LIQUIDTECHNOLOGY

Security Risk in the Cloud

According to the Internet Security Threat Report (ISTR) Volume 24, A single misconfigured cloud workload or storage instance could contain organization millions or cause a compliance nightmare **more than 70 million records** were stolen or leaked from poorly configured S3 buckets in 2018.

21% of files

in the cloud contain sensitive data, according to the recent McAfee's Cloud Adoption and Risk Report

The average organization has

2,200

individual IaaS misconfiguration incidents in the cloud. (Source: McAfee's Cloud Adoption and Risk Report)

On average, organizations experience

12.2 incidents

each month in which an unauthorized third-party exploits stolen account credentials to gain access to corporate data stored in a cloud service. (Source: McAfee's Cloud Adoption and Risk Report)

Companies are struggling to modernize their security practices at the same pace that they adopt cloud –

73%

experienced a security incident due to immature practices, according to the Symantec's Cloud Security Threat Report

Lack of visibility into cloud workloads is the leading cause – an overwhelming majority of Symantec's survey respondents (**93%**) report issues with keeping tabs on all cloud workloads

According to IS decision research,

29%

of SMBs (small- to -mid-sized businesses) have suffered a breach of files or folders stored in the cloud

31%

SMBs say that since moving to the cloud for storage, it's been harder to detect unauthorized access

15%

SMBs have suffered significant reputational damage because of unauthorized access to sensitive corporate data stored on cloud networks

21%

SMBs have gone as far as to say they keep their most sensitive data stored on on-premises infrastructure because they don't trust its security in the cloud

When it comes to data security, organizations are clearly worried about trusting third parties:

63% believe that cloud providers should do more to demonstrate they're protecting data

53% are worried about their data being unencrypted when stored in the cloud

56% say that it's difficult managing the security of data living in hybrid infrastructures

2 out of 3

of the most expensive cybersecurity incidents affecting small- to mid-sized businesses are related to the cloud, where 3rd party hosted IT infrastructure failures bring an average **$179K** loss, according to new research from Kaspersky Lab

Cloud Cybersecurity Threats To Watch Out For in 2019

01

PI security flaws

APIs are a common component of SaaS solutions – and though they are incredibly useful, they can also be incredibly vulnerable. Businesses are going to need to become more vigilant in their due diligence when selecting new third-party solutions and when vetting APIs before connecting them into their direct infrastructure

02

Insufficient out-of-the-box security

Out-of-the-box security solutions for many cloud-based applications aren't sufficient to truly keep data safe. And while the companies that are offering cloud services will undoubtedly focus more on security in 2019, businesses shouldn't rely upon them to keep their data secure.

03

Cryptojacking

Cryptojacking was most prominently seen with the WannaCry worm, which proliferated quickly across a multitude of platforms. Cryptojacking attacks are more frequently targeting enterprise cloud environments, which have access to significantly more computing capacity than the average home PC

04

AI-based attacks

Criminals can use artificial intelligence (AI) to analyze vulnerabilities in a cloud environment on-the-fly and launch coordinated attacks against a system with the goal of eventually breaking it down

05

Ransomware

Whether its IaaS or SaaS, cloud-based platforms are still susceptible to ransomware and will undoubtedly be targeted in 2019

Sources:

https://www.symantec.com/security-center/threat-report

https://www.ioecissions.com/cloud-storage-security-issues/

https://www.helpnetsecurity.com/2019/06/26/cloud-security-issues/

https://www.kaspersky.com/about/press-releases/2018_costly-cloud-breaches

https://www.lastline.com/blog/cloud-data-security-5-attacks-to-watch-for-in-2019/

https://www.skyhighnetworks.com/cloud-security-blog/5-key-findings-from-2019-cloud-adoption-and-risk-report/