УДК 004

ПРИНЦИПЫ И МЕТОДЫ МЕЖСЕТЕВОЙ БЕЗОПАСНОСТИ В КОМПЛЕКСНЫХ СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ

Тулупова И.С.

Студент 4 курса,

ФГБОУ ВО "Поволжский Государственный Университет Телекоммуникаций и Информатики"

Самара, Россия

Буранова М.А.

Профессор кафедры информационной безопасности

ФГБОУ ВО "Поволжский Государственный Университет Телекоммуникаций и Информатики"

Самара, Россия

Аннотация. Данная статья посвящена изучению принципов и методов межсетевой безопасности в комплексных системах защиты информации. Межсетевая безопасность является важной составляющей в комплексных системах защиты информации, которая обеспечивает защиту компьютерных сетей от нежелательного доступа, повреждения данных и утечки конфиденциальной информации. Она используется для обеспечения целостности, конфиденциальности и доступности информации, передаваемой в рамках компьютерных сетей и Интернета, а с учетом развития инфокоммуникационных технологий становится все более актуальной.

В работе описываются основные принципы обеспечения межсетевой безопасности: аутентификация, авторизация, конфиденциальность, целостность и доступность в условиях внедрения новых технологий и архитектур построения инфокоммуникационных сетей. Рассмотрены различные методы обеспечения безопасности в межсетевых системах, такие как фильтрация трафика, использование брандмауэров и аппаратных средств, шифрование информации, контроль доступа и др. Особое внимание уделено важности обучения пользователей, которое является необходимым элементом в современных системах защиты информации. Работа также посвящена моделированию межсетевой безопасности в комплексных системах защиты информации, а также анализу применения этих принципов в реальной жизни.

Ключевые слова: межсетевая безопасность, комплексная система защиты информации, безопасность, аутентификация, авторизация, конфиденциальность

PRINCIPLES AND METHODS OF INTER-NETWORK SECURITY IN COMPLEX INFORMATION SECURITY SYSTEMS

Tulupova I.S.

Student 2 course

Volga state University of telecommunications and Informatics,

Samara, Russia

Buranova M.A.

Professor of the Department of Information Security

Volga state University of telecommunications and Informatics,

Samara, Russia

Annotation. This article is devoted to the study of the principles and methods of inter-network security in complex information security systems. Inter-network security is an important component in complex information security systems, which protects computer networks from unwanted access, data corruption and leakage of confidential information. It is used to ensure the integrity, confidentiality and availability of information transmitted within computer networks and the Internet and given the development of infocommunication technologies, it is becoming increasingly relevant.

An overview of the existing principles of inter-network security is presented, namely: authentication, authorization, confidentiality, integrity and availability. The methods of ensuring inter-network security, such as traffic filtering, the use of firewalls and hardware, information encryption, access control, etc. are considered. Also, special attention is paid to the issues of user training, the importance of which in modern information security systems cannot be overestimated. The work is devoted to the modeling of inter-network security in complex information security systems, as well as the analysis of specific cases of their application in real life.

Keywords: inter-network security, integrated information security system, security, authentication, authorization, confidentiality

1 Введение

Очевидно, что в интернет-сети безопасность информации – ключевая задача для компаний и организаций любого уровня, учитывая возможные угрозы, связанные с нарушением конфиденциальности, целостности и доступности информации. Эти угрозы могут привести к серьезным последствиям, затрагивающим как индивидуальных пользователей, так и целые компании, и организации. Понимание важности защиты информации и реализация соответствующих мер - важный элемент деятельности в современном мире.

Интернет, который используется миллионами людей ежедневно для общения, коммерческой деятельности и развлечений, базируется на сетевой архитектуре, разработанной более 40 лет назад. Это подчеркивает необходимость постоянного обновления и совершенствования средств защиты информации, чтобы гарантировать ее безопасность во время ее нахождения в глобальной сети.

