Безопасность в облаке: Главные вызовы и решения

Алексей Соколов
Руководитель группы backend разработки Itransition Group

Аннотация: Настоящая статья обращается к ключевым аспектам безопасности в облаке, выделяя главные вызовы, с которыми сталкиваются организации, а также предлагая эффективные решения для их преодоления.

Ключевые слова: безопасность, облачные решения, кибербезопасность, безопасность данных, многофакторная аутентификация, шифрование данных, доступ к данным.

Облачные технологии становятся все более важным фактором в развитии бизнеса, предоставляя компаниям гибкость, масштабируемость и доступность данных. В связи с этим возникает и необходимость в обеспечении безопасного использования этих сервисов. Рассмотрим основные угрозы, с которыми сталкиваются компании и эффективные методы защиты от них.

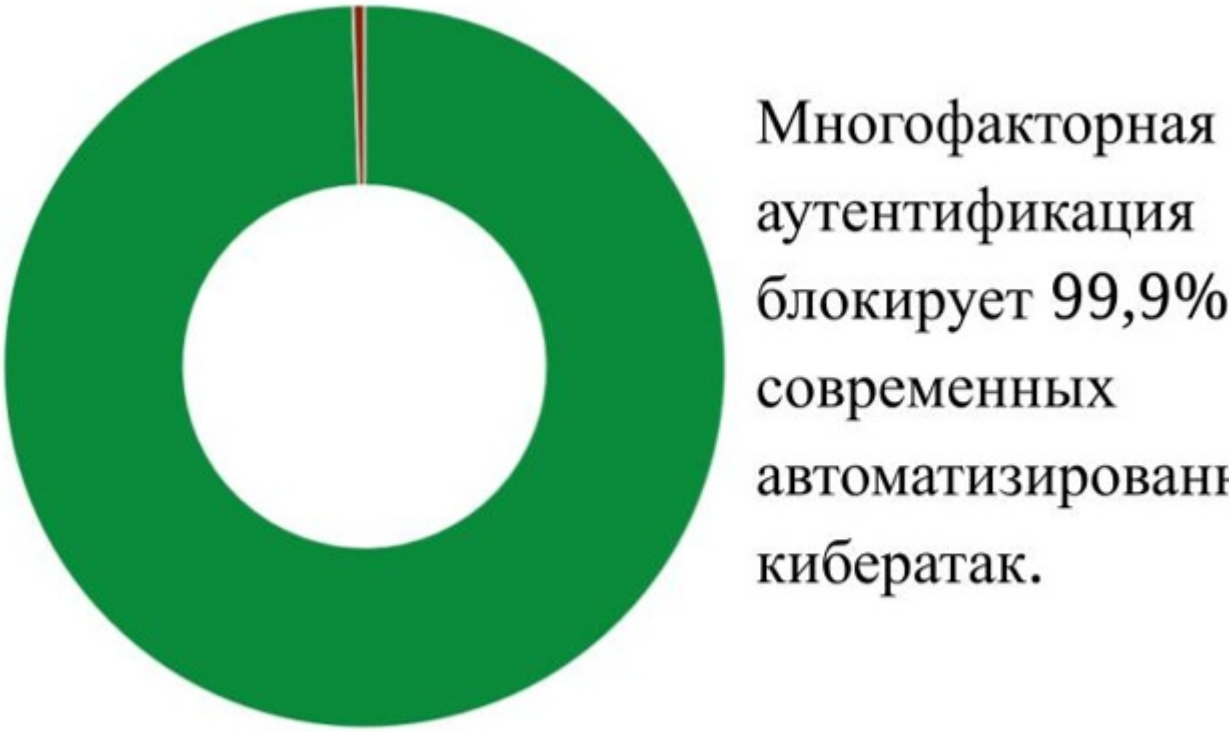
Безопасность данных

В условиях облачной среды, одним из вызовов является угроза безопасности данных. С увеличением объема информации, передаваемой и хранимой в облаке, несанкционированный доступ и потенциальные утечки становятся серьезными проблемами для организаций.

