УДК 004 **Информационные технологии**

Вартанян Артур Артурович, *магистрант, ФГБОУ ВО*
Донской государственный технический университет,
г. Ростов-на-Дону, РФ
e-mail: varttann@rambler.ru

УГРОЗЫ И АТАКИ СЕТЕВОЙ БЕЗОПАСНОСТИ

Аннотация: Сетевая безопасность охватывает множество технологий, процессов и устройств, направленных на обеспечение целостности, конфиденциальности и доступности компьютерных сетей. Независимо от их размера, отрасли или типа инфраструктуры организациям требуется сетевая безопасность для защиты от постоянно меняющегося ландшафта угроз, связанных с кибератаками.

Ключевые слова: информационная безопасность, ландшафта угроз, киберугроза, сети, сетевая безопасность.

Annotation: Network security spread of many technologies, processes and devices aimed at ensuring the openness, confidentiality and availability of computer networks. Regardless of their size, or industry type, a confidential organization needs network security to protect against the ever-changing threat of cyberattacks.

Key words: information security, landscape threat, cyber threat, networks, network security.

Введение

Сетевая безопасность охватывает множество технологий для обеспечения безопасности компьютерных сетей и защиты от вредоносных атак [3]. Некоторые из ключевых технологий, связанных с сетевой безопасностью, включают в себя:

1. Брандмауэры (firewalls) – программное или аппаратное обеспечение, которое может обнаруживать и блокировать нежелательный трафик в компьютерной сети.

2. VPN (Virtual Private Network) – технология шифрования, которая обеспечивает безопасное соединение между удаленными устройствами в разных локациях и защищает пересылаемые данные.

3. IDS (Intrusion Detection System) – системы обнаружения вторжений, которые помогают выявлять попытки несанкционированного доступа к компьютерной сети.

4. IPS (Intrusion Prevention System) – системы предотвращения вторжений, которые могут блокировать попытки несанкционированного доступа к компьютерной сети и незаконного использования данных.

5. Антивирусные программы и антиспам – программное обеспечение, которое обнаруживает и блокирует вредоносные программы и электронную почту, содержащую спам.

6. SIEM (Security Information and Event Management) – системы сбора, хранения и анализа информации о событиях в компьютерной сети, позволяющие быстро обнаруживать инциденты безопасности и вести расследование в случае необходимости.

7. Системы шифрования – технологии, которые обеспечивают конфиденциальность данных, защищая их от несанкционированного доступа.

Эти технологии используются в комплексе и взаимодействуют между собой, чтобы обеспечить надежную защиту сетей и информации, хранящейся в них.

Основная часть

Традиционный подход к сетевой безопасности предполагает использование правил и конфигураций, которые используют программные и аппаратные технологии для защиты сети и ее данных. Однако этот механизм не отвечает требованиям современных сложных сетевых архитектур, которые имеют большую и более уязвимую поверхность для атак, чем традиционные сети

прошлого, основанные на периметре [1].

Злоумышленники хорошо разбираются в использовании уязвимостей современных сетей и используют передовые технологии, такие как автоматизация и ботнеты на основе искусственного интеллекта, чтобы обнаружить и использовать эти слабые места, избегая при этом обнаружения. Они тщательно изучают каждый аспект сети, включая устройства, данные, пользователей, местоположения и приложения.

Распространенные угрозы сетевой безопасности включают вредоносное ПО, фишинговые схемы и DDoS-атаки. Неспособность защититься от этих угроз может привести к несоблюдению нормативных требований, что повышает уровень риска. Для смягчения этих угроз организациям требуется широкий спектр технологий, включая брандмауэры, сегментацию сети, IP-адреса и принципы безопасности с нулевым уровнем доверия.

Когда дело доходит до защиты компьютерных систем и сетей, сетевая безопасность и кибербезопасность являются двумя важными областями. Сетевая безопасность в первую очередь направлена на обеспечение безопасности сетевой инфраструктуры, включая периметр сети, маршрутизаторы и коммутаторы [2]. С другой стороны, кибербезопасность охватывает сетевую безопасность и распространяется на другие области, такие как хранение и транспортировка данных.

Хотя сетевая безопасность и кибербезопасность имеют некоторые общие черты, их планирование отличается. План кибербезопасности включает в себя план сетевой безопасности, но планы сетевой безопасности могут существовать независимо без более широкой стратегии кибербезопасности.

Вредоносное программное обеспечение (вредоносное ПО) - это программа, нацеленная на информационные системы и имеющая различные формы, каждая из которых предназначена для выполнения определенных вредоносных действий. Например, программы-вымогатели шифруют файлы и удерживают их для получения выкупа, шпионские программы незаметно шпионят за жертвами, а троянские программы проникают в системы.

