DOI 10.37882/2223-2966.2024.01.10

АНАЛИЗ СТРУКТУРЫ СИСТЕМЫ ЗАЩИТЫ ОБЛАЧНОГО ЦЕНТРА ОБРАБОТКИ ДАННЫХ (ЦОД)

ANALYSIS OF THE PROTECTION SYSTEM STRUCTURE CLOUD DATA CENTER (DPC)

V. Burygin

Summary. The article discusses the analysis of the structure of the cloud Data Processing Center (DPC) security system. It is noted that the active use of cloud technologies today is becoming an advantage for enterprises of all sizes — from small companies to large corporations and even public sector organizations. The development of the high relevance of issues of ensuring the protection of data transmitted through open data transmission channels is substantiated. It is noted that protecting data in the cloud is the responsibility of any cloud provider, since this directly affects its competitiveness, image and reputation. It has been revealed that the problem of protecting data and equipment in the cloud is a source of controversy when considering the use of cloud resources. It is noted that ensuring information security of cloud data centers is implemented using complex multi-level protection systems. It is concluded that the structure of the cloud data center protection system is to a certain extent similar to the protection systems of a large corporation and its implementation requires the use of several levels of protection, the inclusion of organizational, software and hardware protection tools with the only difference that greater emphasis is placed on to protect network connections and transmitted data.

Keywords: cloud technologies, information security, cloud security, data center, cloud services.

Бурыгин Вячеслав Михайлович
Аспирант, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича;
программист-разработчик, ООО «ВК»
slashburygin@gmail.com

Аннотация. В статье рассматривается анализ структуры системы защиты облачного Центра обработки данных (ЦОД). Отмечено, что активное использование облачных технологий сегодня становится преимуществом предприятий самого разного масштаба — от небольших компаний до крупных корпораций и даже организаций государственного сектора. Обосновано развитие высокой актуальности вопросов обеспечения защиты данных, передаваемых посредством открытых каналов передачи данных. Отмечено, что защита данных в облаке представляет собой обязанность любого облачного провайдера, поскольку это прямым образом влияет на его конкурентоспособность, имидж и репутацию. Выявлено, что проблема защиты данных и оборудования в облаке является источником противоречий при рассмотрении вопросов использования облачных ресурсов. Отмечено, что обеспечение информационной безопасности облачных центров обработки данных реализуется с использованием сложных многоуровневых систем защиты. Сделан вывод о том, что система защиты облачного ЦОД по структуре в определенной степени схожа с системами защиты крупной корпорации и для её реализации требуют применять несколько уровней защиты, включать в состав организационные, программные и аппаратные средства защиты с той лишь разницей, что больший упор делает на защиту сетевых подключений и передаваемых данных.

Ключевые слова: облачные технологии, защита информации, защита облака, центр обработки данных, облачные сервисы.

Развитие облачных технологий сегодня происходит стремительно, что обусловлено огромными возможностями и конкурентными преимуществами, которое облако предоставляет своему потребителю. Любая организация в первую очередь получает финансовую выгоду, связанную с меньшими затратами на оборудование и его обслуживание, экономию времени и ресурсов. Для этого достаточно иметь скоростной канал доступа к сети Интернет. Однако для обрабатываемых данных требуется высокий уровень защиты, поскольку безопасность обрабатываемых данных является обязательным требованием для любой программной среды, при этом облако не является исключением [5].

Надежность и качество функционирования облачных систем зависят от большого числа различных условий, для обеспечения которых используются разные элементы:

— система энергоснабжения обеспечивает весь ЦОД электричеством: для обеспечения бесперебойного электроснабжения используют несколько вводов, а также реализуют резервную систему энергоснабжения, которая будет обеспечивать бесперебойной работы облачного ЦОД в случае перебоев на основных линиях подачи электричества;
— система охлаждения и кондиционирования воздуха следит за температурой в помещениях и обеспечивает оптимальную рабочую температуру для оборудования;
— система обеспечения безопасности обеспечивает сохранность данных, программного и аппаратного обеспечения ЦОД посредством функционирования целого ряда входящих в её состав подсистем — пожаротушения, защиты от физического проникновения, обеспечения защиты каналов передачи данных, приложений и подобных;
— каналы связи выполняют роль инструмента взаимодействия между клиентами и облачным ЦОД:

с целью обеспечения бесперебойной работы подключение ЦОД к сетям передачи данных выполняется с использованием нескольких линий связи;
— система диспетчеризации позволяет осуществлять контроль за всеми перечисленными компонентами, предоставляя оперативные оповещения по всем происходящим событиям [8].

