УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией, составить и ответить на вопросы, законспектировать .

2. Предоставит отчет и презентацию в течении трех дней.

3. Отправить преподавателю на почту **v.vika2014@mail.ru** и указать свою Ф.И.О, группу, и название дисциплины тел 072-17-44-9-22

Тема: Виды информационных атак.

Основные виды атак на инфраструктуру и концепция защиты от них

На сегодняшний день большое количество кибератак является успешным по нескольким причинам: они не зависят от местоположения киберпреступника и удаленности от него потенциальной жертвы, а также временных рамок и часовых поясов. Взломанная ИТ-среда может повлечь за собой критические для бизнеса последствия: нанести репутационный ущерб и снизить уровень доверия со стороны клиентов, ведь их данные тоже могут попасть в чужие руки. Взлом инфраструктуры сопряжен и с финансовыми рисками: вследствие оттока заказчиков и потери уникальных инновационных разработок организации, ее конкурентоспособность может значительно упасть на рынке. Ситуация усложняется тем, что методы и тактики злоумышленников постоянно эволюционируют. Хакеры непрерывно адаптируют свои атаки к новым реалиям и технологиям. Современные кибератаки максимально автоматизированы, что позволяет злоумышленникам ускорять их проведение и использовать искусственный интеллект для повышения успеха их реализации. Используемые сегодня средства защиты эффективно выполняют свою задачу по обеспечению безопасности – они блокируют типовые атаки, однако они пока не совершенны в отношении точечных, мануальных угроз.

Основные типы и виды кибератак на инфраструктуру

Как правило, не имеет значение, какую инфраструктуру вы используете – локальную или облачную. Если данные, которые вы передаете, имеют ценность, кто-то захочет их получить. Действия злоумышленников можно разделить на два основных вида – распределенные и целевые атаки.

- **Распределенные кибератаки** представляют собой использование бот-сети и направлены одновременно на большое количество пользователей и ресурсов компаний. Как правило, в таких атаках используются утекшие базы данных организаций и пользователей.

- **Целевыми атаками (APT)** называют заранее спланированное «нападение» на конкретную компанию или инфраструктуру. При этих инцидентах злоумышленник не только получает доступ к внутренним ресурсам, но и остается в сети компании, пока его не обнаружат, – это могут быть дни, месяцы и даже годы. Целевые атаки реализуются хакерами с высокими техническими компетенциями. Они используют автоматизированные инструменты, самостоятельно определяют векторы атаки, эксплуатируют 0-day уязвимости и некоторые особенности системы, опираясь на свой опыт.

Кибератаки представляют опасность как для обычных пользователей, так и для бизнеса. В обоих случаях последствия могут быть не просто неприятными, но и критическими. Согласно статистике за 2020 год, представленной компанией Acronis, DDoS-атаки, фишинг и атаки на видеоконференции возглавили список киберугроз. Однако и другие типы атак приносят массу проблем как бизнесу, так и обычным пользователям. Злоумышленники шантажируют пользователей мессенджеров с помощью ботов, влезают в сеть через QR-коды и используют уязвимости в настройках или шифровании легальной сети, а также прибегают к классике жанра – атакам «грубой силы». Для того, чтобы лучше понимать действия злоумышленников, необходимо знать, какие существуют типы атак на инфраструктуру и их ключевые особенности.

1. **DDoS-атаки**. Распределенные атаки типа «отказ в обслуживании» реализуются за счет использования нескольких скомпрометированных компьютерных систем в качестве источников атакующего трафика. Эти атаки забивают системы большим количеством запросов, в результате чего пропускная способность снижается, и системы становятся перегруженными и недоступными. По сути, DDoS-атака похожа на неожиданную пробку, забивающую шоссе.
2. **Фишинг.** В основе фишинговых атак лежит использование электронных писем, которые могут быть замаскированы под легитимные сообщения от различных компаний. В таком фейковом сообщении злоумышленники могут предлагать перейти по ссылке, скачать зараженный файл или просить передать конфиденциальные данные пользователя – логины, пароли и номера счетов банковских карт.
3. **Brute-force.** Атаки «грубой силой» являются довольно простым методом проникновения в инфраструктуру и представляют собой «угадывание» учетных записей пользователя. Некоторые злоумышленники используют приложения и скрипты в качестве инструментов перебора, которые пробуют множество комбинаций паролей, чтобы обойти процессы аутентификации. Если пароль слабый, то злоумышленникам понадобится всего пару секунд, поэтому бизнес должен применять строгую политику паролей.
4. **Боты.** Это программный робот, который имитирует или заменяет поведение человека и выполняет простые задачи со скоростью, которая превышает пользовательскую активность. Некоторые боты бывают

полезными, и их действия направлены на поддержку пользователей, однако существуют и вредоносные. К примеру, они используются для автоматического сканирования веб-сайтов и поиска уязвимостей, а также выполнения простых кибератак.

