doi:10.32620/oikit.2018.81.12

УДК 004

И.Н. Бабак, А.А. Микитенко

Анализ механизмов обеспечения безопасности информации в облаке Amazon Web Services (AWS)

Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт»

Рассмотрены преимущества и недостатки использования облачных технологий в компаниях. Проанализированы программные механизмы защиты данных и ресурсов пользователей от несанкционированного доступа, предоставляемые поставщиком облачных услуг Amazon Web Services (AWS). Проанализированы основные уязвимости, которые могут присутствовать при наличии эффективных программных средств обеспечения безопасности облачных ресурсов. Выделены такие проблемы, как устаревание ключей доступа, открытые порты и ненастроенные правила безопасности, наличие неиспользуемых ресурсов в облаке. Предложены подходы для повышения уровня безопасности и защиты информации в облаке AWS. Предложена разработка фреймворка, основными функциями которого являются: сканирование и удаление устаревших ключей, открытых портов, неиспользуемых ресурсов и уязвимых конфигураций безопасности данных в облаке. Для удобства применения такого фреймворка предполагается разработка скриптов для автоматизации процесса его развертывания.

Ключевые слова: AWS, облачные технологии, механизмы защиты данных, уязвимости, фреймворк.

Введение

Требования современного рынка приводят все больше компаний к необходимости использования рабочих станций, хранилищ файлов, баз данных, серверов и хостингов. Их применение является достаточно дорогостоящей статьей расходов компании, так как возникает необходимость закупать, конфигурировать и связывать между собой от нескольких десятков до нескольких тысяч вычислительных устройств, на которых держится бизнес компании, а в будущем – еще и постоянно обновлять и поддерживать эти устройства и каналы связи. В таких условиях использование виртуальных ресурсов в облаке становится достаточно привлекательной альтернативой использованию физических вычислительных ресурсов. Однако вопрос обеспечения надежности хранения и безопасности доступа к информации в облаке представляет собой один из главных аспектов для компаний при принятии решения об использовании облачных ресурсов, поэтому исследование механизмов обеспечения заданного уровня безопасности и их улучшения является актуальным.

1 Постановка задачи

Понятие облачных ресурсов и концепция облачных вычислений впервые были обозначены в 2006 году [1]. Постепенно качество предоставляемых облачных услуг и ресурсов улучшилось и, как следствие, за последние 3 – 5 лет много компаний разных масштабов и сфер деятельности перешло на использование виртуальных облачных ресурсов [2]. Привлекательность их использования держится на нескольких базовых принципах [3]:

- pay-as-you-go – потребитель платит только за те ресурсы, которые реально используются, т. е. не платит за простой благодаря использованию посекундной и поминутной тарификации;

- неограниченность ресурсов – возможность потребления облачных ресурсов (дискового пространства, оперативной памяти, процессорного времени и т.п.) в любой момент времени зависит только от способности компании платить за их использование без необходимости затрат времени и финансов на покупку, транспортировку, физическое размещение;

- перенос ответственности за состояние физических ресурсов на провайдера облачных ресурсов – снижает для компании такую большую статью затрат, как поддержка и профилактика физических (on premise) вычислительных ресурсов, а именно расход на дорогие материалы и комплектующие, а также на оплату труда высококвалифицированных специалистов.

Несмотря на все перечисленные преимущества, на сегодняшний день в нашей стране часто можно встретиться с недоверчивым отношением к облачным ресурсам, многие компании сомневаются, нужен ли им «переезд» с «железа» на «облако». Основными причинами сомнений являются следующие:

- кажущаяся незащищенность информации, которая хранится в облаке: все ресурсы доступны через Интернет, следовательно, есть дополнительная возможность для злоумышленника получить несанкционированный доступ к данным;

- осознание того факта, что при переходе на использование облачных ресурсов компания так или иначе передает все свои данные (конфиденциальные, персональные) третьему лицу, которым является провайдер облачных ресурсов;

- страх перед тем, что в конце месяца придет огромный счет за использование виртуальных ресурсов;

- кажущаяся неустойчивость инфраструктуры, построенной в облаке – слишком много составляющих, которые являются виртуальными, или, что еще хуже, эфемерными (такими, которые теряют все накопленные данные и состояния после удаления)

Можно заметить, что большинство перечисленных недостатков использования облачных ресурсов основывается на простом человеческом недоверии к провайдеру.