С начала зарождения облачных технологий возникали вопросы касаемо их безопасности, поскольку фактически в одном месте собраны огромные массивы данных, передача которых при этом происходит посредством открытых сетей. Обеспечение защиты данных в облаке происходит с использованием сложной системы, представляющей собой целый набор технологий, протоколов и инструментов. При этом осуществляется не только защита данных, но и облачных сред, приложений и операционных систем. Обеспечение корректной работы системы защиты является обязанностью провайдера облачных услуг, который должен обеспечить реализацию защитных мероприятий с целью обеспечения безопасной работы таких компонентов ЦОД, как:
— физические устройства и сети — сюда относится сетевое оборудование, кабели электропитания и сетей передачи данных, системы вентиляции и кондиционирования и т.д.;
— носители данных — жесткие диски, которые используются в вычислительных платформах, либо на внешних носителях для хранения резервных копий;
— серверы — аппаратное и программное обеспечение во внутренней сети ЦОД-а;
— сети виртуализации — это программное обеспечение, установленное на виртуальные машины;
— операционные системы — программное обеспечение, реализующее взаимосвязь между аппаратным обеспечением вычислительной платформы и остальным ПО;
— среды выполнения — программное обеспечение, применяемое для обеспечения работоспособности и запуска ПО;
— данные — информация, хранимая в облаке, и предоставляемая пользователям по запросу;
— оборудование пользователей — это устройства, посредством которых пользователь выполняет работу с облаком. Сюда можно отнести персональные компьютеры и ноутбуки, планшетные компьютеры, смартфоны и т.д.[4]

Реализация систем защиты облачного ЦОД обладает некоторыми отличиями, связанными с тем фактом, что базовые рекомендации по обеспечению защиты опирались на реализацию локального хранения данных, с их передачей посредством локальной сети, принадлежащей организации. В данной ситуации владельцы данных в полной мере могут контролировать все операции по их обработке, а также пути, которые они проходят. В случае работы с облаком пользователи лишены такой возможности, вся ответственность практически в полной мере возложена на провайдера облачного ЦОД. Пользователи в определенной степени могут обеспечить безопасность отправляемых данных, однако вся дальнейшая их судьба всецело будет зависеть от системы защиты облака. Помимо этого, сложность обеспечения защиты облака состоит в том, что происходит взаимодействие различных служб, сервисов и систем. Для каждого элемента необходимо обеспечить свою защиту, независимо от его функционального назначения. То есть важно выполнять реализацию механизмов защиты для множества разрозненных элементов, обеспечивая при этой управление правами доступа на всех уровнях, что обеспечивает проверку информации, её контроль, а также проверку всех подключений [9].

Структура любого облачного ЦОД содержит такие элементы, как гипервизор, оборудование центра, каналы связи, а также программное обеспечение, функционирующее как на стороне сервера, так и на стороне пользователя. Любой элемент в составе данного перечня может быть подвержен атаке либо воздействию вредоносного программного обеспечения. Именно по данной причине при реализации систем защиты данных в облаке используется целый набор различных методик с целью реализации структурных компоненты системы защиты. К данным методиками относят:
— шифрование данных;
— использование паролей с высоким уровнем сложности в совокупности с двухфакторной аутентификацией;
— обязательное использование SSL;
— использование инструментов мониторинга сетевых подключений;
— реализация мероприятий по обеспечению безопасности API и защите от DDoS атак [10].

Рассмотрим перечисленные методы реализации компонентов системы защиты облака более подробно.