Для решения этой проблемы разрабатываются комплексные системы защиты информации, включающие в себя методы межсетевой безопасности. Принципы межсетевой безопасности позволяют обеспечить защиту информации на различных уровнях, начиная от аутентификации пользователя и проверки прав доступа до фильтрации трафика, шифрования и контроля доступа на уровне сетевых устройств.

Цель данной работы - ознакомление с принципами и методами межсетевой безопасности в комплексных системах защиты информации, их применение и анализ примеров успешного использования в реальной жизни. Работа представляет собой обзор существующих методов и принципов межсетевой безопасности, а также подробное рассмотрение их применения в комплексных системах защиты информации на современном этапе развития инфокоммуникационных сетей [1].

2 Межсетевая безопасность

Межсетевая безопасность является важной составляющей в комплексных системах защиты информации, которая обеспечивает защиту компьютерных сетей от нежелательного доступа, повреждения данных и утечки конфиденциальной информации. Она используется для обеспечения целостности, конфиденциальности и доступности информации, передаваемой в рамках компьютерных сетей и Интернета.

Также, следует отметить, что ключевым элементом комплексной системы защиты информации является обучение пользователей безопасным методам

работы с компьютерной техникой. Это включает в себя правильный выбор и использование паролей, регулярное обновление систем безопасности, использование антивирусных и противофишинговых программ, и т.д.

Таким образом, принципы и методы межсетевой безопасности идут в ногу с развитием технологий и охватывают комплексный подход в области защиты информации. Они помогают распознать и предотвратить угрозы в рамках сетевой безопасности, что в свою очередь обеспечивает сохранность и целостность конфиденциальной информации, а также предотвращает возможные утечки и кражи. Следование принципам межсетевой безопасности и использование соответствующих методов защиты – это важная составляющая в надежной защите информации в условиях быстро развивающихся технологий.

3 Принципы и методы межсетевой безопасности

Принципы межсетевой безопасности - это основные принципы, которые должны быть применены для обеспечения безопасности сетей и передачи данных между ними [2]. Рассмотрим каждый принцип подробнее:

1. Идентификация объектов, получающих доступ к ресурсам – подразумевает аутентификацию.

2. Защита ресурсов от подслушивания во время транспортировки – подразумевает конфиденциальность

3. Предотвращение несанкционированного доступа – подразумевает авторизацию и конфиденциальность.

4. Обеспечение надежной доставки запрашиваемых ресурсов в неизмененном виде – подразумевает целостность.

5. Доступность - это возможность получения доступа к данным информации в любое время, когда это необходимо. Доступность может быть обеспечена использованием резервного хранения, отказоустойчивых систем и других техник.

Кроме того, существуют различные методы межсетевой безопасности, которые используются для защиты информации. Некоторые из них включают в себя следующие:

1. Фильтрация трафика - это контроль трафика, проходящего через сеть, чтобы убедиться, что он соответствует политике безопасности.

2. Использование брандмауэров и аппаратных средств - это метод, заключающийся в использовании средств обеспечения безопасности для блокировки нежелательного трафика и противодействия атакам.

3. Шифрование информации - это метод, используемый для защиты информации от несанкционированного доступа путем применения алгоритмов шифрования.

4. Контроль доступа - это метод, используемый для регулирования доступа пользователей к ресурсам сети на основе ролей и прав доступа.

5. Обучение пользователей - это важный метод обеспечения безопасности в комплексных системах защиты информации, так как большинство уязвимостей связаны с неопытностью и ошибками пользователей.

Применение этих принципов и методов межсетевой безопасности в комплексных системах защиты информации может существенно улучшить безопасность сетей и предотвратить потенциальные угрозы, связанные с нарушением доступа, изменением или уничтожением данных [3].

4 Обучение пользователей межсетевой безопасности

Одним из наиболее важных аспектов межсетевой безопасности в комплексных системах защиты информации является обучение пользователей. Все современные системы защиты информации разработаны с учётом того, что люди являются слабым звеном в процессе защиты информации и могут стать жертвами социального инжиниринга, фишинга или других видов мошенничества [4].

