Why you cannot ignore a layered approach in cloud security

YASSER ZEINELDIN
TREND TRACKER

THE MOVEMENT OF APPLICATIONS and data to the cloud needs to be balanced by an equivalent investment into security solutions to protect those assets now being used from the cloud.

The lack of understanding of the importance of security in the cloud can be linked to going away for a vacation and entrusting the keys with a stranger. Any movement towards usage of applications and storing of data in the cloud needs to be balanced, by an equivalent investment in security solutions supporting that movement.

The more critical the system infrastructure, data folders and business workloads being moved from on-premises to in-cloud, the more rigorous should be the security evaluation required to protect data through encryption and end-user access to applications.

By default, cloud service providers tend to roll out shared security responsibility models around user access for their services. Budgeting for security in the cloud by end-users, starts by considering which applications and infrastructure elements will be hosted in the cloud. In a software-as-a-service (SaaS) model, the cloud provider will usually guarantee the integrity and scalability of the hosted application, ensuring that there are seldom workload failures. However, end-users need to opt for securing user identity and user access to applications in the public cloud, as well as data encryption, through their own additional investments. For infrastructure-as-a-service (IaaS), almost the entire security environment is left to the management of the end-user.

Such investments must be sufficient to ensure that security standards in the cloud are compliant with the organisation's security policy, and also at par with those implemented on-premises. Global research surveys indicate that data breaches from the cloud remain the biggest concerns for end-users migrating to SaaS or IaaS.

'Swiss-cheese' approach

A layered security approach uses multiple, different, security controls to protect underlying data and applications in the cloud from malicious threats. A layered approach is also part of a military strategy to slow down attackers, since they have to penetrate multiple and successive layers of defense. A layered security approach is also similar to a 'swiss-cheese' model of defence.

In the swiss-cheese model, each layer of cheese may have holes distributed in random across their surfaces. If each layer of cheese was the same, the holes would line up. But if the layers of cheese are different, each layer of cheese presents a varied distribution of holes, that when stacked on top of each other, do not line up. Almost, a perfect barrier.

Much like the swiss-cheese model, a layered security approach, uses best of breed security solutions, from multiple vendors. When used in a consecutive fashion in layers, to fortify networks, applications, and data, a layered stack of solutions can offer a respectable defence in the cloud.

The swiss-cheese layer model attempts to protect weaknesses in the security layer above, by not having the same weaknesses within or in subsequent layers, rather having stronger protection in the corresponding positions where a weakness exists above. While sounding relatively straight forward in description, the swiss-cheese model does have its limitations unless implemented in a diligent fashion.

If the approach of layering security solutions from multiple vendors is followed in an ad-hoc fashion and the various solutions are incompatible with each other, this may lead to more complexity and continuing weaknesses. And in essence, the swiss-cheese defence layer will fail. Using multiple solutions from a single vendor, on the other hand, improves interoperability and may offer a significant cost benefit.

The best of breed approach, as a third alternative, is an attempted combination of the best of both worlds. This includes the best security solutions available for each layer, that are interoperable, cost-effective and fit into a holistic organisational security strategy and security policy. Implementing the swiss-cheese model does require operational planning and user training.

Cloud security

The swiss-cheese layers required to secure a cloud platform can be categorised into three areas:

System security: This is typically securing the infrastructure plumbing including operating systems, networks, virtual machines, management dashboards, utilities and containers. Service providers that automatically apply patches and make updates are preferable since they are helping end-users to secure their environments. This is mostly applicable to infrastructure as a service and platform as a service.

Application security: This is about enabling the IT department to limit the extent to which end users can use a cloud application, without following the organisation's access and security policies. Once the IT department has visibility into user behaviour through policies, the next step is to apply multi-factor authentication and identity management. Multi-factor authentication uses multiple devices or applications to verify the status and presence of the end-user.

Identity management creates a single-user sign-on, thereby securing the access of any end user, as well as applying the policies of the organisation, to any cloud-based login. A virtual private network connection helps to secure access to any cloud login. All these measures help the IT organisation to gain control over user behaviour and not rely on the cloud service provider for this level of security.

> Data breaches from the cloud remain the biggest concerns for end-users migrating to software-as-a-service or infrastructure-as-a-service

Data security: Cloud service providers are not responsible for the security of the data generated by the end-user through usage of cloud applications. End user data saved in the cloud needs to be encrypted and moreover, the keys for the encryption need to be available with the IT organisation. While moving data back and forth from the cloud, the data should remain encrypted during transfer.

In summary, cloud security is not an afterthought. It is well built into the original security policy and is an extension of the on-premises, security policies into cloud based, application workloads and data creation.

Since the stakes around cloud security are high, the responsibility needs to be shared between the cloud services provider and the end user organisation. A well-prepared, service level agreement will go a long way towards ensuring this important goal.

The writer is CEO of eHosting DataFort. Views expressed are his own and do not reflect the newspaper's policy.