IBM Newsroom

IBM: Security in the Cloud Remains Challenged by Complexity and Shadow IT

New Data Pinpoints Top Security Risks for Companies to Address as Cloud Migration Accelerates

CAMBRIDGE, Mass., June 10, 2020 /PRNewswire/ -- IBM (NYSE:IBM) Security today released new data examining the top challenges and threats impacting cloud security, indicating that the ease and speed at which new cloud tools can be deployed can also make it harder for security teams to control their usage. According to IBM survey data and case-study analysis, basic security oversight issues, including governance, vulnerabilities, and misconfigurations, remain the top risk factors organizations should address to help secure increasingly cloud-based operations. The case-study analysis of security incidents over the past year also sheds light on how cybercriminals are targeting cloud environments with customized malware, ransomware and more.

With businesses rapidly moving to cloud to accommodate remote workforce demands, understanding the unique security challenges posed by this transition is essential for managing risk. While the cloud enables many critical business and technology capabilities, ad-hoc adoption and management of cloud resources can also create complexity for IT and cybersecurity teams. According to IDC, more than a third of companies purchased 30+ types of cloud services from 16 different vendors in 2019 alone.[1] This distributed landscape can lead to unclear ownership of security in the cloud, policy "blind spots" and potential for shadow IT to introduce vulnerabilities and misconfiguration.

In order to get a better picture of the new security reality as companies quickly adapt to hybrid, multi-cloud environments, IBM Institute for Business Value (IBV) and IBM X-Force Incident Response and Intelligence Services (IRIS) examined the unique challenges impacting security operations in the cloud, as well as top threats targeting cloud environments. Top findings include:

- **Complex Ownership:** 66% of respondents surveyed[2] say they rely on cloud providers for baseline security; yet perception of security ownership by respondents varied greatly across specific cloud platforms and applications.[2]
- **Cloud Applications Opening the Door**: The most common path for cybercriminals to compromise cloud environments was via cloud-based applications, representing 45% of incidents in IBM X-Force IRIS cloud-related case studies.[3] In these cases, cybercriminals took advantage of configuration errors as well as vulnerabilities within the applications, which often remained undetected due to employees standing up new cloud apps on their own, outside of approved channels.
- **Amplifying Attacks**: While data theft was the top impact of the cloud attacks studied[3], hackers also targeted the cloud for cryptomining and ransomware[4] – using cloud resources to amplify the effect of these attacks.

"The cloud holds enormous potential for business efficiency and innovation, but also can create a 'wild west' of broader and more distributed environments for organizations to manage and secure," said Abhijit Chakravorty, Cloud Security Competency Leader, IBM Security Services. "When done right, cloud can make security scalable and more adaptable – but first, organizations need to let go of legacy assumptions and pivot to new security approaches designed specifically for this new frontier of technology, leveraging automation wherever possible. This starts with a clear picture of regulatory obligations and compliance mandate, as well as the unique technical and policy-driven security challenges and external threats targeting the cloud."

Who owns Security in the Cloud?

A survey from IBM Institute for Business Value found that responding organizations that relied heavily on cloud providers to own security in the cloud, despite the fact that configuration issues – which are typically users' responsibility – were most often to blame for data breaches (accounting for more than 85% of all breached records in 2019 for surveyed organizations).[4]

Additionally, perceptions of security ownership in the cloud for surveyed organizations varied widely across various platforms and applications. For example, the majority of respondents (73%) believed public cloud providers were the main party responsible for securing *software-as-a-service* (SaaS), while only 42% believed providers were primarily responsible for securing cloud *infrastructure-as-a-service* (IaaS).[3]

While this type of shared responsibility model is necessary for the hybrid, multi-cloud era, it can also lead to variable security policies and a lack of visibility across cloud environments. Organizations that are able to streamline cloud and security operations can help reduce this risk, through clearly defined policies which apply across their entire IT environment.

Top Threats in the Cloud: Data Theft, Cryptomining and Ransomware
In order to get a better picture of how attackers are targeting cloud environments, X-Force IRIS incident response experts conducted an in-depth analysis of cloud-related cases the team responded to over the past year.[5] The analysis found:

- **Cybercriminals Leading the Charge**: Financially motivated cybercriminals were the most commonly observed threat group category targeting cloud environments in IBM X-Force incident response cases, though nation state actors are also a persistent risk.

