпоративных аккаунтах.
- Ограничение количества сотрудников, имеющих доступ к соцсетям компании.
- Использование инструментов мониторинга социальных сетей для выявления и удаления утекшей информации.

Шифрование и защита внутренних документов

- Ограничение прав доступа к важным документам.
- Использование водяных знаков (watermarking) для отслеживания источника утечки данных.

Блокировка доступа с ненадежных устройств

- Разрешение входа в корпоративные аккаунты только с управляемых устройств.
- Внедрение Mobile Device Management (MDM) для контроля данных на мобильных устройствах сотрудников.

4.5.2. Организационные меры

Разработка политики информационной безопасности в соцсетях

- Создание политики конфиденциальности в соцсетях, которая четко определяет, что сотрудники могут и не могут публиковать.

- Запрет на публикацию внутренних данных, рабочих документов или обсуждение конфиденциальных вопросов в соцсетях.
- Установление санкций за утечку информации.

Обучение сотрудников защите информации

- Проведение курсов кибербезопасности по защите персональных и корпоративных данных в соцсетях.
- Обучение сотрудников распознавать фишинг и атаки социальной инженерии.

Строгий контроль корпоративных аккаунтов в соцсетях

- Назначение специальной команды для управления официальными аккаунтами компании.
- Внедрение процедуры утверждения перед публикацией корпоративного контента.

Регулярные проверки безопасности

- Мониторинг соцсетей для выявления потенциальных утечек информации.
- Анализ журналов входа в корпоративные аккаунты для выявления подозрительной активности.
- Проведение тестирования социальной инженерии (pentest social engineering) для оценки осведомленности сотрудников в области безопасности.

5. Отсутствие регулярного резервного копирования

Компания не поддерживает регулярное создание резервных копий данных, что увеличивает риск их полной утраты в случае аварий или кибератак.

5.1. Вид угрозы

Этот инцидент относится к категории риска потери данных (Data Loss Risk), связанного с отсутствием регулярных механизмов резервного копирования. Если компания не имеет четкой политики резервного копирования или выполняет его неправильно, риск потери данных возрастает в следующих случаях:

- Сбой системы или отказ оборудования (Hardware Failure) – жесткие диски, серверы или хранилища могут выйти из строя.

- Кибератаки (Cyberattacks) – атаки, такие как Ransomware, могут зашифровать или уничтожить критически важные данные.
- Человеческий фактор (Human Error) – случайное удаление данных, ошибки конфигурации или перезапись файлов.
- Природные катастрофы (Natural Disasters) – наводнения, пожары, землетрясения или другие катастрофические события могут привести к уничтожению данных.

5.2. Источник угрозы

- Отсутствие четкой политики резервного копирования – компания не определяет частоту и методы создания резервных копий.
- Неполные или устаревшие резервные копии – использование ручного или нерегулярного резервного копирования, что приводит к недостаточной защите данных.
- Хранение резервных копий на том же носителе – сохранение бэкапов на тех же серверах или устройствах, что повышает риск потери как оригинальных данных, так и их резервных копий.
- Отсутствие тестирования восстановления данных – отсутствие регулярных проверок, гарантирует ли резервное копирование возможность восстановления информации в

5.3. Способ реализации

Атака ransomware

- Хакеры шифруют данные во всей системе и требуют выкуп.
- Без резервных копий компания может потерять все данные или быть вынуждена заплатить выкуп.

Отказ оборудования

- Поломка жестких дисков, SSD или RAID-массивов без резервных копий приводит к безвозвратной потере данных.
- Неожиданный сбой оборудования может остановить бизнес-процессы.

Человеческие ошибки

- Сотрудник может случайно удалить важные файлы или форматировать хранилище.
- Без резервного копирования данные не подлежат восстановлению.

Инсайдерские атаки

- Недовольный сотрудник может намеренно удалить или повредить критически важные данные.
- Без резервных копий восстановление утраченной информации будет невозможным.

Природные катастрофы

- Пожары, наводнения, землетрясения могут уничтожить серверы и хранилища данных.
- Без удаленных резервных копий (offsite backup) вся информация может быть безвозвратно утеряна.

5.4. Цель

- Прерывание работы бизнеса – потеря критически важных данных может остановить все бизнес-процессы.
- Вымогательство (Ransomware) – злоумышленники требуют выкуп за восстановление зашифрованных или удаленных данных.
- Кража и уничтожение данных – хакеры могут скопировать информацию перед удалением, а затем использовать ее для шантажирования или продажи конкурентам.
- Подрыв репутации компании – утечка или потеря данных подрывает доверие клиентов и партнеров, что может привести к серьезным финансовым и юридическим последствиям.

5.5. Меры предосторожности

5.5.1. Технические меры

Внедрение стратегии 3-2-1 Backup Strategy

- 3 копии данных – оригинал и два резервных бэкапа.
- 2 типа носителей – хранение на разных устройствах (локальный сервер, облачное хранилище).
- 1 копия вне основной площадки (offsite backup) – хранение резервной копии в удаленном дата-центре.
- Определение частоты резервного копирования (ежедневное, еженедельное) в зависимости от критичности данных.

Использование автоматизированных систем резервного копирования

- Внедрение Backup as a Service (BaaS) от надежных поставщиков, таких как AWS Backup, Azure Backup, Google Cloud Backup.
- Использование специализированного ПО для автоматического бэкапа (Veeam, Acronis, Commvault).

