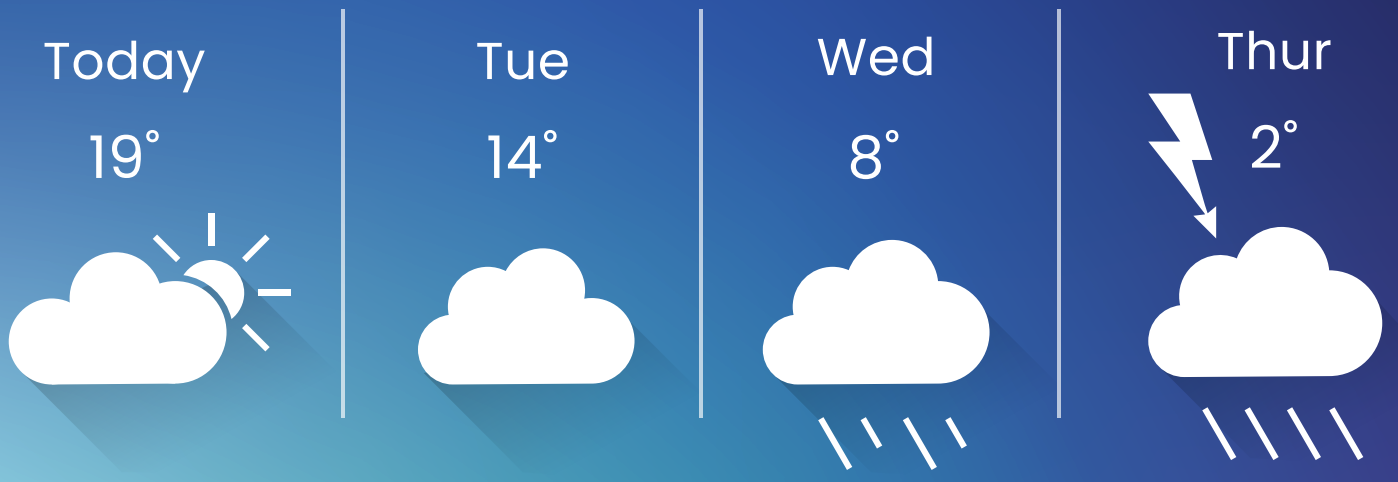
ISTARI Perspectives

Lessons from Cyberattacks on the Cloud: Implementing Cloud Native Security and Zero Trust

Cyberattacks on the cloud are becoming more frequent. Identifying and countering them requires a different toolkit and capabilities.

JD Sherry
Jim Reavis
Yotam Meitar

10 • 2023



Lessons from Cyberattacks on the Cloud: Implementing Cloud Native Security and Zero Trust

Cyberattacks on the cloud are becoming more frequent. Identifying and countering them requires a different toolkit and capabilities.

There was nothing unusual when an analyst in the security operations center of a large North American technology company received an alert of anomalous network behavior on one of the company's public-facing cloud servers. The cloud server had started to scan assets on the company's virtual private cloud. As is standard procedure, the analyst initiated an internal investigation, analyzing the server for signs of compromise. Although the network logs clearly indicated the scan had taken place, the investigation found no evidence of malicious tools or the execution of malevolent commands.

Yet, the sensitivity of the data hosted on the servers prompted the company to launch a comprehensive external investigation. The investigators discovered that the server had indeed been compromised, but the attackers were relying only on pre-existing cloud-native tools to navigate through the environment – without deploying malware or malicious tools. This finding allowed for a swift resolution of the malicious activity, but it raised a bigger concern for the company – how can attacks that use these cloud-native tools be effectively detected and remediated going forward?

Cloud environments are neither more nor less prone to cyberattacks compared to on-premises technology environments. But they are different, in three major ways. First, the perpetual online connectivity of cloud environments removes the necessity for attackers to wait for infected devices, like laptops, to be online to move laterally across networks.

Second, cloud environments are largely homogenous, allowing attackers to automate and re-use many of their tactics across their targets. Attackers only need minimal time to learn how to navigate different systems, swiftly adapting to exploit vulnerabilities.

