IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Data Centre and Virtualization

Cloud Misconfigurations – A Greater Threat Than One Might Think

Assaf Morag

Assaf Morag
Lead Data Analyst
Team Nautilus
Aqua Security

Biography

Assaf Morag s a Lead Data Analyst at Aqua Security (https://www.aquasec.com). As part of Aqua's research group – Team Nautilus – his work focuses on supporting the diverse data needs of the team.

He has previously served as Chief Cyber Threat Intelligence Analyst at BlueVoyant and Web Fraud Team Leader at IBM.

Assaf is an alumnus of the prestigious Tel Aviv University. As part of Aqua's research group – Team Nautilus – his work focuses on supporting the diverse data needs of the team.

Assaf blogs at https://blog.aquasec.com/

Keywords **Cloud native, Security, Misconfigurations, Cyber attack, Docker, Shift-left testing**
Paper type Research

Abstract

New research from Team Nautilus revealing that a significant majority of companies that move to multi-cloud environments are not properly configuring their cloud-based services. According to new findings from Aqua's '2021 Cloud Security Report: Cloud Configuration Risks Exposed', these misconfigurations, for example leaving bucket or blog storage open, can open companies up to critical security breaches. Even when companies are aware of errors, most have not addressed the bulk of these issues in a timely manner – especially larger enterprises who are taking an average of 88 days to address issues after discovery. In this article the author explains why failing to address misconfiguration issues comes with serious consequences which are all too real to ignore.

Introduction

As cloud native technologies have matured, they have become cheaper, more widely available and most importantly, far easier to use. This confluence of factors has led to a significant rise in the adoption of cloud approaches by businesses in all sectors and of all sizes. In fact, IDC has forecast[1] that at least 500 million digital apps and services will be both developed and deployed using a cloud native approach in the next two years.

IT for CEOs & CFOs is published by House of Words Media Limited.

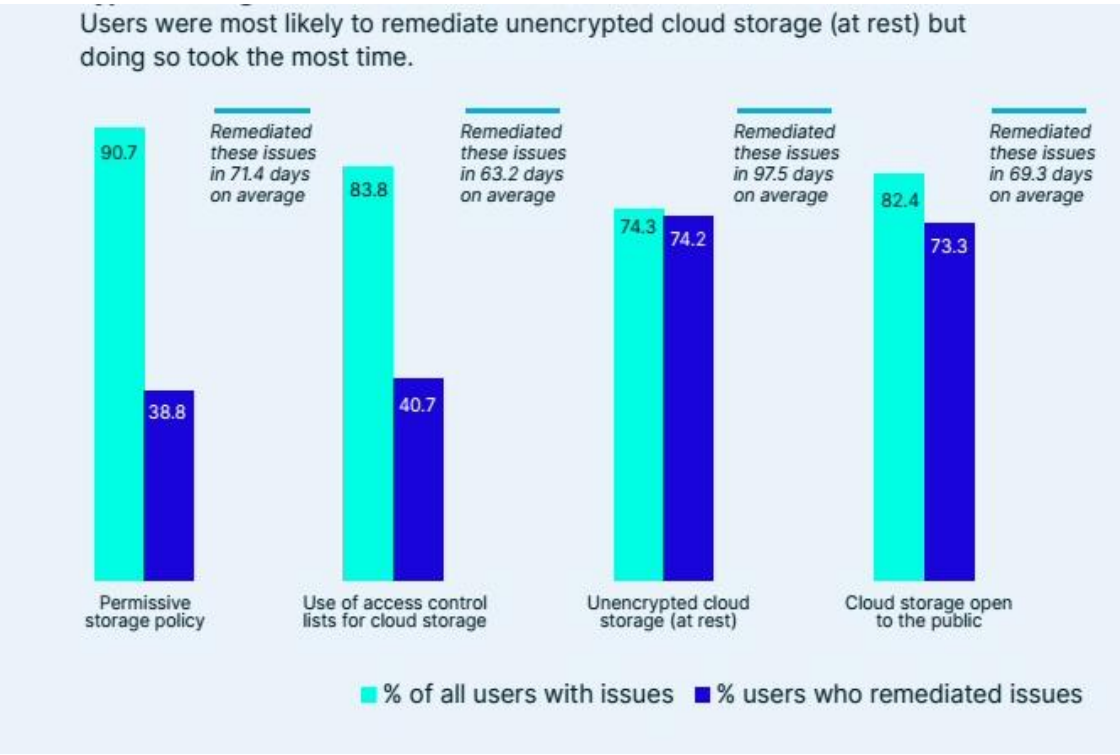
The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Whilst the benefits of cloud native to businesses are well-defined[2], the move to a cloud native approach does bring a variety of security risks to the fore; namely new, specialized threats and a wider attack surface. It is important to remember that the cloud native approach is about componentizing the application. With so many smaller components making up a larger whole, development and innovation is more agile, but the attack surface becomes inherently wider.

A dive into the cloud native vulnerabilities

The function of our own research team, Team Nautilus, is to keep abreast of emerging cloud native threats and the dangers they may pose to organizations. New research, *2021 Cloud Security Report: Cloud Configuration Risks Exposed*[3] seeks to understand both the scale of misconfigurations as well as how organizations cope with key issues. Team Nautilus analyzed a sample of misconfiguration issues including: storage (bucket/blob) misconfigurations, identity and access management (IAM) misconfigurations, data encryption issues, exploitable services behind open ports, and container technology exploitation. Among them, 90% of the companies analyzed had a security issue due to cloud misconfigurations. This indicates that a great many more organizations are similarly struggling to detect and secure the ever-growing cloud native attack surface.

