УДК 004.08

МЕТОДИКИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ХРАНИЛИЩ ДАННЫХ

А. А. Леонов
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Рассмотрены методики обеспечения безопасности облачных хранилищ данных. Отмечена роль в этом процессе провайдеров и пользователей. Обоснована целесообразность регулярного анализа облачных конфигураций. Такой подход гарантирует, что случайных изменений не произошло или они безвредны. Это также помогает определить небезопасные конфигурации, повысить производительность и исключить затраты на ненужные облачные ресурсы.

Ключевые слова: безопасность, облачные хранилища данных, анализ безопасности объектов, методики обеспечения безопасности.

CLOUD STORAGE SECURITY METHODS

A. A. Leonov
Don State Technical University (Rostov-on-Don, Russian Federation)

The article discusses methods for securing cloud storage. The role of providers and users in this process is noted. The expediency of regular analysis of cloud configurations is justified. This approach ensures that no accidental changes have occurred or that they are harmless. It also helps you identify insecure configurations, improve performance, and eliminate the cost of unnecessary cloud resources.

Keywords: security, cloud data storage, object security analysis, security methods.

Введение. Безопасность облака — это раздел кибербезопасности, посвященный защите облачных вычислительных систем. Речь идет о защите конфиденциальности данных во всех объектах сетевой инфраструктуры, онлайн-приложениях и платформах. Адекватность защиты обеспечивают как поставщики облачных услуг, так и пользователи — частные и юридические лица.

Облачные службы размещаются на серверах с постоянным подключением к интернету. Хранящиеся в облаке личные данные должны быть надежно защищены от несанкционированного доступа. Это задача провайдера. Тем не менее, облачная безопасность отчасти находится в руках пользователей. Для надежной защиты важно, чтобы обе стороны понимали свою ответственность.

Безопасность облака подразумевает:

— безопасность данных,

— управление идентификацией и доступом,

— административный контроль (предотвращение, обнаружение и устранение угроз),

— планирование хранения данных и обеспечения непрерывности бизнеса,

— соблюдение нормативно-правовых требований.

Следуя этим рекомендациям, можно повысить безопасность критически важных (например, для бизнеса) облачных систем.

Основная часть. В первую очередь рассмотрим вопросы обеспечения достоверности и видимости данных. Облачные среды характеризуются множеством движущихся частей, включая недолговечные облачные экземпляры и контейнеры, «эластичные» тома данных, кластерные активы (например, хранилища данных) и бессерверные функции.

Стоит использовать автоматизированный метод для составления реестра всех текущих и исторических облачных активов, чтобы предотвратить хаотический рост и контролировать поверхность атаки. Невозможно защитить невидимые активы. Таким образом, создание периметра безопасности базируется на обеспечении оперативного и качественного отслеживания:

— активов, которыми владеет компания;

— учетных записей пользователей, которым доступны активы;

— событий, происходящих с каждым активом.

Резервное копирование и восстановление. Данные быстро перемещаются в облаке. Системы прочно связаны, поэтому одна ошибка или вредоносная команда могут удалить большие объемы или целые тома данных. Взломанная учетная запись может стать причиной катастрофического ущерба.

В облаке программы-вымогатели распространяются быстрее и наносят больший ущерб, чем в локальных системах (последние более изолированы и имеют четкие границы безопасности).

Для предотвращения потери данных целесообразны:

— облачное резервное копирование для защиты копий данных;

— архивирование (идеально подходит для больших объемов данных, которые не должны использоваться часто, а также могут быть выделены из производственных рабочих мощностей);

— настройка автоматического аварийного восстановления, обеспечивающая мобильность всей среды для быстрого восстановления после утечки данных.

Своевременное обновление. Для успеха стоит убедиться, что облачные системы не обладают уязвимостями, связанными с необходимостью обновлений или исправлений. Это особенно важно, если известны и не устранены какие-то уязвимости. В этом случае злоумышленник точно знает, как использовать слабые места системы.

В некоторых системах достаточно принять обновления. В других случаях для устранения уязвимости придется создать собственный патч. Также с помощью автоматизированных инструментов стоит постоянно проверять, все ли программные системы работают с последней версией.

Кроме того, нужно использовать платформы анализа угроз или данные из открытых источников (например, из баз данных уязвимостей), чтобы не пропустить объявления об уязвимостях. Это позволяет защитить систему, как только будет объявлено об уязвимости, даже если исправление пока недоступно.

Аудит и оптимизация конфигураций. При настройке приложения и инфраструктуры не стоит исходить из того, что систему настроили правильно. Возможны ошибки конфигурации. Даже если их нет, конфигурация может измениться по мере обновления приложений и облачных ресурсов, а также при изменении рабочих процессов или пользователей.

Регулярный анализ облачных конфигураций гарантирует отслеживание изменений и определение их безопасности. Это также помогает выявить менее безопасные конфигурации, повысить производительность и исключить затраты на ненужные облачные ресурсы. С этой целью можно задействовать различные инструменты и процессы, включая автоматические сканеры, тестирование на проникновение и ручные аудиты. Все основные облачные сервисы предлагают ту или иную форму анализа конфигурации. Новая категория инструментов называется «управление состоянием безопасности в облаке» (Cloud Security Posture Management, CSPM). Она обеспечивает комплексное тестирование и анализ уязвимостей безопасности в облачном стеке, включая проблемы конфигурации.

Выводы. Хранящиеся в облаке личные данные должны быть надежно защищены от несанкционированного доступа. Эффективное решение этой задачи предполагает совместные усилия провайдера и пользователя. Последнему для защиты облачных данных необходимо настроить автоматическое аварийное восстановление, регулярно выполнять резервное копирование, архивирование. Следует также своевременно проводить обновления, нацеленные на устранение уязвимостей, анализировать угрозы, проверять и оптимизировать конфигурации.

Библиографический список

1. Что такое безопасность облака // Kaspersky : [сайт]. — URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security (дата обращения: 15.02.2021).

2. Архипенков, С. Хранилища данных. От концепции до внедрения / С. Архипенков, Д. Голубев, О. Максименко. — Москва : Диалог-МИФИ. — Москва, 2008. — 528 с.

3. Забелин, И. Подземные хранилища московского Кремля / И. Забелин. — Москва : Книга по требованию, 2011. — 797 с.

Об авторе:

Леонов Алексей Александрович, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), leon777alexei@yandex.ru.

Author

Leonov, Aleksey A., Student, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), leon777alexei@yandex.ru.