УДК 004 **Информационные технологии**

Цыбенко Олег Сергеевич, *магистрант,*
ДГТУ Ростов-на-Дону, РФ
e-mail: olegohi@rambler.ru

ТЕХНОЛОГИИ И РЕШЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Аннотация: Различные технологии и решения сетевой безопасности могут решить эти проблемы. Брандмауэр и технологии межсетевого экрана нового поколения (NGFW) контролируют входящий и исходящий трафик в сетях и предотвращают попадание вредоносного трафика в сеть. Брандмауэры веб-приложений (WAF) фильтруют, отслеживают и блокируют HTTP-трафик, поступающий в веб-службу и из нее, чтобы предотвратить использование злоумышленниками известных уязвимостей в веб-приложениях. Системы предотвращения вторжений (IPS) обнаруживают или предотвращают атаки на сетевую безопасность, такие как грубая сила и DoS-атаки. Сегментация сети и микросегментация могут помочь определить границы между сегментами сети и логически разделить сеть на отдельные сегменты безопасности соответственно. Эти технологии и решения помогают улучшить контроль доступа и безопасность, защитить каждую виртуальную машину в сети и повысить устойчивость сети к атакам.

Ключевые слова: сетевая безопасность, технологии сетевой безопасности, вторжение, информационная безопасность.

Abstract: Various technologies and network security solutions can solve these problems. Firewall and Next-Generation Firewall (NGFW) technologies monitor incoming and outgoing traffic on networks and prevent malicious traffic from entering the network. Web application firewalls (WAFs) filter, monitor, and block HTTP traffic to and from a web service to prevent attackers from exploiting known vulnerabilities

in web applications. Intrusion prevention systems (IPS) detect or prevent network security attacks such as brute force and DoS attacks. Network segmentation and micro-segmentation can help define the boundaries between network segments and logically divide the network into separate security segments, respectively. These technologies and solutions help improve access control and security, protect every virtual machine on your network, and make your network more resilient to attacks.

Keywords: network security, network security technologies, intrusion, information security.

Введение

Сетевая безопасность – это практика обеспечения защиты компьютерных сетей от несанкционированного доступа, утечек данных, вирусов, вредоносных программ и других угроз, которые могут нанести вред сети, ее устройствам и пользователям. Сетевая безопасность включает в себя использование различных технологий, методов и процессов, таких как шифрование данных, аутентификация и авторизация пользователей, мониторинг активности в сети, обнаружение и предотвращение атак, а также обучение и развитие компетенций пользователей в области безопасности информации.

Основная часть

Для обеспечения безопасного доступа к внутренним или облачным ресурсам используются средства контроля доступа, позволяющие определить, каким пользователям и устройствам разрешен доступ к ним. Двумя распространенными современными реализациями являются безопасный удаленный доступ и доступ к сети с нулевым уровнем доверия (ZTNA). Технологии безопасного удаленного доступа обеспечивают аутентификацию, безопасность конечных точек, повышение привилегий и безопасные удаленные подключения. Виртуальные частные сети (VPN) являются одним из примеров безопасного удаленного доступа, который защищает личность пользователей путем шифрования их данных и маскировки их IP-адреса и местоположения. Это делает его полезным при подключении к небезопасным сетям, таким как

общедоступные соединения Wi-Fi, для защиты пользователей от злоумышленников, пытающихся украсть конфиденциальные данные [1].

Безопасность с нулевым уровнем доверия — это модель, которая требует, чтобы все объекты в сетях были под подозрением, и включает различные средства контроля для защиты от внутренних и внешних угроз. ZTNA, также известная как решения с программно-определяемым периметром (SDP), позволяет организациям определять подробный доступ к приложениям и предоставлять доступ в соответствии с принципом наименьших привилегий.

Контроль доступа к сети (NAC) - это решение, которое предотвращает несанкционированный доступ устройств и пользователей к защищенным сетям с помощью инструментов сетевого администратора и общекорпоративных политик. Это позволяет организациям назначать определенные учетные записи, классифицировать пользователей на основе их должностных обязанностей, предоставлять привилегии ограниченного доступа гостевым пользователям, регистрировать одобренные устройства и ограничивать доступ на основе операционной системы устройства или установленного программного обеспечения безопасности [2].

Решения по предотвращению потери данных (DLP) помогают предотвратить обмен информацией о компании и конфиденциальными данными сотрудников вне сети. Распространенные события DLP включают печать, загрузку, отправку файлов и пересылку сообщений.

