Cloud Advisor

CSPM как средство обеспечения безопасности облачной инфраструктуры

Автор: Cloud Advisor

Тип документа: Whitepaper

Содержание

Проблема безопасности публичных облаков

По данным опроса компании Flexera, в котором принимали участие организации различных масштабов и отраслей со всего мира, 98% всех респондентов в 2023 году так или иначе используют публичные облака. Более половины (53%) всех серверных мощностей уже перенесены в публичное облако и аналитики ожидают, что в следующие 12 месяцев эта цифра достигнет 59%. На данный момент в публичных облаках хранится половина всех данных опрошенных компаний.

Ошибки конфигурации (23%) занимают первое место среди инцидентов в области облачной безопасности, опережая взлом учетных записей (15%), эксплуатацию уязвимостей (14%) и заражение вредоносным ПО (9%).

Отчет Cloud Security Report 2022, Cybersecurity Insiders

Облачная модель потребления услуг набирает обороты и в России. Как свидетельствуют данные iKS-Consulting, в 2022 году выручка крупнейших поставщиков IaaS и PaaS выросла на 49%, достигнув ₽85 млрд, и аналитики ожидают, что к 2025 году этот показатель увеличится до ₽221 млрд. При этом немногие осознают, что перенос рабочей нагрузки в облако требует изменения политики безопасности данных и новых подходов к ее реализации. Данные и серверы находятся вне периметра безопасности организации на мощностях облачного провайдера, что влечет неэффективность, а порой даже неработоспособность традиционных методов защиты. Часть вопросов безопасности провайдер берет на себя, а для решения остальных предоставляет пользователям соответствующие инструменты. Но администратору, неискушенному в нюансах работы облачной платформы, ничего не стоит ошибиться, например, при создании политики доступа, особенно если речь идет о сложных многоуровневых приложениях.

Gartner утверждает, что львиная доля инцидентов, связанных с безопасностью в публичном облаке, вызвана ошибками конфигурации - банальная оплошность может свести на нет все усилия по построению системы защиты ваших ресурсов если окажется, что резервная копия критически важных данных хранится в незащищенном S3-бакете с публичным доступом.

Типичные ошибки при конфигурации облака

- Публичный доступ к объектному хранилищу
- Неверно настроенный доступ по протоколам SSH или RDP
- Публичный доступ к базам данных
- Избыточные привилегии аккаунта
- Отсутствие мультифакторной аутентификации
- Выключенное шифрование данных

Крупнейшие утечки данных из облака

Facebook

Утечка 540,000 записей пользователей (146 GB данных) через стороннее приложение, хранящее данные на недостаточно защищенном сервере AWS. Записи содержали данные идентификации пользователей, имена учетных записей, статистику лайков и комментарии.

Instagram

База данных с 49 миллионами записей пользователей оказалась в свободном доступе в облаке AWS. Свежие данные профилей пользователей, включая известных блогеров и знаменитостей, содержащие личную контактную информацию (адреса электронной почты и номера телефонов), не были защищены даже элементарным паролем. А так как база данных принадлежала компании, предоставляющей инструменты продвижения товаров и услуг через лидеров мнений, то угрозе также подверглись данные о финансовых расчетах с владельцами аккаунтов.

Capital One

Утечка 80 тысяч номеров банковских счетов и более миллиона номеров удостоверений личности благодаря бывшему разработчику Amazon, получившей учетные данные аккаунта, имеющего доступ к критическим данным в S3-хранилище, с помощью подделки запросов на стороне сервера (server-side request forgery attack, SSRF).

Чем же отличается подход к обеспечению безопасности данных в облаке и какие трудности возникают при его реализации?

Подход к обеспечению безопасности в облаке

Прежде всего необходимо осознать, что если ваши данные находятся в облаке, это вовсе не значит, что вся ответственность за них лежит на провайдере. Безусловно, провайдер несет ответственность за эксплуатацию аппаратного обеспечения, осуществляет контроль и управление компонентами на всех уровнях: от уровня виртуализации и операционной системы хостов до уровня физической безопасности объектов в датацентре. Однако, за сохранность своих данных и конфигурацию используемых ресурсов ответственны сами клиенты.