Целью исследования в данной статье является проведение анализа применяемых подходов для обеспечения безопасности использования облачных ресурсов для компании. Особое внимание в исследовании предлагается уделить анализу и выбору дополнительных механизмом защиты от человеческих ошибок в процессе использования облачных ресурсов.

2 Анализ уязвимостей и современных подходов для обеспечения защиты данных в облаке

Сегодня на рынке конкурируют множество поставщиков облачных ресурсов. Но наиболее популярными и подходящими для больших компаний является два представителя – Amazon Web Services (далее AWS) и Microsoft Azure.

В качестве объекта для анализа был выбран AWS, так как в нем реализовано наибольшее количество механизмов обеспечения защиты и эти механизмы поставляются в виде отдельных ресурсов, а не сплошным конгломератом, что упрощает процесс анализа.

В ходе анализа были рассмотрены компании и организации, которые полностью или частично перенесли все свои вычислительные мощности, файловые хранилища и даже базы данных в одно из самых мощных и популярных облаков на сегодняшний день:

- NASA – используют серверы в AWS для обеспечения стриминга медиа данных с робота ATHLETE [4];
- Netflix – мировой лидер в сфере медиа и телевидения с помощью ресурсов AWS анализирует миллиарды сообщений среди 100 тысяч приложений [5];
- Autodesk – компания использует автоматическое масштабирование на платформе AWS для выполнения сотен симуляций в час (ранее для этого требовались часы или даже дни) [6];
- Hitachi – мультинациональный конгломерат, который помогает крупным корпорациям управлять гибридной облачной инфраструктурой и SaaS [7];
- McDonalds – после перехода в облако повысили эффективность на 66% и сейчас инфраструктура может обслуживать 8600 транзакций в секунду [8];
- Лаборатория Касперского – крупнейшая в мире компания, работающая в сфере информационной безопасности, использует сервисы AWS для разработки и поддержки своих продуктов;
- Royal Opera House – является одним из самых посещаемых оперных театров в мире, в прошлом имел большие инфраструктурные проблемы, связанные с невозможностью гибкого масштабирования ресурсов. После перехода в облако все эти проблемы удалось успешно решить [9];
- Coursera – образовательное учреждение, которое сотрудничает с лучшими университетами мира. Веб-сайт компании работает на платформе AWS, что позволяет ежемесячно обрабатывать более 500 Тб трафика [10];
- Foursquare – использует AWS для анализа миллионов пользовательских меток, что помогает компании снизить расходы на лицензирование и использовать сотрудников компании для решения более важных задач [11].

Следует заметить, что анализировались лишь программные механизмы защиты. Такие аспекты, как безопасность физических ресурсов (например, сеть, межпроцессорное взаимодействие в свете последних новостей о Spectre и Meltdown), в дата-центрах AWS не рассматривалась, так как этой стороной занимается полностью поставщик и пользователь даже не задумывается о том, где и как это все физически реализовано.