Figure 1: Type of storage issue and time to remediate



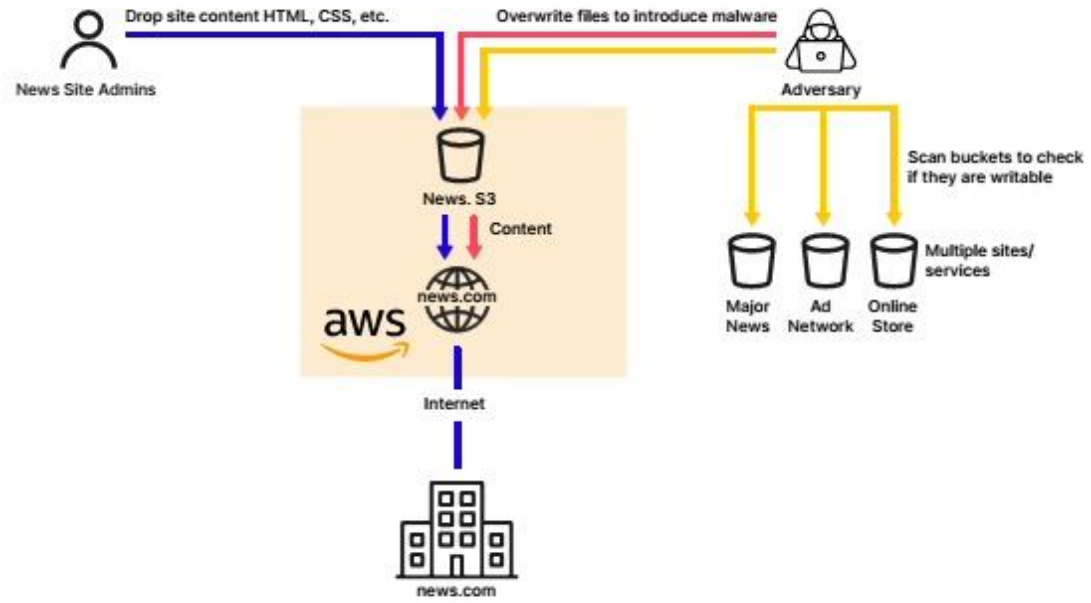
Source: Aqua Security

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Amongst some of the other findings, Team Nautilus uncovered that 82.4% of all organizations had at least one storage resource (for example, AWS S3 bucket) publicly open to all inbound traffic. Although opening a storage resource can often be a part of the basic design of the application, this is not always the case, and 73.3% of all cases were closed after receiving an alert, implying these were incorrectly left open. What's more, it took organizations an average of two and half months to close these storage resources.

Figure 2: Buckets exposed to the world



Source: Aqua Security

Similarly, 40.6% of organizations had at least one case of a misconfigured Docker API over the 12-month research period. Whilst the vast majority (90%) of these issues were fixed, it took, on average, two months to do so. This is particularly problematic because further research by Team Nautilus also showed that it takes on average five hours for attackers to detect and attack hosts with misconfigured Docker API. The median was 56 minutes. If issues aren't fixed for two months, a host had probably endured dozens of attacks.

Organizations struggle to keep pace

As well as the aforementioned wider attack surface for cloud native approaches, Cloud Service Providers (Amazon, Microsoft, Google etc.) are innovating at cloud speed. Updates to services come thick and fast, and keeping up with the security implications of this is difficult unless there is a dedicated team in an organization that can do so.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

We must consider the shift-left approach, wherein developers have end-to-end responsibility for their apps and components. This is great for speeding up testing and enabling a continuous delivery model, but has the knock-on effect that having a security team review all changes is not always possible.

All these factors combined can result in critical configuration issues, which are not always easy to detect or mitigate efficiently. This is a particular concern for larger organizations. Our data sets indicate that larger enterprises take an average of 88 days to address issues after discovery.

The future – where do organizations go from here?

If the issues of misconfigurations, and the time it takes to remediate them, are to be resolved, organizations will need a solution that goes beyond host-based security tools. A Cloud Security Posture Management (CSPM) solution that operates at the cloud provider control plane level, and can leverage APIs from the underlying public cloud vendor, is needed. This is vitally important because it provides the necessary visibility into the configuration of the cloud services.

Organizations must take a more proactive approach when dealing with cloud misconfigurations. They need to set a policy and ongoing practices as well as monitor for and fix service configuration issues. Failure to do so creates preventable exposure to threats that could easily be avoided, and could lead to severe breaches or cyberattacks.

Reference

1 Gens, F., Whalen, M., Mohan, D., Carnelley, P., Carvalho, L., Chen, G., Yesner, R., Dayaratna, A., Della Rosa, F., Wester, J., Villars, R., Jyoti, R., Matsumoto, S., Minton, S., Nadkarni, A., North Rizza, M., Parker, R., Smith, E., Johnston Turner, M. and Gillen, A (October 2019), 'IDC FutureScape: Worldwide IT Industry 2020 Predictions (October 2019), IDC FutureScape. Available at: https://www.idc.com/research/viewtoc.jsp?containerId=US45599219

2 Aqua Security, 'Cloud Native Applications 101'. Available at: https://www.aquasec.com/cloud-native-academy/cloud-native-applications/cloud-native-applications-101/

3 Aqua Security (May 2021), *2021 Cloud Security Report: Cloud Configuration Risks Exposed*. Aqua Security. Available at: https://info.aquasec.com/cspm-threat