Для решения этой проблемы важно применять эффективные методы шифрования. Они предоставляют дополнительную защиту, сохраняя конфиденциальность информации и предотвращая несанкционированный доступ. Важно также проводить мониторинг и анализ безопасности, которые позволят оперативно выявлять подозрительную активность и предпринимать меры по предотвращению нежелательных инцидентов. Еще одним шагом является строгая политика менеджмента разрешений и внедрение многофакторной аутентификации. Сочетание этих методов обеспечит комплексный подход к сохранности данных в облачной среде, поддерживая надежную защиту и целостность информации.

Аутентификация и управление доступом

Аутентификация и управление доступом представляют собой двойной вызов, который требует внимания на различных уровнях. Этот вызов включает в себя не только проверку личности пользователей, но и администрирование их разрешений. В условиях динамичной облачной среды, где сотрудники могут обращаться к информации из различных мест и устройств, необходимо гарантировать, что только авторизованные пользователи могут работать с данными.



Согласно статистике, 81% нарушений, связанных со взломом происходят из-за слабых или украденных паролей. При этом многофакторная аутентификация блокирует 99,9% современных автоматизированных кибератак. В таком случае она становится стандартом в безопасности, определяя дополнительные уровни проверки для подтверждения личности. Это может быть комбинация пароля, биометрических данных или мобильных устройств для подтверждения личности. Для эффективного контроля необходимо применять системы управления правами доступа, которые позволяют точно определить, какие ресурсы и функции может использовать каждый пользователь. Все эти методы направлены на создание более устойчивых систем, способных справляться с развитием современного бизнеса в облаке.

Сетевая безопасность в облаке

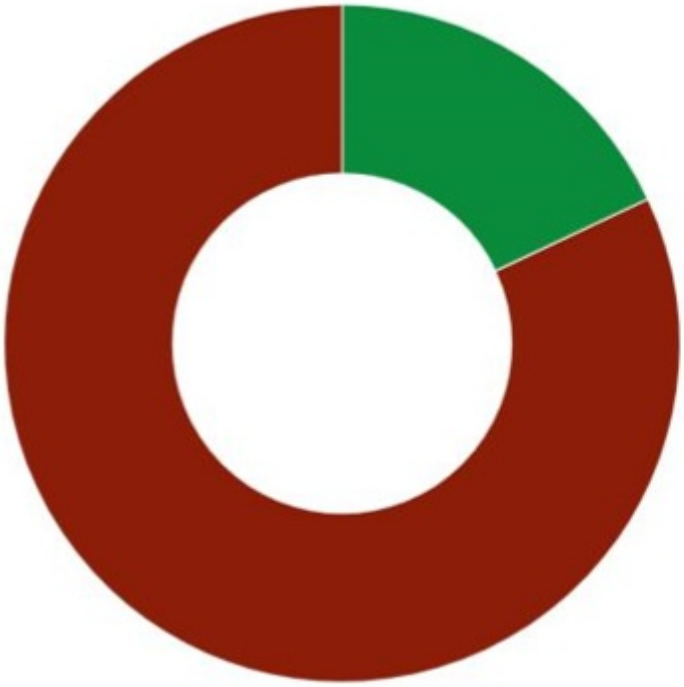
Распределенная природа облачных сервисов предъявляет особые требования к защите сети для сохранения целостности и конфиденциальности данных и поддержанию уровня кибербезопасности. Обеспечение сетевой безопасности в облаке начинается с разработки эффективных мер защиты которые позволят контролировать и фильтровать трафик, предотвращая несанкционированный доступ и атаки.

По исследованию Verizon, порядка 60% кибератак были обнаружены в течение нескольких дней, однако для 20% прошли месяцы, прежде чем компании поняли, что что-то не так. Именно поэтому необходимы системы обнаружения вторжений, которые мониторят сетевой трафик и выявляют подозрительную активность. Это позволит оперативно реагировать на угрозы и предотвращать возможные атаки до того, как они нанесут ущерб. Важными элементами защиты также являются обеспечение целостности сетевой инфраструктуры, шифрование данных и контроль над доступом к облачным ресурсам. Все эти меры, интегрированные в общую стратегию безопасности, создают надежное и устойчивое окружение, где сетевая инфраструктура остается защищенной от разнообразных угроз.