Безопасное хранение резервных копий

- Исключение хранения резервных копий на том же сервере, что и основные данные.
- Использование air-gapped backup – изолированных копий, недоступных из сети, чтобы предотвратить заражение ransomware.
- Шифрование резервных данных с помощью AES-256 для защиты от утечек.

Периодическое тестирование восстановления данных

- Регулярное проведение тестов восстановления (disaster recovery testing), не реже одного раза в квартал.
- Гарантия быстрого восстановления данных для минимизации простоев бизнеса.

Мониторинг безопасности резервных копий

- Настройка систем мониторинга, которые отслеживают подозрительные попытки доступа к резервным копиям.
- Внедрение многофакторной аутентификации (MFA) для защиты учетных записей, имеющих доступ к системам резервного копирования.

5.5.2. Организационные меры

Разработка политики управления резервным копированием

- Определение типов данных, подлежащих резервному копированию, сроков хранения и методов копирования.
- Установка Recovery Point Objective (RPO) – максимальной допустимой потери данных.
- Определение Recovery Time Objective (RTO) – допустимого времени восстановления данных.

Обучение сотрудников защите данных

- Инструктаж по личному резервному копированию данных в рабочих процессах.
- Обучение методам реагирования на атаки ransomware и восстановлению данных из резервных копий.

Ограничение доступа к резервным копиям

- Предоставление доступа к бэкапам только ответственным сотрудникам.
- Внедрение Role-Based Access Control (RBAC) для минимизации риска несанкционированного доступа.

Разработка плана восстановления данных (Disaster Recovery Plan)

- Определение четких процедур восстановления при масштабной потере данных.
- Выделение резервных дата-центров, обеспечивающих бесперебойную работу бизнеса при авариях.

Регулярные проверки безопасности

- Проведение penetration testing для оценки уязвимостей резервных данных.
- Мониторинг логов и систем оповещения, чтобы выявлять подозрительные активности.

Заключение

В современных условиях информационной безопасности компании сталкиваются с множеством угроз, каждая из которых может привести к серьезным последствиям – от финансовых потерь до утраты конфиденциальных данных и подрыва репутации. Разбор рассмотренных инцидентов показывает, что недостаточная защищенность цифровой инфраструктуры, отсутствие четкой политики безопасности и недостаточная осведомленность сотрудников могут стать критическими уязвимостями.

1. Фишинговые атаки представляют собой один из наиболее распространенных методов кибератак, направленных на компрометацию учетных данных и получение несанкционированного доступа к корпоративным системам. Эффективное противодействие требует внедрения многофакторной аутентификации (MFA), мониторинга подозрительной активности и регулярного обучения сотрудников.
2. DDoS-атаки направлены на дестабилизацию корпоративных веб-ресурсов, что может привести к финансовым и репутационным потерям. Основными методами защиты являются использование специализированных сервисов защиты от DDoS, балансировка нагрузки и фильтрация трафика.
3. Взлом Wi-Fi-сети через атаку "человек посередине" (MITM) позволяет злоумышленникам перехватывать сетевой трафик, включая учетные данные пользователей. Предотвращение таких атак требует использования современных стандартов шифрования (WPA3), регулярного обновления прошивок маршрутизаторов, а также применения VPN и контроля доступа к Wi-Fi.
4. Разглашение информации в социальных сетях сотрудниками, даже если оно происходит ненамеренно, может привести к утечке конфиденциальных данных и использованию их злоумышленниками для целенаправленных атак. Политики информационной безопасности, обучение сотрудников и мониторинг публичных упоминаний компании помогают минимизировать этот риск.
5. Отсутствие регулярного резервного копирования делает компанию уязвимой к атакам программ-вымогателей (ransomware), сбоям в работе оборудования и человеческим ошибкам. Для обеспечения сохранности данных необходимо реализовать стратегию 3-2-1, использовать автоматизированные системы резервного копирования и регулярно проверять возможность восстановления данных.

Общие рекомендации по защите корпоративной информации:

- Многоуровневая защита (Defense-in-Depth): Использование нескольких уровней защиты (фильтрация трафика, аутентификация, шифрование, мониторинг и резервное копирование) для минимизации риска успешных атак.
- Обучение сотрудников: Повышение осведомленности персонала о методах кибератак и правилах безопасного обращения с данными.
- Разработка и соблюдение политик безопасности: Четко определенные правила работы с корпоративными данными, доступом к системам и взаимодействия в сети.
- Мониторинг и аудит безопасности: Внедрение SIEM-систем для анализа активности в сети, обнаружения аномального поведения и быстрого реагирования на угрозы.
- Регулярное тестирование защиты: Проведение пентестов и оценка уязвимостей для предотвращения возможных атак.

Список использованных источников

1. https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/phishing-attack-prevention.html
2. https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110
3. https://en.wikipedia.org/wiki/Denial-of-service_attack
4. https://www.microminderc s.com/blog/common-ddos-mitigation-strategies-a-comprehensive-guide
5. https://websitechuyennghiep.vn/cyber-attack-la-gi.html
6. https://antoanthongtin.gov.vn/gp-atm/cac-phuong-phap-tan-cong-ngan-hang-102499
7. https://www.microsoft.com/vi-vn/security/business/security-101/what-is-a-ddos-attack
8. https://cystack.net/vi/blog/tan-cong-mang-cyber-attack