Security hardning

- temp
- Introduction to security hardening
- OS hardening practices
- Brute force attacks and OS hardening
- Network hardening practices
- Network security applications
- Kelsey: Cloud security explained
- Security hardening Wrap-up & Glossary terms from week 4
- Cloud Hardening

temp

things to review

1. On-path attack
2. Distributed denial of service attack (DDoS)
3. Denial of service attack (DoS)
4. SYN flood attack
5. IP spoofing
6. Packet sniffing

Introduction to security hardening

I want to take a moment to congratulate you on your progress so far.
First, you learned about network operations.
Then, you learned about the tools and
protocols that help network systems function.
Next, you learned how vulnerabilities in
networks expose them to various security intrusions.

Now, we'll discuss security hardening.
Then, we'll learn about OS hardening, explore network hardening practices, and discuss cloud hardening practices.
Security hardening can be implemented in devices, networks,
applications, and cloud infrastructure.
Security analysts may perform tasks, such as patch updates and
backups, as part of security hardening.

We'll discuss these tasks as you progress through the course.
As a security analyst, hardening will play a major role in your day-to-day tasks,
which is why it's important for you to understand how it works.
I'm excited to accompany you on this journey.

Security hardening

Security analysts and the organizations they work with have to be
proactive about protecting systems from attack.
This is where security hardening comes in.
Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface.
All the potential vulnerabilities that a threat actor could exploit
are referred to as a system's attack surface.

Let's use an example that compares a network to a house.
The attack surface would be all the doors and
windows that a robber could use to gain access to that house.
Just like putting locks on all the doors and windows in the house,
security hardening involves minimizing the attack surface or
potential vulnerabilities and keeping a network as secure as possible.

As part of security hardening, security analysts perform regular maintenance procedures to keep network devices and systems functioning securely and optimally.
Security hardening can be conducted on any device or system that can be compromised, such as hardware, operating systems, applications, computer networks, and databases.
Physical security is also a part of security hardening.
This may include securing a physical space with security cameras and security guards.

Some common types of hardening procedures include software updates, also called patches, and device application configuration changes.
These updates and changes are done to increase security and fix security vulnerabilities on a network.
An example of a security configuration change would be requiring longer passwords or more frequent password changes.
This makes it harder for a malicious actor to gain login credentials.
An example of a configuration check is updating the encryption standards for data that is stored in a database.
Keeping encryption up to date makes it harder for malicious actors to access the database.

Other examples of security hardening include removing or disabling unused applications and services, disabling unused ports, and reducing access permissions across devices and network.
Minimizing the number of applications, devices, ports, and access permissions makes network and device monitoring more efficient and reduces the overall attack surface, which is one of the best ways to secure an organization.

Another important strategy for security hardening is to conduct regular penetration testing.
A penetration test, also called a pen test, is a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process.
Penetration testers document their findings in a report.
Depending on where the test fails, security teams can determine the type of security vulnerabilities that require fixing.
Organizations can then review these vulnerabilities and come up with a plan to fix them.

Coming up, you'll learn more about how security hardening is an essential aspect of securing networks.
It's a foundational part of network security that strengthens the network in order to reduce the number of successful attacks.

OS hardening practices

Hi there. In this video,
we'll discuss operating system, or OS, hardening and why it's
essential to keep the entire network secure.
The operating system is the interface between computer hardware and the user.
The OS is the first program loaded when a computer turns on.
The OS acts as an intermediary between software applications and the computer hardware.
It's important to secure the OS in each system because one insecure OS can
lead to a whole network being compromised.
There are many types of operating systems, and they all share similar security hardening practices.
Let's talk about some of those security hardening practices that are recommended to secure an OS.

Some OS hardening tasks are performed at regular intervals, like updates, backups, and keeping an up-to-date list of devices and authorized users.
Other tasks are performed only once as part of preliminary safety measures.
One example would be configuring a device setting to fit a secure encryption standard.
Let's begin with OS hardening tasks
that are performed at a regular interval, such as patch installation, also known as patch updates.