5. **Атака через посредника (MITM).** При данном типе атаки киберпреступник становится «третьим лишним» и пропускает весь веб-трафик через себя. В этот момент потенциальная жертва ни о чем не подозревает, что приводит к тому, что все учетные данные для входа в системы оказываются у злоумышленника. После полученная информация может быть использована для кражи корпоративных данных или несанкционированных переводов средств.

Как обезопасить бизнес

Грамотный выбор инструментов обеспечения безопасности ИТ-ландшафта – залог сохранения конфиденциальности и сохранности корпоративных данных. Меры по обеспечению ИБ можно разделить на три ключевых вида: технические средства, организационные меры и профилактические проверки уровня защищенности.

Технические средства

1. **WAF-комплекс.** Это межсетевой экран для веб-приложений, основными функциями которого являются выявление и блокировка атак. С помощью WAF-комплекса можно не только выявлять вредоносный трафик, но и также определять, какие атаки были направлены на бизнес-критичные системы. Внедрение этого инструмента позволяет бизнесу защититься от атак на бизнес-логику приложений.

2. **Межсетевые экраны (FW).** Межсетевые экраны являются цифровым защитным барьером вокруг ИТ-инфраструктуры, который защищает сеть и предотвращает несанкционированный доступ. Межсетевые экраны обеспечивают безопасность сети путем фильтрации входящего и исходящего сетевого трафика на основе набора правил. В целом, задача межсетевых экранов состоит в том, чтобы уменьшить или исключить возникновение нежелательных сетевых подключений, позволяя при этом свободно протекать всем законным коммуникациям.

3. **Антивирус.** Антивирус – это программа, которая обнаруживает заражение и выполняет действия по его устранению: лечит или удаляет зараженные файлы. Антивирусное ПО работает и как профилактическое средство: оно не только борется, но и предотвращает заражение компьютера в будущем. Антивирусное программное обеспечение позволяет бизнесу защититься от шпионского ПО, вредоносных программ, фишинговых атак, спам-атак и других киберугроз.

4. **DLP** – это набор инструментов и процессов, которые применяюся для предотвращения потери и нелегитимного использования конфиденциальных данных. DLP-система отслеживает весь трафик в защищенной корпоративной сети и позволяет выявлять нарушение политик, несанкционированный доступ к данным со стороны неавторизованных

пользователей и блокировать попытки несанкционированной передачи критически важных корпоративных данных.

5. **Почтовая защита.** Основная линия защиты корпоративной почты – это безопасный шлюз. Он фильтрует вредоносные сообщения и отправляет их в карантин. Безопасный шлюз электронной почты может блокировать до 99,99% спама, обнаруживать и удалять письма, содержащие вредоносные ссылки или вложения.

6. **SIEM-системы.** Такие системы собирают и объединяют данные со всей ИТ-инфраструктуры: от хост-систем и приложений до устройств безопасности. После происходит классификация и анализ инцидентов и событий. SIEM-системы на основе правил корреляции получаемых событий выявляют потенциальные инциденты ИБ и уведомляют об этом администратора безопасности.

Организационные меры

1. Повышение осведомленности. Регулярные внутрикорпоративные вебинары и обучение основам ИБ жизненно необходимы для каждой компании. Это позволяет повысить осведомленность сотрудников и убедиться, что они обладают навыками, необходимыми для обнаружения и противодействия атакам.

2. Разграничение прав и ролей сотрудников. Полный доступ каждого сотрудника ко всем данным компании имеет свои риски – утечка клиентских баз, инсайдерская торговля и раскрытие информации об инновационной деятельности. Компаниям необходимо четко разграничивать права доступа пользователей к корпоративным системам, файлам и оборудованию.

Регулярная проверка защищенности: PenTest + аудит

Аудит информационной безопасности ИТ-инфраструктуры – это независимая оценка уровня защищенности компании на соответствие признанным практикам в области обеспечения ИБ, а также законодательным требованиям: международному стандарту ISO/IEC 27001, ФЗ-152 «О персональных данных» и ФЗ-187 «О безопасности критической информационной инфраструктуры». В аудит входят оценка эффективности и надежности существующих методов защиты, анализ слабых мест и уязвимостей, а также оценка их критичности и разработка рекомендаций по их устранению.

Аудит ИБ – важнейшая мера при разработке концепции защиты ИТ-ландшафта. Однако по-настоящему она эффективна только в том случае, если осуществляется с определенной периодичностью, а не как разовая инициатива.

Помимо аудита, стоит обратить внимание и на тестирование на проникновение – PenTest. Это имитация реальной атаки с применением техник и методов, которые используют злоумышленники с целью выявления уязвимых точек в ИТ-инфраструктуре компании. Проведение PenTest позволяет бизнесу получить реальную оценку и полноценную картину уровня защищенности инфраструктуры и всех информационных систем, а также

сформировать список действий и мероприятий, необходимых для повышения уровня безопасности.

