Cloud Advisor

Поиск уязвимостей в ПО и ОС в публичных облаках

Автор: Cloud Advisor

Тип документа: Whitepaper

Содержание

Введение

За последние годы облако из новой перспективной технологии, которой многие поначалу опасались полностью доверить свои данные, превратилось в важнейший инструмент бизнес-стратегии. Все больше компаний доверяют облачным провайдерам свои критичные нагрузки, перенося важные процессы и ресурсы на облачные площадки. Это позволяет упростить бизнес-процессы, ускорить запуск новых продуктов и в итоге повысить конкурентоспособность своих решений и компании в целом. Однако, не все осознают, что использование новых технологий требует новых подходов к информационной безопасности.

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

Одной из основных практик для обеспечения безопасности всегда являлось предотвращение эксплуатации уязвимостей. Проникновение через уязвимость в программном обеспечении считается одним из самых популярных векторов атаки. Посмотрим, какие методы управления уязвимостями существуют на данный момент и насколько хорошо они работают в облаке.

Сканирование

Классические подходы к сканированию уязвимостей

На сегодняшний день наиболее распространены следующие технологии сканирования уязвимостей.

1. Неаутентифицированное сканирование

При таком подходе виртуальная машина сканируется в режиме “черного ящика”, о котором известно только одно – ее IP-адрес. Сканер не знает, что происходит непосредственно на ВМ, а только пытается строить догадки в зависимости от ответов ВМ на входящие сетевые запросы, отправляемые сканером. Минусы такого подхода очевидны:

a. Риск пропустить нечто важное, т.к. данные могут быть получены только от ограниченного числа открытых на момент сканирования портов и доступных служб.
b. Большое число ложных срабатываний.
c. Низкая детализация полученной информации.
d. Необходимость наличия сетевого доступа от модуля сканирования к сканируемому хосту.

2. Сканирование с помощью агентов

В этом случае сканирование осуществляется с помощью агентов, которые устанавливаются непосредственно на ВМ, собирают информацию и отправляют ее управляющему модулю. Основные недостатки:

a. На практике невозможно добиться 100% покрытия агентами всей инфраструктуры, что оборачивается наличием т.н. «слепых зон».
b. Необходимость устанавливать и обновлять агенты на каждой ВМ увеличивает общую стоимость владения.
c. Агенты своей работой оказывают влияние на производительность системы.
d. Агенты могут быть удалены, отключены или обойдены злоумышленниками или вредносным кодом.
e. Сами агенты могут содержать уязвимости и таким образом увеличивать поверхность атаки (например, CVE-2022-0015 или CVE-2021-1647).

3. Аутентифицированное сканирование

При этом подходе проверяющий модуль получает сетевой доступ к ВМ с использованием аутентификации по протоколам SSH или RDP и осуществляет сканирование в контексте целевой системы.
Здесь наблюдаются следующие минусы:

a. Наличие на каждой ВМ дополнительной учетной записи, обладающей широкими привилегиями, необходимыми для осуществления сканирования, увеличивает поверхность атаки.
b. Недостаток покрытия, аналогично сканированию с помощью агентов, благодаря невозможности “достучаться” до каждой системы в распределенной инфраструктуре или отсутствию дополнительной учетной записи для сканирования.
c. Требование ротации паролей этой учетной записи усложняет поддержку решения.
d. Такая проверка оказывает влияние на производительность системы.

Сканирование Cloud Advisor

Метод, реализуемый решением Cloud Advisor, использует преимущества, доступные в облаке, и поэтому лишен описанных выше недостатков. Напротив, такой подход:

- Обеспечивает 100% покрытие всех виртуальных машин сразу после их развертывания.
- Позволяет развернуть Cloud Advisor за минуты и получить полную информацию обо всех уязвимостях в вашей инфраструктуре в течении часа.
- Не требует работ по установке и обновлению агентов, снижая общую стоимость владения.
- Не оказывает влияния на производительность виртуальных машин.
- Не требует сетевой связности между машиной и сканирующим модулем.