A patch update is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product.
Now we'll discuss patch updates provided to the company by the OS software vendor.
With patch updates, the OS should be upgraded to its latest software version.
Sometimes patches are released to fix a security vulnerability in the software.
As soon as OS vendors publish a patch and the vulnerability fix, malicious actors know exactly where the vulnerability is in systems
running the out-of-date OS.
This is why it's important for organizations to run patch updates as soon as they are released.
For example, my team had to perform an emergency patch to address a recent vulnerability found in a commonly used programming library.
The library is used almost everywhere, so we had to quickly patch most of our servers and applications to fix the vulnerability.
The newly updated OS should be added to the baseline configuration, also called the baseline image.
A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds,
releases, and updates.
For example, a baseline may contain a firewall rule with a list of allowed and disallowed network ports. If a security team suspects
unusual activity affecting the OS, they can compare the current configuration to the baseline and make sure that nothing has been changed.

Another hardening task performed regularly is hardware and software disposal.
This ensures that all old hardware is properly wiped and disposed of.
It's also a good idea to delete any unused software applications since some popular programming languages
have known vulnerabilities.
Removing unused software makes sure that there aren't any unnecessary vulnerabilities connected with the programs that the software uses.

The final OS hardening technique that we'll discuss is implementing a strong password policy.
Strong password policies require that passwords follow specific rules.
For example, an organization may set a password policy that requires a minimum of eight characters,
a capital letter, a number, and a symbol.
To discourage malicious actors, a password policy usually states that a user will lose access to the network after entering the wrong password a certain number of times in a row.
Some systems also require multi-factor authentication, or MFA.
MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network.
Ways of identifying yourself include something you know, like a password, something you have like an ID card, or something unique about you, like your fingerprint.

To review, OS hardening is a set of procedures that maintains OS security and improves it.
Security measures like access privileges and password policies frequently undergo regular security checks as part of OS hardening.
Coming up, we'll discuss network hardening practices.

Brute force attacks and OS hardening

In this reading, you'll learn about brute force attacks. You'll consider how vulnerabilities can be assessed using virtual machines and sandboxes, and learn ways to prevent brute force attacks using a combination of authentication measures. Implementing various OS hardening tasks can help prevent brute force attacks. An attacker can use a brute force attack to gain access and compromise a network.

Usernames and passwords are among the most common and important security controls in place today. They are used and enforced on everything that stores or accesses sensitive or private information, like personal phones, computers, and restricted applications within an organization. However, a major issue with relying on login credentials as a critical line of defense is that they're vulnerable to being stolen and guessed by malicious actors.

Brute force attacks

A **brute force attack** is a trial-and-error process of discovering private information. There are different types of brute force attacks that malicious actors use to guess passwords, including:

- *Simple brute force attacks.* When attackers try to guess a user's login credentials, it's considered a simple brute force attack. They might do this by entering any combination of usernames and passwords that they can think of until they find the one that works.
- *Dictionary attacks* use a similar technique. In dictionary attacks, attackers use a list of commonly used passwords and stolen credentials from previous breaches to access a system. These are called "dictionary" attacks because attackers originally used a list of words from the dictionary to guess the passwords, before complex password rules became a common security practice.

Using brute force to access a system can be a tedious and time consuming process, especially when it's done manually. There are a range of tools attackers use to conduct their attacks.

Assessing vulnerabilities

Before a brute force attack or other cybersecurity incident occurs, companies can run a series of tests on their network or web applications to assess vulnerabilities. Analysts can use virtual machines and sandboxes to test suspicious files, check for vulnerabilities before an event occurs,

or to simulate a cybersecurity incident.

Virtual machines (VMs)

Virtual machines (VMs) are software versions of physical computers. VMs provide an additional layer of security for an organization because they can be used to run code in an isolated environment, preventing malicious code from affecting the rest of the computer or system. VMs can also be deleted and replaced by a pristine image after testing malware.

VMs are useful when investigating potentially infected machines or running malware in a constrained environment. Using a VM may prevent damage to your system in the event its tools are used improperly. VMs also give you the ability to revert to a previous state. However, there are still some risks involved with VMs. There’s still a small risk that a malicious program can escape virtualization and access the host machine.

You can test and explore applications easily with VMs, and it’s easy to switch between different VMs from your computer. This can also help in streamlining many security tasks.

Sandbox environments

A sandbox is a type of testing environment that allows you to execute software or programs separate from your network. They are commonly used for testing patches, identifying and addressing bugs, or detecting cybersecurity vulnerabilities. Sandboxes can also be used to evaluate suspicious software, evaluate files containing malicious code, and simulate attack scenarios.