Основные виды атак на инфраструктуру и концепция защиты от них

На сегодняшний день большое количество кибератак является успешным по нескольким причинам: они не зависят от местоположения киберпреступника и удаленности от него потенциальной жертвы, а также временных рамок и часовых поясов. Взломанная ИТ-среда может повлечь за собой критические для бизнеса последствия: нанести репутационный ущерб и снизить уровень доверия со стороны клиентов, ведь их данные тоже могут попасть в чужие руки. Взлом инфраструктуры сопряжен и с финансовыми рисками: вследствие оттока заказчиков и потери уникальных инновационных разработок организации, ее конкурентоспособность может значительно упасть на рынке. Ситуация усложняется тем, что методы и тактики злоумышленников постоянно эволюционируют. Хакеры непрерывно адаптируют свои атаки к новым реалиям и технологиям. Современные кибератаки максимально автоматизированы, что позволяет злоумышленникам ускорять их проведение и использовать искусственный интеллект для повышения успеха их реализации. Используемые сегодня средства защиты эффективно выполняют свою задачу по обеспечению безопасности – они блокируют типовые атаки, однако они пока не совершенны в отношении точечных, мануальных угроз.

Основные типы и виды кибератак на инфраструктуру

Как правило, не имеет значение, какую инфраструктуру вы используете – локальную или облачную. Если данные, которые вы передаете, имеют ценность, кто-то захочет их получить. Действия злоумышленников можно разделить на два основных вида – распределенные и целевые атаки.

- **Распределенные кибератаки** представляют собой использование бот-сети и направлены одновременно на большое количество пользователей и ресурсов компаний. Как правило, в таких атаках используются утекшие базы данных организаций и пользователей.
- **Целевыми атаками (APT)** называют заранее спланированное «нападение» на конкретную компанию или инфраструктуру. При этих инцидентах злоумышленник не только получает доступ к внутренним ресурсам, но и остается в сети компании, пока его не обнаружат, – это могут быть дни, месяцы и даже годы. Целевые атаки реализуются хакерами с высокими техническими компетенциями. Они используют автоматизированные инструменты, самостоятельно определяют векторы атаки, эксплуатируют 0-day уязвимости и некоторые особенности системы, опираясь на свой опыт.

Кибератаки представляют опасность как для обычных пользователей, так и для бизнеса. В обоих случаях последствия могут быть не просто неприятными, но и критическими. Согласно статистике за 2020 год, представленной компанией Acronis, DDoS-атаки, фишинг и атаки на видеоконференции возглавили список киберугроз. Однако и другие типы атак приносят массу проблем как бизнесу, так и обычным пользователям.

Злоумышленники шантажируют пользователей мессенджеров с помощью ботов, влезают в сеть через QR-коды и используют уязвимости в настройках или шифровании легальной сети, а также прибегают к классике жанра – атакам «грубой силы». Для того, чтобы лучше понимать действия злоумышленников, необходимо знать, какие существуют типы атак на инфраструктуру и их ключевые особенности.

1. **DDoS-атаки**. Распределенные атаки типа «отказ в обслуживании» реализуются за счет использования нескольких скомпрометированных компьютерных систем в качестве источников атакующего трафика. Эти атаки забивают системы большим количеством запросов, в результате чего пропускная способность снижается, и системы становятся перегруженными и недоступными. По сути, DDoS-атака похожа на неожиданную пробку, забивающую шоссе.
2. **Фишинг.** В основе фишинговых атак лежит использование электронных писем, которые могут быть замаскированы под легитимные сообщения от различных компаний. В таком фейковом сообщении злоумышленники могут предлагать перейти по ссылке, скачать зараженный файл или просить передать конфиденциальные данные пользователя – логины, пароли и номера счетов банковских карт.
3. **Brute-force.** Атаки «грубой силой» являются довольно простым методом проникновения в инфраструктуру и представляют собой «угадывание» учетных записей пользователя. Некоторые злоумышленники используют приложения и скрипты в качестве инструментов перебора, которые пробуют множество комбинаций паролей, чтобы обойти процессы аутентификации. Если пароль слабый, то злоумышленникам понадобится всего пару секунд, поэтому бизнес должен применять строгую политику паролей.
4. **Боты.** Это программный робот, который имитирует или заменяет поведение человека и выполняет простые задачи со скоростью, которая превышает пользовательскую активность. Некоторые боты бывают полезными, и их действия направлены на поддержку пользователей, однако существуют и вредоносные. К примеру, они используются для автоматического сканирования веб-сайтов и поиска уязвимостей, а также выполнения простых кибератак.
5. **Атака через посредника (MITM).** При данном типе атаки киберпреступник становится «третьим лишним» и пропускает весь веб-трафик через себя. В этот момент потенциальная жертва ни о чем не подозревает, что приводит к тому, что все учетные данные для входа в системы оказываются у злоумышленника. После полученная информация может быть использована для кражи корпоративных данных или несанкционированных переводов средств.

