Добрый день, уважаемые студенты! Я рад вас всех видеть на очередной сессии вопросов и ответов. Мы получили от вас очередной набор вопросов, которые вас интересуют. На этой сессии мы каждый вопрос детально рассмотрим и разберем. Итак, давайте начнем.

Вопрос: «Что означает термин «инфраструктура виртуализации»?» Отвечаю. Начнем с того, что как такого термина «инфраструктура виртуализации» не существует. Это два отдельно стоящих термина сами по себе. Что такое инфраструктура мы с вами уже разобрали. Что такое виртуализация я сейчас вам объясню. Для того чтобы объяснить, что такое виртуализация, давайте вспомним, что такое дата-центр AWS. Как мы с вами помним, дата-центр AWS – это достаточно большое помещение, в котором расположены серверы. Каждый сервер расположен следующим образом: в виде шкафа, на каждой полке этого шкафа находится каждый отдельно взятый сервер. AWS стремится поместить в один шкаф наибольшее количество вычислительных мощностей для того, чтобы оптимально использовать физическое пространство. Таким образом, каждый сервер внутри этого шкафа серверов он в десятки раз мощнее наших самых продвинутых персональных компьютеров и ноутбуков. Теперь двигаемся дальше. Мы с вами помним, что внутри AWS у вас есть возможность выбрать несколько разных типов инстансов, т.е. вы можете выбрать самый слабый с одним ядром процессора, с двумя гигабайтами оперативной памяти и дальше мощнее и мощнее можно выбрать очень мощный сервер, который несколько десятков процессорных мощностей, а также несколько сотен гигабайтов оперативной памяти. Теперь для того, чтобы предоставить возможность вот так делить и выбирать что большой, что маленький сервер, была разработана технология виртуализации. Что она означает? Она означает, простыми словами, есть определенный физический сервер со своими мощностями. Это количество процессоров, а также количество оперативной памяти. Виртуализация позволяет нам разделить вот эти мощности одного сервера и виртуально получить отдельные независимые друг от друга сервера меньшей мощности. Таким образом, мы можем, например, сервер, в котором два процессора и четыре оперативной памяти, через технологию виртуализации поделить на два. Таким образом получить два отдельных, отдельно работающих независимых друг от друга сервера по одному процессору и два гигабайта оперативной памяти. Теперь, если мы возвращаемся к инфраструктуре виртуализации, в этом случае подразумевается все то железо, программное обеспечение и другое оборудование, будь то физическое, либо виртуальное, которое помогает поддерживать процесс виртуализации физических серверов AWS, подразделять, делить на несколько маленьких частей и нам как клиентам AWS предоставлять возможность выбирать от самого маленького сервера отдельно стоящего до супермощного.

Вопрос: «Можете ли объяснить суть implicit allow и implicit deny на конкретном примере?» Отвечаю. Следует понимать, что такое implicit. Implicit – это что-то, что есть по умолчанию изначально. Таким образом, когда мы говорим implicit allow, это значит по умолчанию разрешено. Когда мы говорим implicit deny, это значит по умолчанию запрещено. Если мы говорим про AWS, то все то, что связано с доступами изначально по умолчанию запрещено. Таким образом, есть только implicit deny. Implicit allow в рамках AWS такого не существует. Таким образом, если приводить пример, вы создаете нового пользователя и у этого пользователя нет никаких прописанных policy, будь то inline прописанное для конкретного пользователя, будь то привязанное к нему отдельно стоящее policy. Если таковых не имеется, то у этого пользователя по умолчанию никаких доступов ни на какой сервис не будет. Так как у нас внутри AWS implicit deny.

Вопрос: «Можете ли объяснить суть explicit allow и explicit deny на конкретном примере?» Отвечаю: Когда мы говорим про explicit allow и explicit deny, подразумевается что-то явно прописанное, т.е. мы явно либо разрешаем пользователю какое-то действие на какие-то ресурсы, либо явно запрещаем. Есть третий вариант implicit deny. Это что-то, что по умолчанию. По умолчанию, если явно ничего не прописано, то в этом случае доступ запрещается. Теперь давайте на примере разберем, какие шаги предпринимает AWS для того, чтобы понять разрешен или запрещен доступ к конкретному identity на определенную операцию и на определенные AWS ресурсы. Представим, что мой пользователь, user Yelzhan, хочет открыть список объектов внутри бакета, там, bucket01. В этом случае пользователь user Yelzhan, операция, которую я хочу произвести это list objects и ресурс, над которыми происходит эта операция это bucket01. То есть ARN конкретного ресурса. Теперь, как действует AWS. Как только он получает вот это действие, то он начинает проверять наличие explicit deny. То есть, есть ли хотя бы одна policy, которая явно запрещает конкретное действие. Если explicit deny находится, то в этом случае любое количество explicit allow перечеркивается и доступ не предоставляется. В другом случае, если AWS не находит explicit deny, то есть явно вот это действие не запрещено, в этом случае он переходит на следующий этап. Второй этап – это проверка на наличие explicit allow. То есть, есть ли хотя бы одна policy, которое явно предоставляет доступ к нашей операции. Если он находит эту policy, то доступ моему пользователю посмотреть список объектов внутри bucket01 предоставляется. В случае, если AWS не находит policy, которые явно предоставляют доступ к конкретной операции, в этом случае конкретная операция case не прописана для этого пользователя во всех его policy. В этом случае срабатывает поведение по умолчанию, это implicit deny, в этом случае доступ по умолчанию не предоставляется.