Sandboxes can be stand-alone physical computers that are not connected to a network; however, it is often more time- and cost-effective to use software or cloud-based virtual machines as sandbox environments. Note that some malware authors know how to write code to detect if the malware is executed in a VM or sandbox environment. Attackers can program their malware to behave as harmless software when run inside these types of testing environments.

Prevention measures

Some common measures organizations use to prevent brute force attacks and similar attacks from occurring include:

- **Salting and hashing:** Hashing converts information into a unique value that can then be used to determine its integrity. It is a one-way function, meaning it is impossible to decrypt and obtain the original text. Salting adds random characters to hashed passwords. This increases the length and complexity of hash values, making them more

secure.

- **Multi-factor authentication (MFA) and two-factor authentication (2FA):** MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. 2FA is similar to MFA, except it uses only two forms of verification.
- **CAPTCHA and reCAPTCHA:** CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart. It asks users to complete a simple test that proves they are human. This helps prevent software from trying to brute force a password. reCAPTCHA is a free CAPTCHA service from Google that helps protect websites from bots and malicious software.
- **Password policies:** Organizations use password policies to standardize good password practices throughout the business. Policies can include guidelines on how complex a password should be, how often users need to update passwords, and if there are limits to how many times a user can attempt to log in before their account is suspended.

Key takeaways

Brute force attacks are a trial-and-error process of guessing passwords. Attacks can be launched manually or through software tools. Methods include simple brute force attacks and dictionary attacks. To protect against brute force attacks, cybersecurity analysts can use sandboxes to test suspicious files, check for vulnerabilities, or to simulate real attacks and virtual machines to conduct vulnerability tests. Some common measures to prevent brute force attacks include: hashing and salting, MFA and/or 2FA, CAPTCHA and reCAPTCHA, and password policies.

Network hardening practices

Earlier, you learned that OS hardening focuses on device safety and uses patch updates, secure configuration, and account access policies.
Now we'll focus on network hardening.
Network hardening focuses on network-related security hardening, like port filtering, network access privileges, and encryption over networks.
Certain network hardening tasks are performed regularly, while others are performed once and then updated as needed.

Some tasks that are regularly performed are firewall rules maintenance, network log analysis, patch updates, and server backups.
Earlier, you learned that a log is a record of events that occurs within an organization's systems.
Network log analysis is the process of examining network logs to identify events of interest.
Security teams use a log analyzer tool or a security information and event management tool, also known as a SIEM, to conduct network log analysis.
A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization.
It gathers security data from a network and presents that data on a single dashboard.
The dashboard interface is sometimes called a single pane of glass.
A SIEM helps analysts to inspect, analyze, and react to security events across the network based on their priority.
Reports from the SIEM provide a list of new or ongoing network vulnerabilities and list them on a scale of priority from high to low, where high priority vulnerabilities have a much shorter deadline for mitigation.

Now that we've covered tasks that are performed regularly, let's examine tasks that are performed once.
These tasks include port filtering on firewalls, network access privileges, and encryption for communication, among many things.
Let's start with port filtering.
Port filtering can be formed over the network.
Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication.
A basic principle is that the only ports that are needed are the ones that are allowed.
Any port that isn't being used by the normal network operations should be disallowed.
This protects against port vulnerabilities.
Networks should be set up with the most up-to-date wireless protocols available and older wireless protocols should be disabled.
Security analysts also use network segmentation to create isolated subnets for different departments in an organization.
For example, they might make one for the marketing department and one for the finance department.

This is done so the issues in each subnet don't spread across the whole company and only specified users are given access to the part of the network that they require for their role.
Network segmentation may also be used to separate different security zones.
Any restricted zone on a network containing highly classified or confidential data should be separate from the rest of the network.
Lastly, all network communication should be
encrypted using the latest encryption standards.
Encryption standards are rules or methods used to conceal outgoing data and uncover or decrypt incoming data.
Data in restricted zones should have much higher encryption standards, which makes them more difficult to access.
You've learned about the most common hardening practices.
This knowledge will be useful as you complete the certificate program and it's essential to your career as a security analyst.

Network security applications

This section of the course covers the topic of network hardening and monitoring. Each device, tool, or security strategy put in place by security analysts further protects—or hardens—the network until the network owner is satisfied with the level of security. This approach of adding layers of security to a network is referred to as defense in depth.

In this reading, you are going to learn about the role of four devices used to secure a network—firewalls, intrusion detection systems, intrusion prevention systems, and security incident and event management tools. Network security professionals have the choice to use any or all of these devices and tools depending on the level of security that they hope to achieve.