And third, attackers can take advantage of native cloud applications that are already part of the cloud application suite. When targeting on-premises servers, attackers usually have to initiate a detectable connection to meet their goals, but cloud environments offer readily available mechanisms to execute code directly on them, requiring only credentials for the cloud environment.

In the case of the North American technology company, attackers had not just compromised one server – they had gained access to three sets of different credentials: login credentials to the cloud management console, credentials to access specific servers in the cloud, and application credentials to the sensitive databases.

The good news is that CISOs see cloud security as the number one priority, according to market research from ISTARI. The second highest priority for them is to embark on a zero trust journey. These two priorities are interrelated – a zero trust approach can play a significant part in mitigating the biggest vulnerability in many cloud environments: insufficient privileged identity management (according to CSA research).

Zero trust is an approach to security that removes implicit trust and enforces strict identity authentication and authorization to protect networks, applications and data, unlike the perimeter security mode. It is based on the idea of removing inherent trust from a network while continually verifying access to systems.[1]

It embraces the idea of least privilege access, meaning users are granted the lowest levels of permission required to carry out a specific task. Continual verification and authorization of each access to ensure the interaction meets security policies must also be carried out. It is an approach that often combines different tools and policies.

The case study on the American technology company and the many others who have experienced cloud attacks offers important lessons on how organizations can securely move from an on-premises environment to the cloud and operate securely in a hybrid environment.

1) Privileged Identity Management strategy should be the focus of attention, with least-privilege & zero trust at its core. The purpose of the privileged identity management strategy should be to understand access entitlements across cloud and multi-cloud environments and to remove higher levels of access than necessary. Even in well-managed cloud environments, implicit trust of legacy on-premises environment can be the Achilles heel, highlighting the need to combine effective cloud identity management with a comprehensive zero trust approach. A good starting point for an identity strategy is Cloud Infrastructure Entitlement Management (CIEM) tools that provide an overview of the cloud identity maturity.

2) Cyberattacks on cloud environments require cloud-native detection capabilities. A simple extension of on-premises security operation centers is often not sufficient to detect cloud attacks similar to the one that has impacted the North American technology company. Establishing cloud-specific detection capabilities that take into account the differing attack surfaces in cloud environments enables early detection and prevention of incidents or breaches.

3) Speed of detection and response is even more critical. Cloud environments are more homogenous compared to on-premises environments. That makes companies more efficient and unlocks automation opportunities, but it also enables attackers to use higher levels of automation to identify misconfigurations and carry out their attacks. In other words, attackers are using the benefits of the cloud to their own advantage. As a countermeasure, companies must invest in faster detection and response capabilities, leveraging automation for defensive response measures as well.

So, how did the attackers gain access to the three sets of cloud credentials in the case of the North American technology company? In their analysis, investigators identified a single code repository in GitHub, an online service for software development and to store computer code, containing all three credentials. A closer look at this repository revealed that the company's programmers had accidentally made the repository publicly available. The code was only visible publicly for 30 minutes before being taken down, but it was long enough for cyber criminals to find and exploit the sensitive credentials.

About the authors:

JD Sherry

JD Sherry is a Client Partner at ISTARI serving the Americas region, and a member of the supervisory board at Sonrai. For nearly three decades, JD Sherry has established himself as a trusted senior advisor for the protection of Payment Card Industry (PCI), Health Information Privacy Act (HIPAA) and Personally Identifiable Information (PII) data, offering strategic consulting at the c-level and board level.

Jim Reavis

Jim Reavis is the CEO at Cloud Security Alliance. For many years, Jim has worked in the information security industry as an entrepreneur, writer, speaker, technologist and business strategist. Jim's innovative thinking about emerging security trends have been published and presented widely throughout the industry and have influenced many.

Yotam Meitar

Yotam Meitar works as Director of Incident Response at Sygnia, an elite cyber technology company providing high-end consulting and incident response support for top organizations worldwide, including Fortune 500 companies.

[1]The Cloud Security Alliance provides resources in their Zero Trust Advancement Center, including Zero Trust research, professional training and webinar series.