FORTINET

The Security Risks and Challenges of Cloud Computing

Cloud Misconfigurations Lead to Security Gaps

Many security issues with cloud environments start at the beginning. The strategy for setting up cloud security differs from setting up protections for physical data centers. Cloud misconfigurations typically happen because of the following reasons:

- Security professionals lacking full awareness of all cloud security policies
- Too many untracked APIs
- Insiders not following protocols for cloud containers and other software

When the users tasked with cloud setup fail to secure every endpoint properly, it leads to openings for cyber thieves to steal, ransom, and sell data. For example, they could get into the web apps housed on the cloud server and install scripts that execute when users enter sensitive information. The captured data gets sent back to a server owned by the bad actors, which they sell or use as they wish.

The Clouds Adds to Security Risk

As more companies decide to use cloud services to improve efficiency and increase cost savings, hackers view them as avenues for exploitation. The security risks presented by cloud technology will only accelerate as organizations increase their adoption rate. For that reason, companies must look to new security techniques to protect their new infrastructure.

One big issue is the lack of control around who has access to essential components. Because one of the primary purposes of cloud infrastructure is to make it easier for companies to share and use information, it's harder for them to set up proper access controls. Users end up with unnecessary access they shouldn't have.

Additionally, internal security threats are the risks presented by shadow IT. Any user with a credit card can spin up a new instance and add it to their cloud real estate. Once an application gets deployed within a cloud environment, any untracked bugs or viruses could make their way in and start wreaking havoc. Without software that looks for potential threats, one could infect the entire system.

The Increase of Ransomware and Other Threats

The evolution of the threat landscape has led to more sophisticated cyberattacks involving ransomware. One survey notes that 67% of organizations fell victim to ransomware activity in December 2020.[1]

With ransomware, hackers can obtain access to a system in various ways without the need for keystrokes. The prevalence of ransomware has led to a need for companies to take note of the robustness of their current security infrastructure.

Ransomware is just one form of malware used by hackers to infiltrate organizations. If they manage to get malicious code into a company's cloud infrastructure, it could affect every application and process running in that space.

If companies don't track threats launched at different endpoints, like a vulnerable company workstation using a Software-as-a-Service (SaaS) product, the threat could repeat itself continuously until there is something in place to recognize the vulnerability.

Slow Response Time

A zero-day attack is when a hacker manages to locate and exploit a vulnerability present in a network or computer system before IT personnel can deploy a fix. Those kinds of attacks are even more damaging because they allow cyber thieves to work around traditional cyber defenses.

A report from Mandiant noted that hackers managed to exploit 80 zero-day opportunities in 2021, double that picked up on in 2019.[2] That shows a need for increased awareness throughout various industries about the need to detect and repair vulnerabilities before they fall victim to bad actors.

Another reason to worry is that cybercriminals often figure out how to find and exploit vulnerabilities faster than security professionals can develop, publish, and apply patches. The ability for hackers to move more quickly than most security professionals often means organizations don't realize there is a problem until a lot of time has passed.

The attacks can come from around the world. Many companies have had security vulnerabilities exploited by groups of hackers based in places like China and Russia. However, many work alone in their attempts to search out and take advantage of holes in the security layer of various organizations.

The Added Challenge of Hybrid-cloud Environments

One of the challenges of working in a hybrid-cloud environment is a lack of consistency in enforcing security. Part of that is because organizations may have limited visibility into public cloud providers. Because of that, many IT professionals end up using various cybersecurity products to address concerns around data security. However, improper configuration of these solutions or too much variation in their enforcement can lead to even more security issues.

In addition to the issues that crop up because of cloud misconfigurations, SaaS models add another layer of confusion. Privileged cloud accounts can still become vulnerable to attacks that compromise their credentials because of unprotected endpoints.

The tangled mass of solutions that emerges from trying to protect cloud and hybrid environments can make it harder to track down the source of a threat. When gaps appear, security professionals must wade into the morass to find the issue that could lead to a data breach.

Another problem with taking the patchwork approach to hybrid-cloud security is that it's harder for companies to enforce consistent protocols and practices.

Lack of Cloud Security Protocols

It only takes one developer downloading a bad image to put the entire company at risk. Or there's a lack of enforcement around allowing access to specific cloud infrastructure, making it easier for someone to inadvertently allow a hacker into a secure space.

These things happen because companies fail to set up robust security protocols around cloud infrastructure. That can result from businesses being overconfident in the ability of their security personnel to defend them against cyberattacks.

It was a failure to set up cybersecurity protections that led to the attack on gas company Colonial Pipeline in 2021. The ransomware left behind by hackers shut down company systems and led to backups in gasoline supply along the East Coast.

Too many companies continue to overlook the essentials of good security hygiene, like:

- Tracking, reporting on, and cutting off suspicious user activity
- Constantly scanning endpoints to pick up on repeated attempts to launch attacks
- Enacting timely patches of system, software, and network vulnerabilities

Without automatic monitoring of endpoints, organizations can't build a list of suspicious items to use as a starting point for cleaning up compromised instances.

Overwhelmed Security Operations Centers

Analysts working in security operations centers (SOCs) must sort through an ever-increasing mountain of data each day to try and locate potential threats. When they identify an issue, they must evaluate whether it is a genuine threat or a false alarm.

If it is a false positive, workers can get so used to alerts not amounting to anything that it numbs awareness of real danger. Getting it wrong can lead to catastrophic consequences for an organization. For that reason, many SOCs are turning to artificial intelligence (AI) to help them keep pace with evolving threats like distributed denial-of-service (DDoS) attacks and malware.

It only takes minutes for hackers to execute an advanced attack that compromises organizational endpoints. Older security tools can't keep up with the pace of growing cybersecurity dangers. The need to provide manual triage and response makes them too slow to deal with moving threats.

Because companies allow the use of various devices to connect to company systems, security professionals have even more endpoints to track. One improperly monitored tablet or cell phone could become a vehicle for an attack that locks up a company's cloud infrastructure.

Summary

Cloud computing comes with its benefits but also introduces security risks and challenges. Take stock of your security strategy to secure your cloud workloads. Solutions like secure access service edge (SASE) and zero-trust network access (ZTNA) bring part of that to the table but may not be able to close all of your security gaps. Look at add an EDR solution, which will be better at detecting and resolving a threat once it has bypassed the perimeter or likewise controls.

[1] "The 2021 Ransomware Survey Report," Fortinet, November 2021

[2] "Zero Tolerance: More Zero-Days Exploited in 2021 Than Ever Before," Mandiant, April 2021.