Решения для управления информацией о безопасности и событиями (SIEM) обеспечивают полную видимость действий в защищенной сети путем сбора и объединения данных журналов из различных структур безопасности внутри организации. SIEM создает отчет о безопасности, включающий анализ, в котором отмечается ненормальная сетевая активность и инциденты безопасности. Администраторы могут использовать анализ SIEM для быстрого устранения угроз с помощью различных средств, таких как изоляция сетевых сред, блокирование вредоносных полезных нагрузок и ограничение доступа пользователей. Он также предоставляет подробную информацию о сетевом

трафике и сигнатурах, чтобы помочь администраторам принимать обоснованные решения по повышению сетевой безопасности и минимизации воздействия угроз [3].

Защита конечных точек: Безопасность конечных точек - это подход, который включает в себя несколько уровней защиты от угроз, которые могут исходить от пользовательских конечных точек, таких как ноутбуки, планшеты и смартфоны, подключенные к сети. Цель состоит в том, чтобы обеспечить безопасность устройств, данных и сетей путем внедрения различных механизмов, таких как антивирусное программное обеспечение, шифрование и предотвращение потери данных [2].

Рекомендации по сетевой безопасности:

Аудит сети и системы контроля безопасности: Сетевой аудит необходим для получения точной информации для оценки состояния безопасности организации. Преимущества сетевого аудита включают выявление потенциальных уязвимостей, требующих внимания, обнаружение неиспользуемых или ненужных приложений, оценку надежности брандмауэра для точной настройки, измерение состояния сетевых серверов, программного обеспечения, приложений и оборудования, подтверждение эффективности всей инфраструктуры безопасности и оценку состояния текущих резервных копий серверов. Для организаций крайне важно проводить регулярные и последовательные проверки с течением времени.

Преобразование сетевых адресов (NAT): NAT компенсирует нехватку адресов в сети IPv4 путем преобразования частных адресов внутри организации в маршрутизируемые адреса в общедоступной сети, такой как Интернет. Организации используют NAT для подключения нескольких компьютеров к общедоступному Интернету с использованием одного IP-адреса. NAT работает в паре с брандмауэрами, обеспечивая дополнительную защиту внутренних сетей. Хосты внутри защищенных сетей обычно могут взаимодействовать с внешним миром. Однако внешние системы должны проходить через блоки NAT, чтобы войти во внутреннюю сеть. NAT также позволяет использовать меньшее

количество IP-адресов для обмана злоумышленников, чтобы они не знали, на какой хост нацелиться.

Централизованное ведение журнала и немедленный анализ журнала: Организациям следует регистрировать подозрительные логины и различные компьютерные события для выявления аномалий. Цель состоит в том, чтобы восстановить то, что произошло во время существующих или прошлых атак, чтобы определить необходимые шаги для улучшения процесса обнаружения угроз и ускорения реагирования на будущие события. Субъекты угроз часто пытаются избежать обнаружения, поэтому мониторинг и запись событий в журнале имеют решающее значение для выявления потенциальных нарушений безопасности.

План резервного копирования и восстановления: Компании работают в среде, где вопрос заключается в том, когда они будут взломаны, а не в том, будут ли они взломаны. Цель стратегии резервного копирования и восстановления - свести к минимуму время простоя и ограничить общую стоимость нарушений и других инцидентов. Важно создавать резервные копии критически важных и конфиденциальных данных, чтобы обеспечить непрерывность и предотвратить потерю данных. Планы резервного копирования и восстановления особенно важны для обеспечения устойчивости к различным угрозам, особенно атакам программ-вымогателей и сбоям в работе системы.

Заключение

В статье содержатся ценные рекомендации по обеспечению сетевой безопасности в организациях. Сетевой аудит необходим для выявления потенциальных уязвимостей и получения доступа к состоянию безопасности организации. Это помогает организациям подключать несколько компьютеров к общедоступному Интернету, используя один IP-адрес, обеспечивая при этом дополнительную защиту внутренних сетей. Рекомендуется централизованное ведение журнала и немедленный анализ журналов для выявления потенциальных нарушений безопасности и улучшения процессов обнаружения угроз. Наконец, планы резервного копирования и восстановления имеют

решающее значение для обеспечения устойчивости к различным угрозам и предотвращения потери данных.

Выполняя эти рекомендации, организации могут повысить безопасность своей сети и защитить от киберугроз. Организациям важно принимать упреждающие меры для обеспечения безопасности своей сети и данных в современных условиях, когда вопрос заключается не в том, будут ли они взломаны, а в том, когда.

Библиографический список:

1. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.

2. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.

3. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.