This reading will discuss the benefits of layered security. Each tool mentioned is an additional layer of defense that can incrementally harden a network, starting with the minimum level of security (provided by just a firewall), to the highest level of security (provided by combining a firewall, an intrusion detection and prevention device, and security event monitoring).

An image showing the differences between a firewall, IPS, and IDS.

Take note of where each tool is located on the network. Each tool has its own place in the network's architecture. Security analysts are required to understand the network topologies shown in the diagrams throughout this reading.

Firewall

So far in this course, you learned about stateless firewalls, stateful firewalls, and next-generation firewalls (NGFWs), and the security advantages of each of them.

Most firewalls are similar in their basic functions. Firewalls allow or block traffic based on a set of rules. As data packets enter a network, the packet header is inspected and allowed or denied based on its port number. NGFWs are also able to inspect packet payloads. Each system should have its own firewall, regardless of the network firewall.

A firewall circled by dashes, protecting the internal network from internet traffic that comes in

Intrusion Detection System

An **intrusion detection system** (IDS) is an application that monitors system activity and alerts on possible intrusions. An IDS alerts administrators based on the signature of malicious traffic.

The IDS is configured to detect known attacks. IDS systems often sniff data packets as they move across the network and analyze them for the characteristics of known attacks. Some IDS systems review not only for signatures of known attacks, but also for anomalies that could be the sign of malicious activity. When the IDS discovers an anomaly, it sends an alert to the network administrator who can then investigate further.

The limitations to IDS systems are that they can only scan for known attacks or obvious anomalies. New and sophisticated attacks might not be caught. The other limitation is that the IDS doesn't actually stop the incoming traffic if it detects something awry. It's up to the network administrator to catch the malicious activity before it does anything damaging to the network.

An IDS circled above an image of a switch, which rests between a firewall and the network.

When combined with a firewall, an IDS adds another layer of defense. The IDS is placed behind the firewall and before entering the LAN, which allows the IDS to analyze data streams after network traffic that is disallowed by the firewall has been filtered out. This is done to reduce noise in IDS alerts, also referred to as false positives.

Intrusion Prevention System

An **intrusion prevention system (IPS)** is an application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected, unlike the IDS that simply reports the anomaly to a network administrator.

An IPS searches for signatures of known attacks and data anomalies. An IPS reports the anomaly to security analysts and blocks a specific sender or drops network packets that seem suspect.

An IPS is situated between a firewall and the internal network.

The IPS (like an IDS) sits behind the firewall in the network architecture. This offers a high level of security because risky data streams are disrupted before they even reach sensitive parts of the network. However, one potential limitation is that it is inline: If it breaks, the connection between the private network and the internet breaks. Another limitation of IPS is the possibility of false positives, which can result in legitimate traffic getting dropped.

Full packet capture devices

Full packet capture devices can be incredibly useful for network administrators and security professionals. These devices allow you to record and analyze all of the data that is transmitted over your network. They also aid in investigating alerts created by an IDS.

Security Information and Event Management

A **security information and event management system (SIEM)** is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools additionally analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. SIEM tools are a way to aggregate security event data so that it all appears in one place for security analysts to analyze. This is referred to as a single pane of glass.

Below, you can review an example of a dashboard from Google Cloud's SIEM tool, Chronicle. **Chronicle** is a cloud-native tool designed to retain, analyze, and search data.

Image of the Chronicle dashboard

Splunk is another common SIEM tool. Splunk offers different SIEM tool options: Splunk Enterprise and Splunk Cloud. Both options include detailed dashboards which help security professionals to review and analyze an organization's data. There are also other similar SIEM tools available, and it's important for security professionals to research the different tools to determine which one is most beneficial to the organization.

A SIEM tool doesn't replace the expertise of security analysts, or of the network- and system-hardening activities covered in this course, but they're used in combination with other security methods. Security analysts often work in a Security Operations Center (SOC) where they can monitor the activity across the network. They can then use their expertise and experience to determine how to respond to the information on the dashboard and decide when the events meet the criteria to be escalated to oversight.

Key takeaways

Devices / Tools	Advantages	Disadvantages
Firewall	A firewall allows or blocks traffic based on a set of rules.	A firewall is only able to filter packets based on information provided in the header of the packets.
Intrusion Detection System (IDS)	An IDS detects and alerts admins about possible intrusions, attacks, and other malicious traffic.	An IDS can only scan for known attacks or obvious anomalies; new and sophisticated attacks might not be caught. It doesn't actually stop the incoming traffic.

