STATE OF CLOUD SECURITY TODAY

The cloud has rapidly become one of the most popular technologies for organizations and individuals across the world, thanks to its multitude of use cases from data storage to on-demand computing capacity. The ubiquity of the cloud is incredible with more users and organizations making use of it each day. This ubiquity is also the reason for concerns regarding data privacy and the security of cloud computing services.

Cloud Security in the Headlines

Data privacy and security are placed under a lot of scrutiny these days thanks to the numerous information leaks that became public knowledge in recent years. Fears of cloud security are well-founded considering the infamous cloud data leaks that have happened over the years with incidents like the iCloud celebrity photo leaks garnering massive attention from the media and public at large. While "Celebgate" was perhaps the most talked about breach of cloud security, it was not the only instance of such an occurrence.

With all of these security breaches in the public eye, it's no wonder that cloud security is at the forefront of so many IT professionals' minds. In fact, the Sophos' State of Cloud Security 2020 survey results show that " of organizations are concerned about their current level of cloud security."

The independent study from Sophos of 3,521 IT managers leveraging the public cloud across 26 countries and six continents reveals many insights into the world of cloud security, with some of the key takeaways being:

- " of organizations reported they were hit by malware, ransomware, data theft, account compromise attempts, or cryptojacking in the last year."
- Data loss/leakage is the topmost concern with 44% of organizations reporting "data loss as one of their top three focus areas."
- Multi-cloud organizations report more security incidents than single platform organizations.
- Europe's General Data Protection Regulation (GDPR) may be partly responsible for European organizations seeing the "lowest attack rates of all regions."
- 75% of organizations do not see staff expertise as a top priority despite the prevalence of cyberattacks.
- 66% of attacks were exploitations of misconfigurations and 33% used stolen credentials to gain access.

Not All Countries Are Equally Affected

Thanks to its massive number of respondents from IT professionals across the globe, Sophos was able to perform country-level analyses that show there is a large disparity of cyberattack prevalence. India (227 respondents) is at the top of the list with 93% of organizations reporting attacks in the last year. This is seemingly at odds with the fact that 92% of respondents claimed their organizations "had complete visibility of all cloud assets."

The Asia-Pacific region has the "highest regional rates of exposed data (35%), ransomware attacks (37%), and account compromise (33%) among the survey respondents." On the other hand, Europe suffered the "lowest percentage of security incident rates of all respondents in the last year." Italy, at 45%, is the lowest reporting nation for cyberattack rates with Poland a close second at 47%. "Europe shows the lowest rates of malware infections (29%), exposed data (24%), and ransomware attacks (22%) among the survey respondents."

With 68% of 413 respondents reporting their organizations experienced public cloud security incidents, the United States "was in the bottom 35% of countries suffering security incidents in the last year." This relatively strong performance may be a direct result of U.S. organizations having a high reported rate of "understanding their responsibility for cloud security" at 90% and 85% reported awareness of all their cloud assets. The Sophos' report goes on to say, "he U.S. is a full 17 percentage points higher than the global awareness average."

Methods of Attack

As mentioned already, 66% of reported cyberattack breaches were a result of security misconfiguration. Misconfigurations are essentially self-inflicted wounds as a result of failure to properly implement security controls. Cloud misconfigurations continue to be a problem for public clouds and are likely to contribute to a slowing of overall cloud migration. A lack of visibility is often the primary obstacle for detecting and mending misconfiguration issues.

The other 33% of reported cyberattacks were a result of stolen cloud account credentials. These attackers "utilized Identity and Access Management (IAM) roles and permissions to navigate the compromised cloud accounts." Sophos reports that only 25% of the organizations in their survey saw management of cloud account access as a top priority, despite its prevalence as a primary security concern.

Sophos reports that 91% of respondent organizations had overprivileged IAM roles and 98% had

multi-factor authentication (MFA) disabled. MFA acts as a vital form of backup security in cases where access credentials are stolen. MFA is often seen as an inconvenience, but the added protection it provides is more than worth the added time it takes to verify access authorization.

Worrying Trends for Cloud Security

The top security concerns from Sophos respondents is data loss/leakage at 44% and identifying and responding to security incidents at 41%. Organizations are also concerned (but less universally so) about managing multiple public cloud providers (28%) and identifying sudden increases in cloud spend (27%), while maintaining regulation compliance is tied with management of user roles and permissions at 26%.

Surprisingly, 3% of respondents said their organization has no public cloud security concerns with 1% responding that they were unsure when asked, "What are your organization's biggest public cloud security concerns?"

Despite the myriad of concerns regarding cloud security, very few (25%) of the respondents reported a lack of staff expertise as a top concern. Evidenced by the prevalence of cyberattacks worldwide, cloud security has struggled to keep up with the pace of cloud adoption and development with 24% of Sophos respondents saying security can't keep up with the pace of their developers.

While the cloud offers incredible benefits and potential, it also poses a serious security risk for organizations that aren't equipped to properly manage this new technology. Cloud security continues to be a growing concern among organizations and individuals as new reports of security breaches roll in. Balancing security with cloud optimization is a delicate task for IT management but one that organizations can't afford to neglect.