Обучение пользователей должно стать обязательным элементом комплексных систем защиты информации, поскольку это позволит устранить многие уязвимости, связанные с человеческим фактором. Пользователи должны знать, как правильно использовать пароли, как не стать жертвами фишинга, как распознать поддельные сайты, как поступать в случае утечки информации и т.д.

Важно понимать, что обучение пользователей не является одноразовым мероприятием, оно должно проводиться регулярно и включать как общие советы, так и конкретные рекомендации, и инструкции по использованию конкретных функций системы защиты информации. Кроме того, стоит обратить внимание на обучение новым пользователям, которые только начинают работать с системой.

Обучение пользователей может проводиться как силами IT-специалистов организации, так и с привлечением внешних экспертов, которые смогут предоставить дополнительные знания и опыт. В любом случае, обучение пользователей является обязательным и необходимым этапом в процессе защиты информации в комплексных системах защиты информации. Только так можно достичь высокого уровня защиты информации и защитить свою организацию от многих угроз, которые могут возникнуть в онлайн-среде.

Помимо обучения пользователей правильному использованию системы защиты информации, также важно обучение пользователей "общеизвестным" средствам защиты. Например, пользователи должны знать, какую антивирусную программу использовать, какие настройки безопасности в браузере применять и какие пароли надёжны.

При разработке комплексных систем защиты информации необходимо учитывать, что пользователи могут допускать ошибки и действовать вопреки рекомендациям. Поэтому следует использовать передовые методы обработки ошибок, а также следить и анализировать поведение пользователей, чтобы выявлять возможные уязвимости.

Наконец, обучение пользователей должно быть не только техническим, но и социальным аспектом. Пользователи должны понимать, что защита информации – это задача не только IT-специалистов, но и каждого сотрудника организации. Они должны понимать ответственность за сохранность информации и внимательно относиться к своим действиям и действиям коллег.

Так, в 2013 году крупный ритейлер Target также стал жертвой кибератаки. В результате атаки были скомпрометированы данные более чем 110 миллионов пользователей. Хакеры использовали фишинг-атаку в системах безопасности компании, чтобы получить доступ к системе платежей, где они украли данные описанные карт пользователя. Target быстро заявил об инциденте и предпринял меры для обеспечения безопасности пользователей, включая бесплатный мониторинг кредитных отчетов и замену карт для всех пострадавших пользователей. Target также усилил свои системы безопасности и начал требовать от поставщиков использование более безопасных методов передачи данных. Эта кибератака стала напоминанием о том, насколько важно иметь безопасность данных на первом месте и предпринимать меры, чтобы улучшить защиту систем и обучить пользователей использовать безопасные практики при работе в интернете.

В целом, обучение пользователей является одним из ключевых направлений в области межсетевой безопасности в комплексных системах защиты информации. Это позволит устранить многие уязвимости, связанные с человеческим фактором, и загнать злонамеренных пользователей в тупик. Поэтому обучение должно стать обязательным этапом в процессе защиты информации в комплексных системах защиты информации [5].

5 Моделирование межсетевой безопасности

Моделирование межсетевой безопасности комплексных систем защиты информации является важным аспектом обеспечения безопасности данных. Оно помогает определить риски и слабые места в системе безопасности и принимать соответствующие меры для защиты информации [6].

Моделирование межсетевой безопасности может происходить на различных уровнях, от инфраструктуры сети до прикладных систем. В этом процессе требуется моделирование архитектуры сети, анализ угроз и уязвимостей, создание политики безопасности и тестирование системы на прочность.

Существует несколько подходов к моделированию межсетевой безопасности, включая статическое и динамическое моделирование, а также моделирование при помощи аналитических инструментов и симуляторов.

Статистическое и динамическое моделирование могут быть использованы в межсетевой безопасности для анализа угроз безопасности и разработки стратегий защиты.

