УДК 004.08

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ХРАНИЛИЩ

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

Рассмотрены вопросы безопасности облачных хранилищ. Цель данной работы — провести исследование того, как сервис-провайдер обеспечивает сохранность хранимых данных и данных при передаче, как определяет подлинность клиента. Автором проведен теоретический анализ на тему будущего облачной безопасности. Представлена сводка по исследованию безопасности облачных сервисов. Приведены примеры нарушений безопасности, исходящих от облачных сервисов, которые иллюстрируют степень уязвимости облачных систем.

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

CLOUD STORAGE SECURITY

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

The article discusses the issues of cloud storage security. The purpose of this work is to conduct a study of how the service provider ensures the safety of stored data and data during transmission, how it determines the client authenticity. The author conducted a theoretical analysis on the future of cloud security. A summary of the cloud services security study is presented. The examples of security breaches originating from cloud services are given, which illustrate the degree of vulnerability of cloud systems.

Keywords: security, cloud computing, data warehouses, object security analysis.

Введение. Безопасность облачных вычислений — это набор технологий и стратегий, которые могут помочь организации защитить облачные данные, приложения и инфраструктуру, а также соответствовать стандартам и нормам [1].

Управление идентификацией, конфиденциальность и контроль доступа особенно важны для облачной безопасности, поскольку облачные системы обычно являются общими и доступными в интернет-ресурсах. Поскольку все больше и больше организаций используют облачные вычисления и поставщиков общедоступных облаков для своей повседневной работы, они должны уделять приоритетное внимание соответствующим мерам безопасности и устранению уязвимых мест [1].

Процессы безопасности облачных вычислений должны учитывать меры безопасности, предлагаемые поставщиками облачных услуг, и организации обязаны понимать разделение ответственности между поставщиком облачных услуг и пользователем облака. Чтобы подготовиться к возможному нарушению безопасности облака, необходимо стандартизировать процессы для обеспечения непрерывности бизнеса и резервного копирования данных облачных систем.

Основная часть. Поводом для внедрения безопасных облачных методов является растущая угроза со стороны киберпреступников, нацеленных на облако. Отчет ISC по облачной безопасности показал, что 28% предприятий сталкивались с инцидентами, связанными с облачной безопасностью. Правовые источники сообщают также, что 32% компаний испытали атаки на облачные системы.

Отчет Check Point 2020 Cloud Security Report содержит дополнительные выводы:

— самая большая угроза, которую назвали респонденты, это ошибка конфигурации облачной платформы (68%), за которой следуют несанкционированный доступ к облаку (58%), незащищенные интерфейсы (52%) и кража учетной записи (50%);

— 55% респондентов заявили, что нехватка квалифицированных специалистов, в том числе специалистов в области безопасности, является самым большим препятствием для внедрения облачных технологий;

— 82% пользователей считают, что существующие решения безопасности вообще не работают или предлагают ограниченную функциональность в облачной среде.

Чтобы понять, как происходят нарушения безопасности, необходимо проанализировать примеры нарушений из реальной жизни. Вот три недавних примера нарушений безопасности, исходящих от облачных сервисов, которые иллюстрируют серьезную уязвимостей облачных систем.

Capital One — 10-й по величине банк США по размеру активов. Его облачная инфраструктура была основана на Amazon Web Services (AWS).

Следующие события привели к публичной утечке в Capital One. Во-первых, брандмауэр веб-приложений был настроен неправильно. Злоумышленник использовал неправильные настройки для создания токена доступа и использовал его для извлечения данных из хранилища AWS. 700 папок и пакетов данных, содержащих информацию о клиентах, были скопированы во внешнее хранилище.

Злоумышленники знали о специальных командах AWS и использовали их для выполнения бокового движения после получения доступа. Более того, нарушение не вызвало никаких предупреждений, и даже передача данных за пределы сети организации осуществлялась под видом обычного сетевого трафика.

Docker Hub. Docker Hub, популярный репозиторий образов контейнеров, был скомпрометирован тем, что было обнаружено 190 000 учетных записей, это нанесло ущерб приверженцам контейнерных технологий. В заявлении, размещенном на веб-сайте Docker, компания сообщила об обнаружении несанкционированного доступа к единой центральной базе данных, в которой хранятся нефинансовые данные пользователей.

Хотя эта уязвимость затронула только 5% клиентов, представленные данные включали токены и ключи доступа, используемые в функциях автоматической сборки репозиториев кода. Это дает возможность злоумышленникам обходить аутентификацию и внедрять вредоносный код в производственные конвейеры многих компаний, а также получать копии проприетарного кода.

Autoclerk, глобальная система управления бронированием отелей, располагала базой данных Elasticsearch на AWS, которая была незащищенной и открывала доступ к сотням тысяч бронирований. Система активно использовалась военнослужащими, и в результате взлома была раскрыта конфиденциальная информация о поездках военных, в том числе высших должностных лиц, и развернутых войсках.

Исследователи безопасности из vpnMentor опубликовали информацию о взломе, заявив, что они видели общедоступные журналы поездок американских генералов в Москву, Тель-Авив и многие другие страны. Они также обнаружили адреса электронной почты, номера телефонов и другие конфиденциальные личные данные путешественников.

Выводы. Облачные технологии дают возможность взаимодействовать и вести совместную работу с непрерывно расширяющимся кругом пользователей независимо от их местоположения. Данные технологии доставляют информацию наиболее экономичным и надежным способом, отличаются простотой распространения и обновления. Именно облачные технологии позволят информации преодолеть существующие барьеры: географические, технологические, социальные.

Внедрение облачных технологий не только снижает затраты на приобретение необходимого программного обеспечения, повышает качество и эффективность производственного процесса, но и делает выше уровень открытости информации. Необходимо учитывать данную информацию и добавлять системы защиты для облачных хранилищ.

Библиографический список

1. Архипенков, С. Хранилища данных. От концепции до внедрения / С. Архипенков, Д. Голубев, О. Максименко // Москва : Диалог-МИФИ, 2002. — 528 с.

Об авторе:

Аверкиев Александр Александрович, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), averckiev.alex@yandex.ru

Author:

Averkiev, Aleksandr A., Student, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), averckiev.alex@yandex.ru