УДК 004 **Информационные технологии**

Рагимов Эседуллах Керимович, *магистрант,*
ДГТУ Ростов-на-Дону, РФ

АНАЛИЗ РИСКОВ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В современную цифровую эпоху зависимость от технологий и Интернета является повсеместной. С увеличением объема данных, генерируемых и хранящихся на серверах, защита этих ценных активов стала важнейшей задачей. Защита серверов включает в себя ряд стратегий и мер, направленных на защиту серверов от потенциальных угроз, таких как несанкционированный доступ, утечка данных, атаки вредоносных программ и системные сбои. В данной статье исследуется важность защиты серверов и освещаются некоторые ключевые подходы к повышению безопасности и отказоустойчивости серверов.

Ключевые слова: информационная безопасность, риски, анализ рисков.

Annotation: In today's digital age, dependence on technology and the Internet is ubiquitous. With the increasing volume of data generated and stored on servers, protecting these valuable assets has become a critical concern. Server security includes a number of strategies and measures aimed at protecting servers from potential threats such as unauthorized access, data leakage, malware attacks and system failures. This article explores the importance of server security and highlights some key approaches to improving server security and resiliency.

Key words: information security, risks, risk analysis.

Введение

Серверы формируют основу ИТ-инфраструктуры любой организации, играя жизненно важную роль в хранении, обработке и распространении данных

и услуг. Последствия взлома сервера могут быть серьезными, включая потерю или кражу конфиденциальной информации, нарушение бизнес-операций, ущерб репутации и финансовые потери. Следовательно, надежная защита сервера необходима для снижения этих рисков и обеспечения конфиденциальности, целостности и доступности ценных данных.

Основная часть

Контроль доступа: Контроль доступа к серверам является первой линией защиты от несанкционированного проникновения. Внедрение надежных механизмов аутентификации, таких как сложные пароли, многофакторная аутентификация и протоколы безопасного доступа, такие как Secure Shell (SSH), помогает гарантировать, что только авторизованный персонал сможет получить доступ к серверу. Кроме того, управление доступом на основе ролей (RBAC) может быть использовано для ограничения привилегий в зависимости от должностных ролей, сводя к минимуму риск внутренних угроз [1].

Шифрование: Шифрование данных как при передаче, так и в состоянии покоя имеет решающее значение для сохранения их конфиденциальности. Протоколы безопасности транспортного уровня (TLS) или Secure Sockets Layer (SSL) могут использоваться для шифрования данных, передаваемых по сетям, в то время как решения для шифрования дисков, такие как BitLocker или FileVault, могут защитить данные, хранящиеся на серверах [2]. Шифрование делает данные нечитаемыми для неавторизованных лиц, даже если им удастся получить доступ к серверу.

Брандмауэры и системы обнаружения вторжений (IDS): Брандмауэры действуют как барьер между внутренними сетями и внешним миром, отслеживая и фильтруя входящий и исходящий трафик на основе предопределенных правил безопасности. Системы обнаружения вторжений дополняют брандмауэры, отслеживая сетевой трафик и выявляя потенциальные нарушения безопасности или подозрительные действия. Эффективно развертывая брандмауэры и идентификаторы, организации могут защитить свои серверы от попыток несанкционированного доступа и сетевых атак [3].

Регулярное внесение исправлений и обновлений: Операционные системы, серверное программное обеспечение и приложения часто выпускают исправления и обновления для устранения уязвимостей и повышения безопасности. Регулярное применение этих обновлений имеет решающее значение для минимизации риска эксплуатации со стороны киберпреступников. Организациям следует внедрить процедуры управления исправлениями, чтобы гарантировать оперативное обновление серверов последними исправлениями безопасности, снижая вероятность успешных атак.

Резервное копирование и аварийное восстановление: Защита сервера заключается не только в предотвращении несанкционированного доступа или внешних угроз. Это также включает в себя подготовку к потенциальной потере данных или системным сбоям. Регулярное резервное копирование критически важных данных и внедрение надежных планов аварийного восстановления помогают смягчить последствия сбоев серверов, стихийных бедствий или киберинцидентов. Резервные копии данных должны храниться в безопасных удаленных местах или на облачных платформах с усиленными мерами безопасности.

Мониторинг и аудит: Постоянный мониторинг активности сервера и протоколирование событий необходимы для обнаружения подозрительного поведения и потенциальных инцидентов безопасности. Системы предотвращения вторжений (IPS) и решения для управления информацией о безопасности и событиями (SIEM) могут обеспечивать мониторинг в режиме реального времени, предупреждая системных администраторов о любых аномалиях или нарушениях безопасности. Регулярные аудиты и оценки безопасности также помогают выявлять уязвимости и обеспечивать соответствие стандартам и нормативным актам безопасности.

Заключение

Защита сервера является фундаментальным аспектом поддержания безопасной и отказоустойчивой ИТ-инфраструктуры. Внедряя комплексные меры безопасности, организации могут защитить свои серверы от

несанкционированного доступа, утечки данных и системных сбоев. Контроль доступа, шифрование, брандмауэры, регулярные обновления, резервное копирование и аварийное восстановление, а также мониторинг - вот лишь несколько ключевых подходов, которые способствуют эффективной защите сервера. По мере развития цифрового ландшафта крайне важно сохранять бдительность, адаптировать систему безопасности.

Библиографический список:

1. Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2005.

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.

3. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.