Ответственность клиента	Конфигурация облачной платформы	Сетевая безопасность
	Управление доступом (IAM)	Резервное копирование
	Безопасность ОС и приложений	Шифрование данных

Ответственность провайдера	Сервисы			
	Виртуальные машины	Хранилище	Базы данных	VPC
	Администрирование			
	Разработка	Физический доступ в датацентр	Доступ к системам облака	Периметр сети

Первый шаг к решению проблемы облачной безопасности - это создание четкой политики, отвечающей специфике работы конкретной организации. При этом необходимо принять во внимание:

- актуальные угрозы
- требования регуляторов
- рекомендации облачного провайдера
- проверенные практики использования облачных сервисов

Политика должна обновляться при добавлении в облако новых возможностей, изменении ландшафта угроз или требований регулирующих органов.

Практически все успешные атаки на облачные сервисы являются результатом их неверной настройки пользователем, неграмотного управления и допущенных ошибок. Менеджеры по безопасности и управлению рисками обязаны инвестировать в процессы и инструменты, обеспечивающие меры безопасности облака, чтобы иметь возможность проактивно и реактивно обнаруживать и устранять эти риски.

Отчет Innovation Insight for Cloud Security Posture Management

Далее, необходимо периодически собирать данные о конфигурации ресурсов и проверять их на соответствие сформированной политике. При использовании механизмов IaC (Infrastructure-as-Code), таких как, например, Terraform, желательно организовать процедуру проверки еще на стадии разработки, чтобы предотвратить появление ресурсов с неверными настройками.

> 59% респондентов назвали адаптацию мер обеспечения информационной безопасности самой сложной задачей при переходе на облачные технологии.
>
> Исследование «Страх облаков», PwC

При обнаружении несоответствий их необходимо отсортировать по приоритетам, исследовать возможные пути исправления, а после исправления - оценить прошлое и актуальное состояние облака и визуализировать ключевые метрики для оценки эффективности принятых мер.

На бумаге все выглядит прозрачно, однако при реализации такого подхода организации нередко сталкиваются с определенными проблемами.

Трудности реализации

Ограниченная наглядность

Большинство пользователей IaaS имеют ограниченную наглядность (visibility) представления активов, развернутых в облаке: не всегда очевидно кто и к каким приложениям получает доступ, какие данные отправляются и принимаются приложением, покидают ли они периметр защиты, а если покидают, то в зашифрованном или открытом виде. Большое количество различных ресурсов - виртуальных машин, IP-адресов, папок объектного хранилища, баз данных, размещенных в разных зонах доступности, разных облаках и каталогах - создает трудности при идентификации активов и обеспечении контроля применения политик безопасности. По данным Cybersecurity Insiders, отсутствие наглядности представления безопасности инфраструктуры и, как следствие, невозможность быстрого обнаружения ошибок конфигурации являются одними из основных вызовов при обеспечении облачной безопасности.

Динамическая природа облака

Легкость развертывания новых ресурсов в облаке стимулирует рост числа облачных активов. Ресурсы постоянно добавляются в облако при запуске новых проектов, миграции текущих рабочих нагрузок в облако. Кроме того, меняется конфигурация существующих ресурсов. Ситуацию усложняют обширные возможности автоматизации, предоставляемые облачным провайдером, с помощью которых сотни ВМ могут быть запущены, остановлены или изменены за считанные секунды. Без должного контроля за настройками безопасности каждого ресурса это приводит к размытию политики безопасности.

Человеческий фактор

IaaS сервисы облачных платформ изначально спроектированы как системы “самообслуживания” для пользователей, упрощающие задачу запуска проектов без длительных этапов планирования, согласования, покупки оборудования и лицензий. Рост скорости запуска проектов приводит к появлению брешей в защите, так как разработчики, взаимодействующие с облачными сервисами и ресурсами, зачастую не обладают достаточной квалификацией для принятия верных решений в области безопасности. Кроме того, сама политика безопасности может состоять из сотен правил и положений, что исключает возможность ручного контроля.

Автоматизированные решения

Становится очевидным, что при обеспечении безопасности данных в облаке не обойтись без специализированных средств управления состоянием облачной безопасности (Cloud Security Posture Management). Эти решения позволяют получать данные о конфигурации сервисов с помощью API облачного провайдера и в автоматическом режиме проверять их на соответствие политике безопасности, сигнализируя пользователю о ее возможных нарушениях и потенциальных угрозах. Некоторые из этих продуктов также предлагают рекомендации по нейтрализации несоответствий и следят за появлением новых угроз, предотвращая возможные инциденты с помощью регулярных обновлений.