BIZCOMMUNITY

Sophos reveals The State of Cloud Security 2020 report

According to The State of Cloud Security 2020, a global survey from Sophos, almost three quarters (71%) of organisations from the MEA region experienced a public cloud security incident in the last year - including ransomware (23%), other malware (43%), exposed data (28%), compromised accounts (28%), and cryptojacking (22%).

Chester Wisniewski, principal research scientist at Sophos

Globally, organisations running multi-cloud environments are greater than 50% more likely to suffer a cloud security incident than those running a single cloud.

Europeans suffered the lowest percentage of security incidents in the cloud, an indicator that compliance with General Data Protection Regulation (GDPR) guidelines are helping to protect organisations from being compromised. India, on the other hand, fared the worst, with 93% of organisations being hit by an attack in the last year.

“Ransomware, not surprisingly, is one of the most widely reported cybercrimes in the public cloud. The most successful ransomware attacks include data in the public cloud, according to the State of Ransomware 2020 report, and attackers are shifting their methods to target cloud environments that cripple necessary infrastructure and increase the likelihood of payment,” said Chester Wisniewski, principal research scientist, Sophos.

> *“The recent increase in remote working provides extra motivation to disable cloud infrastructure that is being relied on more than ever, so it’s worrisome that many organisations still don’t understand their responsibility in securing cloud data and workloads. Cloud security is a shared responsibility, and organisations need to carefully manage and monitor cloud environments in order to stay one step ahead of determined attackers.”*

The Unintentional Open Door: How attackers break in

Accidental exposure continues to plague organisations, with misconfigurations exploited in 61% of reported attacks in MEA.

Detailed in the SophosLabs 2020 Threat Report, misconfigurations drive the majority of incidents and are all too common given cloud management complexities.

Additionally, 37% of MEA organisations report that cybercriminals gained access through stolen cloud provider account credentials. Despite this, only a quarter of organisations say managing access to cloud accounts is a top area of concern. Data from Sophos Cloud Optix, a cloud security posture management tool, further reveals that globally 91% of accounts have overprivileged identity and access management roles, and 98% have multi-factor authentication disabled on their cloud provider accounts.

The silver lining

Nearly all respondents (93%) from MEA admit to concern about their current level of cloud security, an encouraging sign that it's top of mind and important. Appropriately, "data leaks" top the list of security concerns for nearly half of respondents (41%); identifying and responding to security incidents is a close second (38%).

The State of Cloud Security 2020 report highlights findings of an independent survey conducted by Vanson Bourne among more than 3,500 IT managers across 26 countries in Europe, the Americas, Asia Pacific, the Middle East, and Africa that currently host data and workloads in the public cloud.

The full report is available for download.