В ходе анализа также были рассмотрены механизмы, которые на данный момент разработаны в облаках и помогают максимально эффективно защищать данные клиентов от потери, незаконного использования, утечки и корпоративного шпионажа. К наиболее популярным механизмам можно отнести следующие:

- Identity and Access Management (IAM) – механизм, обеспечивающий контроль и разграничение доступа к ресурсам в облаке, основывается на таких сущностях, как группы пользователей, роли и пользователи. Предоставляет доступ через пары ключей и пароли, обеспечивает функцию многофакторной аутентификации [12];
- Key Management Service (KMS) – сервис для работы с ключами шифрования, которые применяют для кодирования всей без исключения информации, которая хранится в облаке. Публичные части ключей хранятся в облаке, приватные – только у клиента. Это обеспечивает невозможность чтения провайдером данных клиента [13];

- Trusted Advisor – сервис, который периодически или постоянно сканирует ресурсы клиента на наличие уязвимостей, сам не предпринимает никаких действий, только показывает клиенту возможные пробелы в безопасности и способы их закрытия [14];

- интеграция с Active Directory сервисом, который будет управлять доступом пользователей к тем или иным ресурсам;

- Cognito – сервис аутентификации пользователей в облаке [15].

Несмотря на такой широкий спектр механизмов защиты, никто не может защитить клиента от человеческих ошибок. Поэтому разработка дополнительных средств защиты ресурсов от человеческих ошибок и последующих утечек данных является важной задачей, для решения которой в данном исследовании предлагаются следующие подходы.

Основная проблема безопасности в облаке – устаревание ключей доступа. Провайдеры всячески настаивают на том, чтобы проводилась постоянная ротация ключей, но не форсируют это. Очевидно, нужен инструмент для принудительной ротации. Более того, инструмент должен удовлетворять политикам конфиденциальности и техническим нормам конкретной организации.

Вторая проблема – не настроенные правила безопасности и чрезмерно открытые порты в сетевой инфраструктуре. Провайдеры эту проблему разрешают, так как это может быть обусловлено спецификой приложения, которое развернуто на данных ресурсах.

Третья проблема – наличие большого количества неиспользуемых ресурсов. Это чревато двумя проблемами:

- повышение стоимости, так как нужно платить за ресурсы, которые простаивают;

- проявление уязвимостей, поскольку зачастую ресурсы, которые не контролируются и оставлены без внимания, могут быть настроены с минимальными правилами защиты.

Для автоматизации закрытия этих перечисленных уязвимостей предлагается проектирование, разработка кода и использование следующих инструментов, которые будут обеспечивать более высокий уровень защиты информации при использовании облачных ресурсов:

- инструмент для сканирования и удаления устаревших ключей доступа, который в качестве параметра будет принимать пороговое значение возраста ключа и удалять все ключи старше заданного количества времени;

- инструмент для сканирования открытых портов и конфигурации правил безопасности, в результате чего будет формировать список портов, рекомендуемых к закрытию или ограничению доступа для более узкого диапазона адресов, а также будет предоставлять возможность для автоматического закрытия портов из списка после сканирования;

- инструмент, который будет выполнять три основные функции: сканировать аккаунты на наличие старых и неиспользуемых ресурсов, удалять эти ресурсы, генерировать отчеты с подробными сведениями об обнаруженных неиспользуемых ресурсах, что, в свою очередь, даст возможность повысить безопасность и снизить стоимость ресурсов.

Данные инструменты разрабатываются как фреймворк и будут выполнять свои функции внутри самого облака для обеспечения максимального быстродействия. В качестве реализации и запуска каждого из инструментов в облаке выбраны так называемые Lambda-функции, которые относятся к классу

Serverless applications, т.е. не требуют отдельных серверов для выполнения. В качестве языка разработки предлагается использовать язык Python. Для удобства применения такого фреймворка предполагается разработка скриптов для автоматизации процесса его развертывания.

Заключение

Перечисленные инструменты предполагается разрабатывать с учетом особенностей применения в облаке AWS, однако будет учтена возможность применения их в других облаках с небольшими дополнительными модификациями. Использование предложенных инструментов позволит максимально быстро просканировать аккаунты в облаке, показать наглядный отчет об уязвимостях и в полуавтоматическом режиме эти уязвимости закрыть.

