Рубежка – вариант 7 – Поговорим про безопасность. Какие существуют направления повышения безопасности в облаке? Какие компоненты безопасности настраивать **обязательно**?

Само по себе облако гарантирует безопасность, по следующим причинам: сертификация по различным стандартам, как например, WS Certified Solutions Architect - топовый сертификат для архитекторов облачных решений для Amazon Web Services или ISO/IEC 27701:2019/ISO/IEC 27017:2015 по стандартам ISO; датацентры, сертифицированные гос-вом, в число которых входят linuxdatacenter, KeyPointGroup и т.д.; изоляция оборудования и широкий спектр сервисов для повышения уровня безопасности, такие как Amazon Macie.

Но, существует 5 основных направлений повышения безопасности в облачной среде, которые необходимо настроить:

1. Шифровка данных, т.е. нужно либо самостоятельно зашифровывать данные на компьютере, а затем пересылать их в облако. Так можно делать резервные копии каких-либо проектов. Либо если файлов много, можно использовать сервисы, которые шифруют данные до отправки в облако.
2. Мониторинг инфраструктуры, а именно блокирование несанкционированных соединений м/у рабочими процессами и предотвращение опасных запросов на подключение. Есть много продуктов для мониторинга, которые позволяют получить полное представление о сетевой активности: видеть всех, кто подключается к сети, и устанавливать правила для пользователей.
3. Ограничение доступа к данным, т.е. настройка контроля доступа в зависимости от роли. В такой системе пользователи не могут передавать права на доступ к информации другим пользователям. Эта модель основана на идентификации пользователей при помощи логина. Когда пользователь залогинен, ему автоматически назначаются роли и решения.
4. Настройка резервного копирования данных. Например, предприятия, использующие облако по модели IaaS, могут пользоваться интерфейсами прикладных систем (API), которые предоставляют облачные провайдеры, для разработки собственного ПО для резервного копирования, или сторонним ПО для резервного копирования на локальные серверы, например, в сетевое хранилище.
5. Разработка плана аварийного восстановления. В случае взлома или утери данных, при наличии площадки оборудованной и обслуживаемой также как основная желательно в другом районе или городе, можно перенести данные туда. А затраты времени и ресурсов на восстановление прежней не пойдут в ущерб работы облака.