Управление идентификацией

Сотрудники, получая доступ к ресурсам с различных устройств, увеличивают риски несанкционированного проникновения. Внедрение единой системы управления идентификацией

облегчает администрирование и изменение организационной структуры.



По отчету Verizone о расследованиях утечек данных за 2022 год, 82% нарушений связано с человеческим фактором.

Системы аудита и мониторинга отслеживают действия пользователей, предостерегают от потенциальных угроз и оперативно реагируют на аномалии. Дополнительно усиливает защиту многофакторная аутентификация. Однако безопасность также требует и осведомленности сотрудников. По отчету Verizone о расследованиях утечек данных за 2022 год, 82% нарушений связано с человеческим фактором. Проведение регулярного обучения создает внутреннюю культуру, где сотрудники сами участвуют в поддержании защищенной среды. Все эти стратегии обеспечивают комплексный подход к управлению идентификацией, гарантируя надежную защиту от угроз, связанных с несанкционированным доступом в облачном окружении.

Контроль целостности данных

Обеспечение целостности данных предотвращает изменения, которые могут повлиять на достоверность и неизменность хранимой информации. С учетом распределенной природы облачных сервисов и возможности множества пользователей одновременно взаимодействовать с файлами, необходимо внедрение технологий, гарантирующих их сохранность.

Эффективные методы контроля целостности включают в себя применение цифровых подписей и хэш-функций, которые позволяют подтверждать авторство и создавать уникальные метки для каждого блока данных. Это дает возможность быстро обнаружить любые изменения. Параллельно с этим необходимо проводить регулярное аудирование и проверку на соответствие ожидаемым значениям. Дополнительное использование технологии блокчейн поможет создавать неизменяемый журнал всех транзакций и изменений. В совокупности эти подходы образуют комплексный механизм поддержания целостности информации в облачной среде.

Обеспечение непрерывности бизнес-процессов

В условиях распределения бизнес-приложений и данных по различным серверам и регионам, возможны различные сбои оборудования, отказы в работе сети и кибератаки, которые могут существенно повлиять на доступность сервисов. Разработка и внедрение стратегий резервного копирования дает возможность создавать дубликаты информационной базы. Они могут быть применены в случае сбоя или утраты данных, поддерживая таким образом бесперебойность бизнес-процессов.

Дополнительным средством обеспечения стабильности является мониторинг и реагирование на события в режиме реального времени и использование механизмов восстановления после сбоев. Такой комплексный подход к поддержанию безостановочной работы позволяет предугадывать, вовремя реагировать и восстанавливаться после сбоев, сохраняя стабильную работу приложений и целостность данных.

Соответствие стандартам и нормативным документам

Бизнес в условиях облачной среды должен строго соблюдать законодательство и отраслевые стандарты, чтобы избежать юридических последствий и поддерживать доверие клиентов. Одним из основных методов сохранения безопасности данных, согласно требованиям, является шифрование, которое обеспечивает конфиденциальность информации. Важной частью соответствия стандартам стали многофакторная аутентификация, мониторинг и анализ защищенности.

Автоматизация процессов позволит более эффективно соблюдать требования регулирований. Такие системы контролируют соблюдение политики защиты информации, быстро реагируют на нарушения и снижают риск человеческого фактора. Эти методы поддерживают соблюдение нормативных стандартов и требований, формируя надежный и соответствующий законодательной базе фундамент для работы в облаке.

Заключение

Обеспечение безопасности в облачной среде представляет собой сложную и стратегически важную задачу для современных организаций. Развитие технологий и все более активное использование современных сервисов подчеркивают необходимость постоянного совершенствования стратегий защиты. Успешное преодоление вызовов содействует стабильному и надежному функционированию бизнеса, а постоянное обновление стратегий безопасности и внимание к инновационным технологиям становятся необходимостью в быстро развивающемся цифровом мире.

Источники:

17 Essential Multi-Factor Authentication (MFA) Statistics [2023], Zippia (https://zippia.com)

Data Breach Investigations Report 2022, Verizon (https://verizon.com)

Что такое безопасность облака?, Kaspersky (https://kaspersky.ru)