Шифрование считается одним из важных элементов в составе системы защиты облачной инфраструктуры. Это связано с его непосредственным функционалом — оно позволяет посредством специальных алгоритмов выполнить преобразование передаваемых сведений в нечитаемую форму, что делает их перехват нецелесообразным для злоумышленника. После получения зашифрованных данных их необходимо преобразовать обратно с использованием ключа шифрования. Подобрать ключ злоумышленники могут лишь с использованием очень мощного оборудования, и при значительных временных затратах, что делает процесс взлома ключа шифрования бессмысленным. Процедура шифрования при работе с облаком происходит на каждом этапе рабо-

ты с данными — при их передаче между облаком и клиентом, а также при их хранении.

Следующий обязательный элемент системы защиты — система авторизации пользователей, основанная на использовании надежных паролей, а также возможности использования многофакторной авторизации. Использование для авторизации пароля с высоким уровнем надежности минимизирует вероятность подбора его злоумышленниками, а подключение многофакторной авторизации делает данную процедуру максимально безопасной. Реализация подобной процедуры выполняется с использованием различных методик, таких как одноразовые пароле, биометрические схемы или аппаратные токены. В любом случае она позволяет устранить вероятность взлома системы авторизации. Помимо шифрования и многофакторной авторизации в рамках системы защиты данных в облаке используют протокол безопасной передачи данных SSL, в котором детально прописываются обязательства со стороны провайдера в области обеспечения защиты данных пользователей.

Перечисленные элементы системы защиты относятся к внешним инструментам обеспечения защиты. Защита облачных сервисов изнутри реализуется такими компонентами, как система мониторинга сетевой активности, система защиты от атак, а также реализация механизмов надежности API приложений.

Первый из компонентов внутренней защиты — система мониторинга сетевой активности. Она отслеживает любое аномальное поведение, будь то попытка получения доступа через порт, аномальное поведение сетевых сервисов, сканирование системы на уязвимости и т.д. В случае выявления подобных отклонений система может реализовать несколько сценариев. Самый простой — блокировка аномалии и оповещение администраторов системы. Более совершенные системы способны реализовать закрытые виртуальные контейнеры, в которые переадресуют возникшую угрозу, одновременно выполняя процедуру установления источника угрозы.

Следующий компонент системы защиты — подсистема защиты от сетевых атак может быть реализована отдельно либо в составе системы мониторинга сети. В любом случае, данная подсистема реализует механизмы противодействия сетевым атакам с целью устранения атак типа «отказы в обслуживании», так как они являются наиболее распространенными сетевыми атаками на облачную инфраструктуру. К таким механизмам относятся инструменты проверки трафика, межсетевые экраны, сетевые анализаторы. Кроме того, внутренняя защита реализуется посредством обеспечения процедур надежности и безопасности API, выполняемой по нескольким направлениям. Например, проводится тестирование на проникновение с имитацией атаки на программное обеспечение, с целью выявления уязвимостей в коде. Кроме того, реализуются дополнительные инструменты шифрования и многофакторной авторизации.

Еще одним из инструментов безопасности является защита приложений и сервисов за счет использование проверенных инструментов и библиотек, а также защиту сред. Речь идет об использовании принципов сегментации и изоляции, согласно которым запуск каждого приложения выполняется в собственной изолированной среде. Для обеспечения безопасности приложений должно выполняться их тестирование и проверка на предмет наличия уязвимостей, с последующим выпуском новых версий, устраняющих проблемы в системе защиты данных приложений.

Рассмотрим набор инструментов, участвующих в рамках и внутренней, и внешней защиты. Прежде всего, это специализированные протоколы [3], такие как:

- SSL/TLS — специализированный криптографический протокол, формирующий защищенное соединение и осуществляющий процедуру шифрования данных «на лету», то есть данные шифруются на стороне того устройства, которое будет выполнять их передачу, и в зашифрованном виде передаются другому устройству посредством открытых каналов связи;
- IPsec — специализированный протокол, позволяющий выполнить процедуры шифрования данных и аутентификации пользователей на уровне IP. Используется широко в веб-сервисах и приложениях, в том числе и в облачной инфраструктуре;
- SSH — прокол удаленного подключения, а также передачи данных между двумя устройствами в сети. В рамках работы с облаком чаще всего используется для организации удаленной работы и обслуживания серных платформ;
- OAuth — протокол доступа к приложениям или сервисам, не требующий передачи учетных данных, что позволяет реализовать процедуры контроля доступа к данным с защитой их от несанкционированного доступа;
- SAML — протокол, выполняющий процессы обмена специализированными утверждениями о безопасности между сервисами идентификации пользователей и непосредственно облачными сервисами. Чаще всего используется для обеспечения единой процедуры входа для пользователей в рамках набора облачных сервисов;
- AES — протокол шифрования данных, хранимых в состоянии покоя.