Злоумышленники используют вредоносное ПО для достижения различных целей, таких как кража конфиденциальных данных, тайное копирование данных, блокирование доступа к файлам, нарушение работы системы или выведение ее из строя.

Фишинг - это вид мошенничества, при котором злоумышленники выдают себя за авторитетные организации лично, по электронной почте или используя другие методы коммуникации. Фишинговые электронные письма обычно используются для распространения вредоносных вложений или ссылок, которые выполняют различные функции, такие как извлечение информации об учетной записи жертвы или учетных данных для входа [4].

Боты - это небольшие программы, которые автоматизируют веб-запросы для различных целей, выполняя свои задачи без вмешательства человека, такие как сканирование содержимого веб-сайтов, и проверка номеров украденных кредитных карт. Атаки ботов используют автоматические веб-запросы для манипулирования приложениями, веб-сайтами, конечными пользователями или API-интерфейсами или нарушения их работы. Первоначально бот-атаки использовались в основном для рассылки спама и отказа в обслуживании, но превратились в сложные операции с экономией средств и инфраструктурой, которые допускают дополнительные, более разрушительные атаки.

Распределенные атаки типа "Отказ в обслуживании" (DDoS). DDoS-атака использует несколько скомпрометированных компьютерных систем для атаки на цель, вызывая отказ в обслуживании пользователей целевого ресурса. Он отправляет поток сообщений, искаженных пакетов или запросов на подключение к целевой системе, заставляя ее замедляться или полностью отключаться, отказывая в обслуживании законным системам и пользователям. DDoS-атаки могут быть нацелены на веб-сайты, серверы и другие сетевые ресурсы.

Расширенная постоянная угроза (APT) - это целенаправленная и устойчивая атака, при которой злоумышленники получают несанкционированный доступ к сети, оставаясь незамеченными в течение длительного времени. Злоумышленники обычно запускают APT-атаки для

кражи данных, а не для нанесения ущерба целевой сети. Большинство атак APT направлены на получение и поддержание долгосрочного скрытого доступа к целевой сети. APT-атаки требуют больших усилий и ресурсов, и субъекты обычно выбирают дорогостоящие цели, такие как крупные корпорации и национальные государства, чтобы обеспечить отдачу от инвестиций [3].

Атака на загрузку с диска - это непреднамеренная загрузка вредоносного кода на компьютер или мобильное устройство, подвергающая жертву кибератаке. В отличие от других кибератак, жертве не нужно активировать атаку. Чтобы заразиться, пользователю не нужно ничего нажимать, загружать или открывать вредоносное вложение электронной почты. Загрузка с диска использует уязвимости приложений, веб-браузера или операционной системы, которые могут возникнуть из-за отсутствия обновлений или сбоев в их работе.

Атаки на систему доменных имен (DNS). DNS-атака происходит, когда злоумышленники используют уязвимости в Системе доменных имен (DNS), которая была разработана для удобства использования, а не для обеспечения безопасности. Злоумышленники используют связь между клиентами и серверами для запуска атак, таких как открытый текстовый обмен данными между клиентами и DNS-серверами или вход на веб-сайт поставщика DNS с использованием украденных учетных данных и перенаправление записей DNS.

Постоянно меняющийся ландшафт угроз является одной из основных проблем, стоящих перед сетевой безопасностью. С быстрым развитием технологий злоумышленники находят новые способы проникновения в корпоративные сети и использования их, что требует внедрения компаниями новых инструментов безопасности для защиты своих сетей. Кроме того, расширение стратегии безопасности организации создает большую площадь для атак, поскольку все пользователи сети несут ответственность за безопасность, что затрудняет разработку стратегии, которой могли бы следовать все.

Заключение

Использование персональных устройств и политик удаленной работы является еще одной проблемой сетевой безопасности. Политики BYOD создают

сложную распределенную сеть и увеличивают площадь атаки, при этом каждое персональное устройство нуждается в защите. Безопасность беспроводных сетей особенно важна для компаний, которые позволяют сотрудникам работать удаленно, поскольку удаленные пользователи часто получают доступ к конфиденциальным корпоративным ресурсам и данным через незащищенную общедоступную сеть.

Безопасность в облаке также является серьезной проблемой. В то время как поставщики облачных услуг и управляемых сервисов несут ответственность за обеспечение безопасности, организации обычно несут ответственность за защиту своих собственных данных и приложений. Поэтому организациям следует осуществлять мониторинг всех точек доступа к сети и внедрять единую стратегию безопасности в гибридной среде.

Библиографический список:

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.