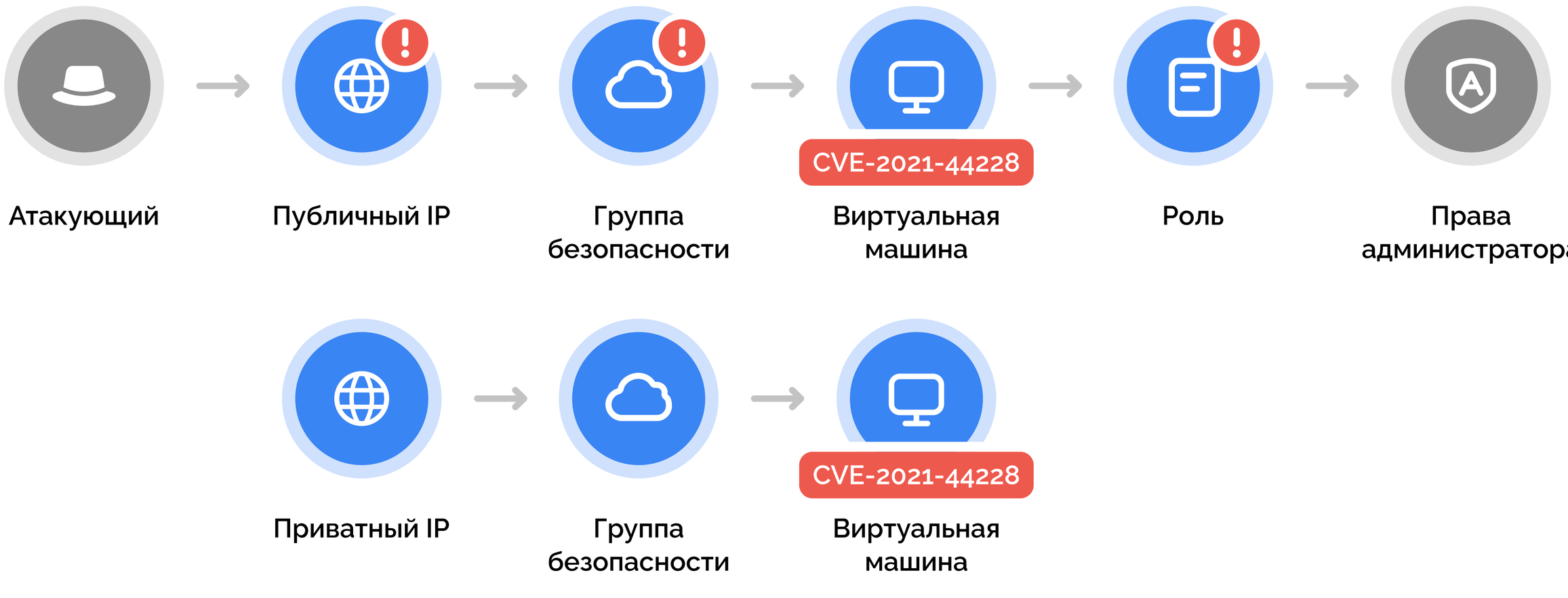
Из недостатков можно упомянуть тот факт, что этот способ работает только в облаке, так как использует возможности по управлению дисками ВМ, которые предоставляет облачный провайдер, а также небольшое повышение расходов на облако, т.к. сканирующие мощности разворачиваются непосредственно в аккаунте пользователя.

Приоритизация

Одной из важнейших задач в процессе управления уязвимостями является их приоритизация.

Традиционный подход

Традиционные средства поиска уязвимостей не имеют данных о сетевой связности и правах виртуальных машин в облаке. Для решений, разработанных для on-prem, приоритет уязвимости Log4Shel на публичном веб-сервере с доступом к важной БД и Log4Shel на забытой приватной машине без каких-либо прав будет одинаковым.



Некоторые продукты предоставляют возможности по приоритизации ВМ, но только в ручном режиме, потому что у средства поиска уязвимостей нет доступа к информации о конфигурации облака, а соответственно, оно не имеет данных о сетевой связности и правах ВМ в облаке. Ручная приоритизация не работает в динамически изменяющейся облачной среде.

В итоге пользователь получает сотни, иногда тысячи алертов о найденных на ВМ уязвимостях. Это приводит к ряду серьезных негативных последствий:

- Увеличение времени реагирования на критический инцидент. Инженер может разбираться с менее приоритетными алертами, в то время как критически важные события остаются без внимания.
- Пропуск важного алерта из-за усталости от оповещений. Среагировать на одно оповещение несложно, на десятки и сотни – на порядок сложнее. И чем больше их становится, тем выше риск того, что сотрудник упустит нечто важное.
- Повышение расходов, связанных с разбором алертов, которые являются ложными срабатываниями. Многие из алертов требуют длительного расследования с привлечением специалистов из других отделов.
- Эмоциональное выгорание инженеров. Постоянный поток оповещений и монотонная работа по их разбору приводит к выгоранию сотрудников, повышению текучести кадров, снижению удовлетворенности работой и производительности.

Подход Cloud Advisor

Единственный способ бороться с большим количеством алертов – их правильная приоритизация. Подобно традиционным средствам управления уязвимостями Cloud Advisor осуществляет приоритизацию, используя информацию о наличии публичных эксплойтов, типе уязвимости, CVSS-оценке и т.д.

> Защитники мыслят списками. Атакующие мыслят графами. Пока это так, атакующие побеждают.
>
> Джон Ламберт, Центр анализа угроз Майкрософт

Однако, обладая полной информацией о сетевой связности облачных ресурсов, Cloud Advisor дополнительно анализирует публичные IP-адреса, балансировщики нагрузки, NAT, а анализ правил групп безопасности, наложенных на ресурс, позволяет вычислить эффективную публичную доступность, то есть разделить публичную доступность со всех IP-адресов и публичную доступность с ограниченного количества IP-адресов. Этот анализ помогает понять какие уязвимости находятся на ресурсах с неограниченным публичным доступом и поэтому должны быть исправлены в первую очередь.

Кроме того, основываясь на данных о правах ресурсов в облаке, Cloud Advisor способен оценивать возможные последствия от их компрометации и поднимать приоритет уязвимостям, обнаруженным на ВМ, имеющих широкие права в облаке (например, доступ к объектному хранилищу или права на запуск других ВМ).

Вывод

Современные средства поиска уязвимостей не созданы для облака. Наличие слепых зон, высокая общая стоимость владения, влияние на производительность облачных ресурсов обусловлены применением старых присущих on-prem подходов. Увеличение времени реагирования на инцидент и пропуск важных алертов связаны с отсутствием правильной приоритизации на основе данных о конфигурации облака.

Cloud Advisor предоставляет легкое в установке и использовании средство, обеспечивающее мгновенное развертывание и 100% покрытие вашей инфраструктуры. Полные данные о конфигурации облака позволяют Cloud Advisor предоставить для реагирования лишь небольшой процент действительно важных инцидентов, которые являются критическими для вашей организации.