Перечисленный состав протоколов может комбинироваться провайдером облачных услуг на свое усмотрение, но в большинстве случаев происходит их одновре-

менное использование, так как это позволит обеспечить максимально возможный уровень защиты в рамках процедур взаимодействия клиента с облаком.

Наиболее эффективным вариантом обеспечения защиты облачной инфраструктуры считается реализация системы защиты, состоящей из нескольких независимых уровней. Первый уровень — обеспечение физической защиты инфраструктуры и оборудования от негативных условий функционирования, либо получения к ним несанкционированного доступа. Следующий уровень — обеспечение инфраструктурной безопасности посредством использования сетевых брандмауэров, систем анализа трафика, выявления вторжений и т.д. Далее отдельными уровнями идут процессы управления правами доступа пользователей и механизмами авторизации, а также набор методов, связанных с шифрованием потоков данных. Последние слои системы защиты — это слой мониторинга и анализа аномального поведения в инфраструктуре, а также управление рисками и соблюдение требований по их устранению.

Таким образом, что система защиты облачного ЦОД по структуре в определенной степени схожа с системами защиты крупной корпорации — для её реализации требуют применять несколько уровней защиты, включать в состав организационные, программные и аппаратные средства защиты с той лишь разницей, что больший упор делает на защиту сетевых подключений и передаваемых данных.

ЛИТЕРАТУРА

1. Аникина Н.А., Фёдорова Т.И. Внешние и внутренние угрозы информационной безопасности // Ростовский научный вестник. 2022. №11. С. 73–78.
2. Белянская О.В., Привалов А.Н. О модели угроз информационной безопасности в центрах обработки данных // Известия ТулГУ. Технические науки. 2021. №9. С. 12–16.
3. Вишняков А.С., Макаров А.Е., Уткин А.В., Зажогин С.Д., Бобров А.В. Обеспечение защиты данных, представленных в облачных сервисах // Вестник науки и образования. 2019. №11-2 (65). С. 68–73.
4. Диченко С.А., Самойленко Д.В., Финько О.А. Особенности обеспечения безопасности информации в условиях угроз, связанных с неконтролируемым предоставлением услуг по хранению данных // I-methods. 2021. №4. URL: https://cyberleninka.ru/article/n/osobennosti-obespecheniya-bezopasnosti-informatsii-v-usloviyah-ugroz-svyazannyh-s-nekontroliruemym-predostavleniem-uslug-po (дата обращения: 15.11.2023).
5. Лукьянов Д.О. Требования при проектировании информационной безопасности центра обработки данных // E-Scio. 2019. №11 (38). URL: https://cyberleninka.ru/article/n/trebovaniya-pri-proektiovanii-informatsionnoy-bezopasnosti-tsentra-obrabotki-dannyh (дата обращения: 15.11.2023).
6. Мерзляков С.Э. К вопросу о понятии информационной безопасности / Экономические и социально-гуманитарные исследования. 2022. №4. С. 175–180.
7. Нестеренко В.Р., Маслова М.А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними / Научный результат. Информационные технологии. 2021. №1. С. 48–54.
8. Серикулы О. Информационная безопасность при облачных вычислениях // Вестник магистратуры. 2019. №6-5 (93). С. 17–23.
9. Хан Д.В., Разгуляев К.А., Тягунов Д.М. Разработка порталов для управления облачными сервисами в составе центра обработки и хранения данных // Научно-технический вестник информационных технологий, механики и оптики. 2019. №6. С.1086–1093.
10. Шукурлаев А.Х. Распределенные облачные дата-центры // ORIENSS. 2021. №10. С. 635–650.

Журнал «Современная наука: актуальные проблемы теории и практики»