HEADQUARTERS
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

Cloud Privileges Misconfiguration - Putting Company Data at Risk

Around 44% of cloud user privileges are misconfigured, leaving companies at risk, as indicated in Varonis's 2021 SaaS (Software As A Service) Risk Report.

A team of data security professionals and analysts at the cybersecurity firm, Varonis gathered and analyzed data from over 200,000 cloud identities and hundreds of millions of cloud assets for the report. Included in their report are key trends; challenges organizations face when trying to control unsupervised identities and shadow privileges that can put data at risk across a fragmented SaaS & IaaS environment.

AppOmni CEO and Co-Founder Brendan O'Connor says, "The misconfiguration and access problems we see now are not new - we are just now waking up to them. When it comes to SaaS applications, the landscape is far more diverse than the consolidated on-prem technologies organizations may have used in the past. Unlike focusing on just a couple of key technologies, like Windows and Mac, or Android and iPhone, most enterprises use dozens or even hundreds of different SaaS applications. This means that security teams will not be able to specialize in these technologies in the same way."

Another challenge for security teams is the dynamic nature of cloud and SaaS platforms, says O'Connor. "In addition to standard business updates - like adding or removing users or changing permissions - there are also frequent vendor releases that often include both new functionality and new security settings. The constant change inherent in cloud and SaaS platforms makes them especially vulnerable to configuration drift."

AppOmni's research has revealed results similar to Varonis's data. AppOmni data has shown that more than 95% of businesses have external users that are over-provisioned with access to sensitive data. Additionally, more than 55% of businesses have sensitive data exposed to the anonymous internet. "These numbers are unacceptable and should be a red flag to all CISOs and CIOs. As major SaaS platforms like Salesforce, Workday, ServiceNow, and Microsoft 365 evolve and grow in functionality and complexity, businesses should be using automated tools and processes to monitor and manage user permissions and configurations continuously." According to O'Connor

Here are a few key findings in the study conducted by Varonis:

- Nearly 44% of cloud privileges are misconfigured.
- 3 out of 4 cloud identities for external contractors remain active after they leave.
- 3 out of 5 users are shadow admins.
- 15% of employees transfer business-critical data to their personal cloud accounts.

Recommendation

As more and more companies utilize cloud SaaS (System as a Service) platforms like Microsoft 365, etc. Company end users, especially those working from home should be constantly reminded regarding cyber hygiene. Just as simple as properly logging out of their cloud access accounts after every use and avoiding frequent sharing and/or uploading of critical data to personal cloud accounts could help decrease data breach and other cloud-related cyber incidents within the company.

References

https://www.securitymagazine.com/articles/95781-of-cloud-privileges-are-misconfigured

https://gcn.com/articles/2020/08/04/cisa-tic-3.aspx

https://gcn.com/articles/2020/08/04/-/media/GIG/GCN/Redesign/Articles/2017/January/cloudefficiency.png

https://kirkpatrickprice.com/blog/5-cloud-security-misconfigurations-for-aws/