Статистическое моделирование может использоваться для анализа данных безопасности и выявления узких мест в системах безопасности. Например, статистическая аналитика может использоваться для идентификации аномального поведения пользователей, что может свидетельствовать о взломе или несанкционированном доступе к сети. Также статистическая модель может использоваться для прогнозирования вероятности атаки или выхода в интернет новых уязвимостей.

Динамическое моделирование может использоваться для симуляции различных сценариев атаки и оценки их последствий. Например, можно создать модель атаки на веб-портал и исследовать, как система реагирует и какие меры защиты наиболее эффективны. Также динамическое моделирование может использоваться для разработки "черных ящиков" или "имитационных моделей", которые эмулируют некоторые аспекты реальной системы и позволяют тестировать различные стратегии защиты, прежде чем они будут внедрены на реальных системах.

Оба подхода могут использоваться для анализа уязвимостей, анализа логов и секьюрити-трассировки, что помогает обеспечивать мультислойную и активную защиту межсетевой безопасности. Кроме того, можно использовать комбинацию этих двух подходов для создания более точных и полных моделей безопасности, что помогает обеспечивать максимальную защиту от существующих угроз и новых видов атак.

Для комплексных систем защиты информации является необходимым создание централизованных систем управления безопасностью, которые большим количеством инструментов и функций позволяют определить уровень угроз, осуществлять мониторинг, контролировать доступ и обнаруживать инциденты безопасности.

Поскольку киберугрозы постоянно меняются, заложенные в механизм безопасности должны быть адаптивными и динамичными, чтобы отвечать изменяющимся условиям. В этом контексте, моделирование межсетевой безопасности комплексных систем защиты данных является важным инструментом для обеспечения безопасности данных и киберзащиты в общем.

6 Заключение

Межсетевая безопасность - это очень важная область, которая стала особенно актуальной в эпоху цифровой трансформации. Постоянные угрозы со стороны хакеров, вирусов, мошенников и других злоумышленников требуют от нас принятия серьезных мер для защиты информации, передаваемой между различными сетями.

Для обеспечения межсетевой безопасности необходимо использовать различные методы и технологии, включая статистическое и динамическое моделирование, контроль доступа, шифрование, аутентификацию и детекцию вторжений. Важным элементом в межсетевой безопасности является также обучение пользователей, что помогает обеспечить более эффективный контроль и сокращение рисков халатности.

Межсетевая безопасность - это не статичный процесс, и требует постоянного совершенствования и адаптации к появляющимся угрозам и новым технологиям. Только благодаря непрерывному совершенствованию и правильному подходу можно создать действительно надежную и эффективную систему межсетевой безопасности, которая обеспечит максимальную защиту от угроз и предоставит защиту для передачи информации между различными сетями.

Библиографический список

1. Бобков, Е.О. Обеспечение информационной безопасности критической информационной инфраструктуры с IOT-технологиями. / Е.О. Бобков, Е.А. Балашова, Д.Н. Панин. // Экономика и общество: перспективы развития. Сборник материалов IV Всероссийской научно-практической конференции. - Киров, 2020. -С. 221-225.

2. Бобков, Е.О. Анализ кибератак на критическую информационную инфраструктуру с IOT-технологиями / Е.О. Бобков, Е.А. Балашова, Д.Н. Панин // Автономия личности. 2020. № 2 (22). С. 55-64.

3. Панин, Д.Н Облачная безопасность-рекомендации по снижению угроз / Д.Н Панин, Д.Н. Филиппова, Д.С. Пирогов.// Информатизация и связь. 2020. № 2. С. 73-76.

4. Кафейников, Д. Н. Межсетевая безопасность. VPN и MPLS / Д. Н. Кафейников. - СПб.: Питер, 2010. - 448 с.

5. Багрин, С. Межсетевая безопасность с использованием FreeBSD / С. Багрин, Е. Григорьев. - М.: Издательский дом "Символ-Плюс", 2004. - 704 с.

6. Малиновский, Б. В. Межсетевая безопасность: физические и логические основы / Б. В. Малиновский. - СПб.: БХВ-Петербург, 2004. - 336 с.

Оригинальность 97%