Как обезопасить бизнес

Грамотный выбор инструментов обеспечения безопасности ИТ-ландшафта – залог сохранения конфиденциальности и сохранности корпоративных данных. Меры по обеспечению ИБ можно разделить на три

ключевых вида: технические средства, организационные меры и профилактические проверки уровня защищенности.

Технические средства

1. **WAF-комплекс.** Это межсетевой экран для веб-приложений, основными функциями которого являются выявление и блокировка атак. С помощью WAF-комплекса можно не только выявлять вредоносный трафик, но и также определять, какие атаки были направлены на бизнес-критичные системы. Внедрение этого инструмента позволяет бизнесу защититься от атак на бизнес-логику приложений.
2. **Межсетевые экраны (FW).** Межсетевые экраны являются цифровым защитным барьером вокруг ИТ-инфраструктуры, который защищает сеть и предотвращает несанкционированный доступ. Межсетевые экраны обеспечивают безопасность сети путем фильтрации входящего и исходящего сетевого трафика на основе набора правил. В целом, задача межсетевых экранов состоит в том, чтобы уменьшить или исключить возникновение нежелательных сетевых подключений, позволяя при этом свободно протекать всем законным коммуникациям.
3. **Антивирус.** Антивирус – это программа, которая обнаруживает заражение и выполняет действия по его устранению: лечит или удаляет зараженные файлы. Антивирусное ПО работает и как профилактическое средство: оно не только борется, но и предотвращает заражение компьютера в будущем. Антивирусное программное обеспечение позволяет бизнесу защититься от шпионского ПО, вредоносных программ, фишинговых атак, спам-атак и других киберугроз.
4. **DLP** – это набор инструментов и процессов, которые применяюся для предотвращения потери и нелегитимного использования конфиденциальных данных. DLP-система отслеживает весь трафик в защищенной корпоративной сети и позволяет выявлять нарушение политик, несанкционированный доступ к данным со стороны неавторизованных пользователей и блокировать попытки несанкционированной передачи критически важных корпоративных данных.
5. **Почтовая защита.** Основная линия защиты корпоративной почты – это безопасный шлюз. Он фильтрует вредоносные сообщения и отправляет их в карантин. Безопасный шлюз электронной почты может блокировать до 99,99% спама, обнаруживать и удалять письма, содержащие вредоносные ссылки или вложения.
6. **SIEM-системы.** Такие системы собирают и объединяют данные со всей ИТ-инфраструктуры: от хост-систем и приложений до устройств безопасности. После происходит классификация и анализ инцидентов и событий. SIEM-системы на основе правил корреляции получаемых событий выявляют потенциальные инциденты ИБ и уведомляют об этом администратора безопасности.

Организационные меры

1. Повышение осведомленности. Регулярные внутрикорпоративные вебинары и обучение основам ИБ жизненно необходимы для каждой

компании. Это позволяет повысить осведомленность сотрудников и убедиться, что они обладают навыками, необходимыми для обнаружения и противодействия атакам.

2. Разграничение прав и ролей сотрудников. Полный доступ каждого сотрудника ко всем данным компании имеет свои риски – утечка клиентских баз, инсайдерская торговля и раскрытие информации об инновационной деятельности. Компаниям необходимо четко разграничивать права доступа пользователей к корпоративным системам, файлам и оборудованию.

Регулярная проверка защищенности: PenTest + аудит

Аудит информационной безопасности ИТ-инфраструктуры – это независимая оценка уровня защищенности компании на соответствие признанным практикам в области обеспечения ИБ, а также законодательным требованиям: международному стандарту ISO/IEC 27001, ФЗ-152 «О персональных данных» и ФЗ-187 «О безопасности критической информационной инфраструктуры». В аудит входят оценка эффективности и надежности существующих методов защиты, анализ слабых мест и уязвимостей, а также оценка их критичности и разработка рекомендаций по их устранению.

Аудит ИБ – важнейшая мера при разработке концепции защиты ИТ-ландшафта. Однако по-настоящему она эффективна только в том случае, если осуществляется с определенной периодичностью, а не как разовая инициатива.

Помимо аудита, стоит обратить внимание и на тестирование на проникновение – PenTest. Это имитация реальной атаки с применением техник и методов, которые используют злоумышленники с целью выявления уязвимых точек в ИТ-инфраструктуре компании. Проведение PenTest позволяет бизнесу получить реальную оценку и полноценную картину уровня защищенности инфраструктуры и всех информационных систем, а также сформировать список действий и мероприятий, необходимых для повышения уровня безопасности.