УДК 004.08

ПРОБЛЕМЫ ОБЛАЧНОЙ БЕЗОПАСНОСТИ

С. Р. Токова
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Рассмотрены вопросы безопасности облачных хранилищ. Проанализированы проблемы, которые затрудняют защиту облачных систем по сравнению с традиционным периметром безопасности, к ним относятся управление доступом, нарушения соответствия, отказ в обслуживании (DoS / DDoS-атаки), небезопасные API.

***Ключевые слова*:** безопасность, облачные вычисления, хранилища данных, анализ безопасности объектов, информационная безопасность.

CLOUD SECURITY ISSUES

S. R. Tokova
Don State Technical University (Rostov-on-Don, Russian Federation)

The paper considers the issues of cloud storage security. The problems that make it difficult to protect cloud systems compared to the traditional security perimeter are analyzed, including access control, compliance violations, denial of service (DoS / DDoS attacks), and insecure APIs.

Keywords: security, cloud computing, data warehouses, security analysis of objects, information security.

Введение. В последнее время все больше компаний предпочитают облака. Во многом причиной стала пандемия COVID-19, которая вынудила значительное количество людей перейти на удаленную работу. Это привело к повышению спроса на доступ к корпоративным ресурсам из любого места. Многие компании за два месяца сделали то, что планировали сделать за пять лет.

В частности, исследование 2020 года показало, что 87% компаний планируют ускорить миграцию в облако после окончания пандемии. 68% компаний используют решения двух и более поставщиков облачных услуг. Но такой резкий рывок вперед дорого обошелся многим организациям.

Исследование Check Point 2020 Cloud Security Report показало, что ускоренный переход к облакам создал огромное количество брешей в безопасности организаций, что привело к увеличению числа атак и растущему беспокойству компаний [1].

Приведены некоторые из основных проблем, которые затрудняют защиту облачных систем по сравнению с традиционным периметром безопасности:

— управление доступом;
— нарушения соответствия;
— отказ в обслуживании (DoS / DDoS-атаки);
— небезопасные API.

Основная часть. Управление доступом. Облако обеспечивает доступ к корпоративным данным из любого места, поэтому компаниям необходимо убедиться, что неавторизованные стороны не могут получить к ним доступ. Этого можно достичь с помощью различных стратегий, включая облачные решения для предотвращения потери данных (DLP), мониторинг, а также бережное использование и обслуживание систем управления идентификацией и доступом (IAM).

Нарушения соответствия. Поскольку регулирующий контроль во всем мире становится более строгим, организации должны соблюдать многочисленные стандарты соответствия. Переходя в облако, можно нарушить обязательства по соблюдению нормативных требований.

Большинство нормативных требований и стандартов соответствия требуют, чтобы компании знали, где находятся данные, кто имеет к ним доступ, а также как ими управляют и как они обрабатываются, что может быть сложной задачей в облачной среде. Другие правила требуют, чтобы поставщики облачных услуг были сертифицированы по стандарту соответствия.

Отказ в обслуживании (DoS / DDoS-атаки). Распределенные атаки типа «отказ в обслуживании» (DDoS) предназначены для потоковой передачи больших объемов трафика на веб-сервер или другую важную систему, не позволяя ей отвечать на законные запросы.

Облачные вычисления основаны на общих распределенных вычислительных ресурсах и используют различные типы технологий виртуализации, что делает DDoS более сложным и трудным для обнаружения и предотвращения.

Например, новые типы DDoS-атак подавляют ресурсы виртуализации, такие как гипервизоры, осуществляют захват систем управления виртуализацией для создания новых скомпрометированных виртуальных машин и компрометацию систем миграции и резервного копирования для получения ненужных копий производственных систем.

Небезопасные API. Пользовательские интерфейсы прикладных программ (API) являются наиболее распространенным способом работы и интеграции облачных систем.

API-интерфейсы могут использоваться сотрудниками внутри компании, а клиентами — за ее пределами, через мобильные или веб-приложения. API-интерфейсы могут предоставлять множество типов данных, включая конфиденциальные, которые имеют ценность для злоумышленников. Поскольку API-интерфейсы общедоступны и их внутренняя работа хорошо документирована, они являются основной целью для злоумышленников [2].

Выводы. Традиционные инструменты не подходят для динамической, виртуальной и децентрализованной природы облака. Они не смогут обрабатывать растущее число взломов. Для решения этих проблем требуется унифицированное, высокоавтоматизированное и экономичное решение облачной безопасности, которое способно обнаруживать и обрабатывать угрозы в многооблачных средах [1].

Библиографический список

1.Основные проблемы облачной безопасности в 2020 году // It world : [сайт]. — URL: https://www.it-world.ru/cionews/security/157160.html (дата обращения: 18.02.2021).

2. Архипенков, С. Я. Хранилища данных. От концепции до внедрения / С. Я. Архипенков, Д. Голубев, О. Максименко. — Москва : Диалог-МИФИ, 2006. — 528 с.

Об авторе:

Токова Снежана Руслановна, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), snezhanatokova@yandex.ru

Author:

Tokova, Snezhana R., Student, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), snezhanatokova@yandex.ru