- **Exploiting Cloud Apps:** The most common entry point for attackers was via cloud applications, including tactics such as brute-forcing, exploitation of vulnerabilities and misconfigurations. Vulnerabilities often remained undetected due to "shadow IT," when an employee goes outside approved channels and stands up a vulnerable cloud app. Managing vulnerabilities in the cloud can be challenging, since vulnerabilities in cloud products remained outside the scope of traditional CVEs until 2020.

- **Ransomware in the Cloud:** Ransomware was deployed 3x more than any other type of malware in cloud environments in IBM incident response cases, followed by cryptominers and botnet malware.

- **Data Theft**: Outside of malware deployment, data theft was the most common threat activity IBM observed in breached cloud environments over the last year, ranging from personally identifying information (PII) to client-related emails.

- **Exponential Returns:** Threat actors used cloud resources to amplify the effect of attacks like cryptomining and DDoS. Additionally, threat groups used the cloud to host their malicious infrastructure and operations, adding scale and an additional layer of obfuscation to remain undetected.

"Based on the trends in our incident response cases, it's likely that malware cases targeting cloud will continue to expand and evolve as cloud adoption increases," said Charles DeBeck, IBM X-Force IRIS. "Our team has observed that malware developers have already begun making malware that disables common cloud security products, and designing malware that takes advantage of the scale and agility offered by the cloud."

Maturing CloudSec Can Lead to Faster Security Response
While the cloud revolution is posing new challenges for security teams, organizations who are able to pivot to a more mature and streamlined governance model for cloud security can help their security agility and response capabilities.

The survey from IBM Institute for Business Value found that responding organizations who ranked high maturity in both Cloud and Security evolution were able to identify and contain data breaches faster than colleagues who were still in early phases of their cloud adoption journey. In terms of data breach response time, the most mature organizations surveyed were able to identify and contain data breaches twice as fast as the least mature organizations (average threat lifecycle of 125 days vs. 250 days).

As the cloud becomes essential for business operations and an increasingly remote workforce, IBM Security recommends that organizations focus on the following elements to help improve cybersecurity for hybrid, multi-cloud environments:

- **Establish collaborative governance and culture:** Adopt a unified strategy that combines cloud and security operations – across application developers, IT Operations and Security. Designate clear policies and responsibilities for existing cloud resources as well as for the acquisition of new cloud resources.

- **Take a risk-based view:** Assess the kinds of workload and data you plan to move to the cloud and define appropriate security policies. Start with a risk-based assessment for visibility across your environment and create a roadmap for phasing cloud adoption.

- **Apply strong access management:** Leverage access management policies and tools for access to cloud resources, including multifactor authentication, to prevent infiltration using stolen credentials. Restrict privileged accounts and set all user groups to least-required privileges to minimize damage from account compromise (zero trust model).

- **Have the right tools:** Ensure tools for security monitoring, visibility and response are effective across all cloud and on-premise resources. Consider shifting to open technologies and standards which allow for greater interoperability between tools.

- **Automate security processes:** Implementing effective security automation in your system can help improve your detection and response capabilities, rather than relying on manual reaction to events.

- **Use proactive simulations:** Rehearse for various attack scenarios; this can help identify where blind spots may exist, and also address any potential forensic issues that may arise during attack investigation.

To view the X-Force IRIS Cloud Security Landscape Report, download the full reporthere.
X-Force IRIS will also host a webinar on June 10, 1:00pm ET to discuss the findings; registerhere.

Media Contact:
Cassy Lalan
IBM Security Media Relations
319-230-2232
cllalan@us.ibm.com

[1] IDC CloudPulse Summary Q119

[2] IBM Institute for Value Survey of 930 senior business and IT professionals

[3] IBM X-Force IRIS: "Cloud Security Landscape Report"

[4] IBM X-Force Threat Intelligence Index, 2020

[5] IBM X-Force IRIS "Cloud Landscape Report," based on client incident response cases taking place betweenJune 2018 and March 2020

SOURCE IBM

https://newsroom.ibm.com/2020-06-10-IBM-Security-in-the-Cloud-Remains-Challenged-by-Complexity-and-Shadow-IT