Devices / Tools	Advantages	Disadvantages
Intrusion Prevention System (IPS)	An IPS monitors system activity for intrusions and anomalies and takes action to stop them.	An IPS is an inline appliance. If it fails, the connection between the private network and the internet breaks. It might detect false positives and block legitimate traffic.
Security Information and Event Management (SIEM)	A SIEM tool collects and analyzes log data from multiple network machines. It aggregates security events for monitoring in a central dashboard.	A SIEM tool only reports on possible security issues. It does not take any actions to stop or prevent suspicious events.

Each of these devices or tools cost money to purchase, install, and maintain. An organization might need to hire additional personnel to monitor the security tools, as in the case of a SIEM. Decision-makers are tasked with selecting the appropriate level of security based on cost and risk to the organization. You will learn more about choosing levels of security later in the course.

Kelsey: Cloud security explained

I'm Kelsey, I'm a distinguished engineer at Google Cloud.
I work on compute platforms and security related topics.
When I was starting, the only jobs I had previous,
the only jobs I was confident were accessible to me were fast food jobs.
I wanted a career, I wanted more than just a job.
So when I zoomed out and asked myself, what were my career options?
I couldn't think of a better place in the year 1999 than going into the world
of technologies.
I mean, on the news people were lining up for the latest operating system.
All the tech people were the new rock stars.
And I remember flipping through the opening jobs or
the job openings in the classified section, and it said anyone that has one
of these certifications let us know because we're hiring.
The delta between getting started and
getting your first job into that career that I always wanted,
it was $35 away in a certification book.
So let's talk about Cloud.
So before the time of Cloud, most companies had their own data center.
Imagine it's just you alone in your house, you can put anything wherever you want.
You may choose to never lock the doors on the inside, it's just you.
And for a long time in our industry,
that's the way people ran their data centers.
Now, we just call that private Cloud, it's just you there.
But Cloud is public.
And so the analogy would be, imagine getting roommates,
now you start to think differently about your stuff.
You start to lock things up even while you're inside of the house, and
your security discipline is going to be very different.
As more and more companies move into Cloud.
You may just be the person who can help one of those organizations finally make
that leap because they have a professional on their team.
All right, so you've gotten the certification,
you've gotten the fundamental skills,
how do you make sure that you can actually use them in the Cloud?
I'm going to let you in a little secret.
Go use the Cloud.
Go take existing software, throw it in the Cloud, and
find all the tools that poke and prod at the thing you just got running and
it's going to tell you where you're weak.
Learn those tools, because those are the tools that the professionals use.
Learning is a superpower.

It gives you the ability to not only get that job that you've been looking at, but it also gives you the ability to define the next one.

Security hardening Wrap-up & Glossary terms from week 4

Great work on learning about security hardening!
Let's take a few minutes to wrap up what you've learned.

You learned about security hardening and its importance to an organization's infrastructure.
First, we discussed how security hardening strengthens systems and networks to reduce the likelihood of an attack.
Next, we covered the importance of OS hardening, including patch updates, baseline configurations,
and hardware and software disposal.
Then we explored network hardening practices, such as network log analysis and firewall rule maintenance.
Finally, we examined cloud network hardening and the responsibilities of both organizations and cloud service providers in maintaining security.

As a security analyst, you'll be working with operating systems, on-premise networks, and cloud networks.
You'll be using all the knowledge that we learned in this section in your career as a security analyst.

Terms and definitions from Course 3, Week 4

Baseline configuration (baseline image): A documented set of specifications within a system that is used as a basis for future builds, releases, and updates

Hardware: The physical components of a computer

Multi-factor authentication (MFA): A security measure which requires a user to verify their identity in two or more ways to access a system or network

Network log analysis: The process of examining network logs to identify events of interest

Operating system (OS): The interface between computer hardware and the user

Patch update: A software and operating system update that addresses security vulnerabilities within a program or product

Penetration testing (pen test): A simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes

Principle of least privilege: Access and authorization to information only last long enough to complete a task

Security hardening: The process of strengthening a system to reduce its vulnerabilities and attack surface

Security information and event management (SIEM): An application that collects and analyzes log data to monitors critical activities for an organization

World-writable file: A file that can be altered by anyone in the world

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.