Multi-Tenancy in Security

Albert B. Kirby

Florida State College at Jacksonville

Multi-Tenancy as I understand it is the sharing of resources usually via the cloud. Multiple consumers and organizations share the same resources and software services. In this environment a lot more dependence on security is required usually entailing multiple layers. Due to the nature of the cloud audits are not always allowed especially if you are using a commercial cloud because most commercial solutions have data from multiple companies and do not want their customer’s data to be breached or accessed by unauthorized users.

Many of the security risks involved are inadequate logical security controls, malicious or ignorant tenants, shared services can become a single point of failure, uncoordinated change controls and misconfigurations, co-mingled tenant data, performance risks, and XaaS specific risks are the most common. There are countermeasures available such as architecting for multi-tenancy, data encryption, controlled change management, transparency and audit ability of administrative access, virtual private cloud, third party assessments, and tenant isolation.

The risks involved are plentiful and this list is by no means a full list of all possible risks as the risks in cyber security are forever evolving and changing without warning. Logical security controls involve having the steps in place so that users can not interfere with each other’s resources meaning if user 1 is using a certain block of RAM then user 2 will not be allowed to edit or manipulate this data. Malicious or ignorant tenants is an example that builds on the last point if the correct controls are not in place and the data from user 1 is overwritten by user 2 that would make the data unusable for user one this often happens by mistake as the separate users are usually unaware they are sharing resources. Most clouds are tailored to individual users to give them the impression they are the only one using this service so they are usually unaware fo other users on the same hardware that they are sharing services with. Shared services can become a single point of failure if the common services are not architected correctly they can become a single point of failure usually caused by accident or misuse in example a user tries to update a particular service but fails during the update that renders the installation broken and other users are no longer able to use or access this service. Uncoordinated change controls and misconfigurations if changes are made to the structure of the cloud without prior knowledge given to other users it have negative repercussions on users that share that particular service. Co-Mingled tenant data means that hosts are storing data for multiple users in the same database or backup files causing confusion as to who’s data is where if users 1, 2, and 3 are all stored in the same partition it can be difficult to find the correct users files when requested and may even inadvertently result if incorrect data shared. Performance risks if one user is hogging resources other user’s performance will be diminished by this particular users over reaching use of services and resources. XaaS specific risks are risks involved in particular services. SaaS means that users may be sharing the same application stack and their data may be backed up and archived together correct use of logical security can mitigate this risk. PaaS specific risks mean the platform stack is shared among the tenants and vulnerabilities in the stack whether known or unknown can cause bleeding between users. IaaS is using cross virtual machines these machines often go long periods of time without being hardened or patched and often have very basic password structures that may be shared among users making things much easier for potential attackers.

There are countermeasures that can be put in place to mitigate risks and keep them to a minimum much like the risks this list is in no way all-inclusive and is ever changing. Architecting for multi-tenancy is necessary and providers should understand that segregation and strengthened common services are very important and they should make these things apparent to their subscribers. Data encryption is very important in keeping your data separate from other users. If you know me you know I’m a big advocate for encryption and recommend it for everyone. Since most clouds are shared environments it is very important that you encrypt you data to keep other users from accidentally accessing your data, in the event another user accesses your data if it is encrypted it is useless to them without the encryption key. Controlled change management involves feathering the release cycles of patches and upgrades to the structure. Providers should have a clear plan accessible to all their subscribers of how and when they will be doing patches or updates. Transparency/audit-ability of administrative access lets users know they have knowledge of administrative access to all of their resources and services. Virtual private cloud is a private cloud within a shared or public cloud. This gives you greater control of your experience and allows you to run in a quarantined environment. Third party assessments involve bringing in a third party or client to assess the viability and set up of your cloud infrastructure. Tenant isolation involves isolating your data from that of other users it does come with increased cost but is well worth it in the long run

In closing I would like to say that security is possible in a cloud environment but is in no way all-inclusive or by any means perfect. With time and the ever evolving of the internet new risks will be discovered and new methods of mitigating and reducing these risks must and will be found

References:

Phil Wainewright (March 18, 2010) http://www.zdnet.com/article/security-risks-of-multi-tenancy/

Unknown Author. <https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security>

Larry Bourgeois (March 9, 2011) http://www.asigra.com/blog/what-multi-tenancy-how-secure-it