Вопрос: «Насколько AWS подвержен атакам злоумышленников?» Отвечаю. Мы с вами на лекции разобрали, что такое Shared Responsibility Model. Это такая модель, которая в зависимости от модели предоставления сервиса определяет за какую часть инфраструктуры отвечает AWS и пользователи AWS, т.е. мы. Под моделью предоставления сервиса имеются в виду три опции: это IaaS – Infrastructure as a service, когда у нас есть полный контроль над ресурсами. PaaS – Platform as a service, когда у нас за часть отвечает AWS, за часть отвечаем мы. И третий SaaS – Software as a service, когда сервис предоставляется как готовый продукт и за большую часть как сервиса, так и с точки зрения безопасности ответственность лежит на стороне AWS. Мы можем только на уровне настроек менять это ПО сервис и ровно только за эту часть ответственность с точки зрения безопасности. То есть, мы должны ответственно сделать настройку этого сервиса таким образом, чтобы не открывать потенциальные места угрозы злоумышленникам. Вне зависимости от того, по какой модели предоставляется сервис и то, что относится к физической составляющей, начиная от одного сервера, заканчивая дата-центром и глобальной инфраструктурой AWS, ответственность лежит на облачном провайдере. Если мы говорим возможные места атаки злоумышленников, то подразделяются соответственно на два. Это те места, где ответственны мы и те места, за которые ответственны AWS. Насколько я понял из вопроса, подразумевается, что мы, как пользователи AWS, максимально все правильно настроили и обезопасили свою IT-инфраструктуру в облаке и имеется в виду тот случай, когда место, где было проникновение и проведена соответствующая злоумышленническая операция, она прошла в том месте, где ответственен сам AWS. В этом случае необходимо вспомнить, что на постоянной основе AWS проходит процедуры сертификации соответствии стандартам качества, регуляторным требованиям и положениям. И все полученные подтвержденные сертификаты публикуют в сервисе AWS Artifact, где вы можете на бесплатной основе по требованию эти сертификаты и эти документы скачать к себе. Наличие различных сертификатов качества, соответствия различным регуляторным требованиям у AWS дают несколько возможностей. Две самые очевидные: это первое – вам уже нет необходимости получать этот сертификат, так как за вас этот сертификат получил AWS. И если вы разворачиваете свою инфраструктуру в облаке AWS, то вы можете эти сертификаты предоставлять по требованию в соответствующие органы и они будут валидными. Второе – это то, что каждый этот сертификат для того, чтобы успешно пройти, необходимо в зависимости от готовности компании от нескольких месяцев до нескольких лет. Таким образом, во время прохождения внутри компании многие процессы, аспекты функционирования этой компании меняются и большинство потенциальных мест атаки злоумышленников исключаются либо настраиваются верным образом и риск того, что злоумышленник успешно произведет эту атаку минимизируется. Из всего этого следует, что наличие этих сертификатов дает некоторую гарантию и уверенность в том, что в частности AWS минимально подвержен атакам злоумышленников по сравнению с любыми другими компаниями, у которых этих сертификатов соответствия качеству не имеется.

Вопрос: «Что такое ключи шифрования?» Отвечаю: что такое ключи шифрования более подробно вы познакомитесь в отдельной дисциплине внутри вашего университета по безопасности, я лишь объясню основные моменты, которые достаточно вам знать для работы в облаке AWS. Давайте рассмотрим пример самого простейшего метода шифрования. Представим, у нас есть слово папа и нам необходимо этот текст зашифровать. Наш метод шифрования – это сдвиг по алфавиту на следующую букву. Таким образом, в слове папа, п становится р, а становится б. И на выходе мы получаем зашифрованный текст, который рбрб. Таким образом, вы получили общее понимание, что такое шифрование. В случае, когда мы говорим, что у нас есть текст определенной длины, который тем или иным способом применяется для того, чтобы входной незашифрованный текст привести в выходной зашифрованный текст, то этот текст мы говорим ключом шифрования. С этим ключом шифрования вы можете зашифрованный текст обратно расшифровать и прочитать исходное сообщение. Без этого ключа вы даже при наличии зашифрованного текста ничего с ним сделать и никакую полезную информацию от него получить не сможете. Так вот, encryption keys у нас встречается в сервисе KMS, то есть Key Management Service, в котором мы более подробно поговорим, какие методы шифрования используются и как он управляет всеми этими ключами шифрования.

Вопрос: «Какая организация верифицирует соответствие сертификатам облачного провайдера AWS или в целом любого облачного провайдера?» Отвечаю, когда мы говорим про сертификаты, будь то сертификат соответствия стандартам качества, либо соответствия некоторым регуляторным требованиям, то за каждым этим сертификатом стоит некоторая компания или организация, которая узконаправленно занимается разработкой этих требований и верифицирует компании, которым необходим этот сертификат, после чего выдает этот сертификат. Ценность отдельного сертификата зависит от того, насколько популярна и важна эта организация. Когда мы говорим про AWS, и в частности, экзамен AWS Certified Cloud Practitioner, чаще всего упоминаются три сертификата. Первый сертификат – это HIPAA, два А в конце. Это сертификат, который прописывает стандарты качества для IT-компаний, которые работают в сфере медицины. Второе – это GDPR. Это тот документ, который регулирует хранение, обработку и передачу персональных данных пользователей, людей, которые находятся в ЕС в Европе. И третий, который также часто приходит, это ISO 27001. Это общеизвестный стандарт качества. Он состоит из нескольких различных разделов, относящихся к различным аспектам функционирования компании, является достаточно общим. И при наличии этого сертификата стандарта качества, говорят, что процессы внутри компании максимально правильно выстроены для того, чтобы эффективно работать и делать свою работу.

На этом мы рассмотрели все вопросы, полученные от вас. Я надеюсь, вы получили ответы. На этом мы завершаем сессию вопросов и ответов. Увидимся с вами на следующих наших активностях. До встречи!