Список литературы

1. APN Partner Stories - Written Case Studies [Electronic resource]. - Mode of access: https://aws.amazon.com/partners/success
2. A HISTORY OF CLOUD COMPUTING: [Electronic resource]. - Mode of access: https://cloudtweaks.com/2011/02/a-history-of-cloud-computing
3. AWS Pricing [Electronic resource]. – Mode of access: https://aws.amazon.com/pricing/?nc1=h_ls
4. AWS Case Study: NASA/JPL's Desert Research and Training Studies [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/nasa-jpl/
5. Netflix & Amazon Kinesis Streams Case Study [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/netflix-kinesis-streams/
6. Autodesk Case Study [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/autodesk/
7. AWS Case Study: Hitachi [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/hitachi/
8. McDonalds Case Study [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/mcdonalds/
9. AWS Case Study: The Royal Opera House [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/royal-opera-house/
10. AWS Case Study: Coursera [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/coursera/
11. Foursquare Case Study [Electronic resource]. – Mode of access: https://aws.amazon.com/solutions/case-studies/foursquare/
12. AWS Identity and Access Management (IAM) [Electronic resource]. – Mode of access: https://aws.amazon.com/iam/
13. AWS Key Management Service (KMS) [Electronic resource]. – Mode of access: https://aws.amazon.com/kms/
14. AWS Trusted Advisor [Electronic resource]. – Mode of access: https://aws.amazon.com/premiumsupport/trustedadvisor/
15. Amazon Cognito [Electronic resource]. – Mode of access: https://aws.amazon.com/cognito/

Поступила в редакцию 26.09.2018

Аналіз механізмів забезпечення безпеки інформації в хмарі Amazon Web Services (AWS)

Розглянуто переваги і недоліки використання хмарних технологій в компаніях. Проаналізовано програмні механізми захисту даних і ресурсів користувачів від несанкціонованого доступу, що надаються постачальником хмарних послуг Amazon Web Services (AWS). Проаналізовано основні вразливості, які можуть бути присутніми за наявності ефективних програмних засобів забезпечення безпеки хмарних ресурсів. Виділено такі проблеми, як застарівання ключів доступу, відкриті порти і ненастроєні правила безпеки, наявність у хмарі ресурсів, які не використовуються. Запропоновано підходи для підвищення рівня безпеки і захисту інформації в хмарі AWS. Запропоновано розроблення фреймворка, основними функціями якого є: сканування і видалення застарілих ключів, відкритих портів, невикористовуваних ресурсів і вразливих конфігурацій безпеки даних у хмарі. Для зручності застосування такого фреймворка передбачається розроблення скриптів для автоматизації процесу його розміщення.

Ключові слова: AWS, хмарні технології, механізми захисту даних, вразливості, фреймворк.

Analysis of Information Security Mechanisms in Amazon Web Services (AWS) cloud

Advantages and disadvantages of using cloud technologies in companies are considered. The programmatic mechanisms for protecting data and users' resources from an unauthorized access that are given by an Amazon Web Services (AWS) cloud service provider are analyzed. The basic vulnerabilities which can be present even when effective programmatic methods for cloud resources safety exist are analyzed. Such problems as obsolescence of the access keys, open ports and untuned safety rules, presence of resources which are not in use in a cloud are highlighted. In the article approaches for increasing data protection strength and information security in the AWS cloud are proposed. Development of the framework is proposed, the main functions of this framework is the following: scanning and removing outdated access keys, open ports, resources which are not in use and vulnerable configurations of protection mechanisms in a cloud. For ease of use of the framework, it is supposed to develop scripts for automating the process of its deployment.

Keywords: AWS, cloud technologies, data security mechanisms, vulnerabilities, framework.

Сведения об авторах:

Бабак Ирина Николаевна – доцент, к.т.н., доцент каф. 105 «Информационные технологии проектирования», Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Украина, irinkababak@gmail.com.

Микитенко Александр Александрович – студент каф. 105 «Информационные технологии проектирования», Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Украина, alexandr.mykytenko@gmail.com