Cloud Hardening

Network security in the cloud

In recent years, many organizations are using network services in the cloud.
So in addition to securing on-premises networks,
a security analyst will need to secure cloud networks.
In a previous video, you learned that a cloud network is a collection of
servers or computers that stores resources and
data in a remote data center that can be accessed via the internet.
They can host company data and applications using cloud computing to
provide on-demand storage, processing power, and data analytics.
Just like regular web servers, cloud servers also require proper maintenance
done through various security hardening procedures.
Although cloud servers are hosted by a cloud service provider,
these providers cannot prevent intrusions in the
cloud—especially intrusions from malicious actors, both internal and
external to an organization.

One distinction between cloud network hardening and
traditional network hardening is the use of a server baseline image for
all server instances stored in the cloud.
This allows you to compare data in the cloud servers to the baseline image to
make sure there haven't been any unverified changes.
An unverified change could come from an intrusion in the cloud network.
Similar to OS hardening, data and applications on a cloud network are kept
separate depending on their service category.
For example, older applications should be kept separate from newer applications,
and software that deals with internal functions should be kept separate
from front-end applications seen by users.

Even though the cloud service provider has a shared responsibility with
the organization using their services, there are still security measures that
need to be taken by the organization to make sure their cloud network is safe.
Just like traditional networks, operations in the cloud need to be secured.
You're doing great! Meet you in the next video.

secure the cloud

Earlier in this course, you were introduced to cloud computing

Cloud computing is a model for allowing convenient and on-demand network access to a shared pool of configurable computing resources. These resources can be configured and released with minimal management effort or interaction with the service provider.

Just like any other IT infrastructure, a cloud infrastructure needs to be secured. This reading will address some main security considerations that are unique to the cloud and introduce you to the shared responsibility model used for security in the cloud. Many organizations that use cloud resources and infrastructure express concerns about the privacy of their data and resources. This concern is addressed through cryptography and other additional security measures, which will be discussed later in this course.

Cloud security considerations

Many organizations choose to use cloud services because of the ease of deployment, speed of deployment, cost savings, and scalability of these options. Cloud computing presents unique security challenges that cybersecurity analysts need to be aware of.

Identity access management

Identity access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. This service also authorizes how users can use different cloud resources. A common problem that organizations face when using the cloud is the loose configuration of cloud user roles. An improperly configured user role increases risk by allowing unauthorized users to have access to critical cloud operations.

Configuration

The number of available cloud services adds complexity to the network. Each service must be carefully configured to meet security and compliance requirements. This presents a particular challenge when organizations perform an initial migration into the cloud. When this change occurs on their network, they must ensure that every process moved into the cloud has been configured correctly. If network administrators and architects are not meticulous in correctly configuring the organization’s cloud services, they could leave the network open to compromise. Misconfigured cloud services are a common source of cloud security issues.

Attack surface

Cloud service providers (CSPs) offer numerous applications and services for organizations at a low cost.

Every service or application on a network carries its own set of risks and vulnerabilities and increases an organization's overall attack surface. An increased attack surface must be compensated for with increased security measures.

Cloud networks that utilize many services introduce lots of entry points into an organization's network. However, if the network is designed correctly, utilizing several services does not introduce more entry points into an organization's network design. These entry points can be used to introduce malware onto the network and pose other security vulnerabilities. It is important to note that CSPs often defer to more secure options, and have undergone more scrutiny than a traditional on-premises network.

Zero-day attacks

Zero-day attacks are an important security consideration for organizations using cloud or traditional on-premise network solutions. A **zero day** attack is an exploit that was previously unknown. CSPs are more likely to know about a zero day attack occurring before a traditional IT organization does. CSPs have ways of patching hypervisors and migrating workloads to other virtual machines. These methods ensure the customers are not impacted by the attack. There are also several tools available for patching at the operating system level that organizations can use.

Visibility and tracking

Network administrators have access to every data packet crossing the network with both on-premise and cloud networks. They can sniff and inspect data packets to learn about network performance or to check for possible threats and attacks.

This kind of visibility is also offered in the cloud through flow logs and tools, such as packet mirroring. CSPs take responsibility for security in the cloud, but they do not allow the organizations that use their infrastructure to monitor traffic on the CSP's servers. Many CSPs offer strong security measures to protect their infrastructure. Still, this situation might be a concern for organizations that are accustomed to having full access to their network and operations. CSPs pay for third-party audits to verify how secure a cloud network is and identify potential vulnerabilities. The audits can help organizations identify whether any vulnerabilities originate from on-premise infrastructure and if there are any compliance lapses from their CSP.

Things change fast in the cloud

CSPs are large organizations that work hard to stay up-to-date with technology advancements. For organizations that are used to being in control of any adjustments made to their network, this can be a potential challenge to keep up with. Cloud service updates can affect security considerations for the organizations using them. For example, connection configurations might need to be changed based on the CSP's updates.

Organizations that use CSPs usually have to update their IT processes. It is possible for organizations to continue following established best practices for changes, configurations, and other security considerations. However, an organization might have to adopt a different approach in a way that aligns with changes made by the CSP.

Cloud networking offers various options that might appear attractive to a small company—options that they could never afford to build on their own premises. However, it is important to consider that each service adds complexity to the security profile of the organization, and they will need security personnel to monitor all of the cloud services.

Shared responsibility model

A commonly accepted cloud security principle is the shared responsibility model. The **shared responsibility model** states that the CSP must take responsibility for security involving the cloud infrastructure, including physical data centers, hypervisors, and host operating systems. The company using the cloud service is responsible for the assets and processes that they store or operate in the cloud.

The shared responsibility model ensures that both the CSP and the users agree about where their responsibility for security begins and ends. A problem occurs when organizations assume that the CSP is taking care of security that they have not taken responsibility for. One example of this is cloud applications and configurations. The CSP takes responsibility for securing the cloud, but it is the organization’s responsibility to ensure that services are configured properly according to the security requirements of their organization.

Key takeaways

It is essential to know the security considerations that are unique to the cloud and understanding the shared responsibility model for cloud security. Organizations are responsible for correctly configuring and maintaining best security practices for their cloud services. The shared responsibility model ensures that both the CSP and users agree about what the organization is responsible for and what the CSP is responsible for when securing the cloud infrastructure.

Revision #2
Created 2023-07-03 10:26:56 UTC by naruzkurai
Updated 2023-07-03 12:16:31 UTC by naruzkurai