CLOUD SECURITY

UNDERSTANDING YOUR RESPONSIBILITIES AND THREATS

By David Lefever

((CENTRIC))

CLOUD SECURITY
WHO BEARS THE RESPONSIBILITY?

Contrary to widespread belief, the main responsibility for protecting corporate data in the cloud lies not with the cloud provider, but with the cloud customer. You are responsible for securing corporate data in the cloud.

This common failure of cloud customers to understand or meet their responsibilities is a leading cause of security incidents in cloud-based systems. Are you prepared?

Securing data in the cloud requires the customer to assume responsibility and management of the virtual machines (including updates and security patches), other associated application software, and the configuration of security groups that act as virtual firewalls.

Customers should carefully consider the cloud services they choose, as responsibilities vary depending on the service and deployment model, integration of services into their IT environments, and applicable laws and regulations.

MANAGING GROWTH

Given the exponential growth of the cloud computing market in recent years, cloud technology continues to transform the way organizations use, store and share data. There are many potential advantages of moving to the cloud, including lower costs, more agile development and increased resiliency.

The cloud also has introduced a host of new security threats and challenges. The security of data in the cloud is a key concern holding back cloud adoption for many companies.

SECURITY IN THE CLOUD VS. SECURITY OF THE CLOUD

WHO MAINTAINS THE RESPONSIBILITY?

We recommend deploying a shared responsibility model for cloud security. That helps ensure collaboration between the user and vendor, assigns clearly defined duties to both parties, and can establish best practices to effectively handle security. Below is what that model would look like.

CLOUD CUSTOMER	CLOUD PROVIDER
You define the controls, compliance and security in the cloud.	**The cloud provider takes care of the security of the cloud.**
Operating Systems	Physical Infrastructure
Platforms	Network Infrastructure
Applications	Storage
Identity and Access Management	Virtualization Layer
Network Configurations	
Network Traffic Protection (encryption, integrity, identity)	
Client-side Encryption and Data Integrity Authentication	
Service-side Encryption (file system and /or data)	

IDENTIFYING THREATS

Now that we've identified general responsibilities of the cloud customer and provider, the following is a high-level view of the top 10 security concerns for cloud services, in no order.

IDENTIFYING THREATS (CONTINUED)

1. DATA BREACHES

A data breach might be the result of human error, insider threat, a targeted attack, application vulnerabilities or poor security practices. It may include personally identifiable information, personal health information, financial information or intellectual property.

The risk of a data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

2. INSUFFICIENT IDENTITY, CREDENTIAL AND KEY MANAGEMENT

Insufficient identity, credential or key management can enable unauthorized access to data and potentially cause damage to organizations. Data breaches often happen due to lack of multifactor authentication and strong passwords, as well as poor practices with cryptographic keys, passwords and certificates.

In the case of federated identity management – allowing registered users to access information and applications using the same credentials across security domains – the use of multiple cloud offerings can mean islands of identities that need to be maintained. That could result in expired or unauthorized access if not effectively managed.

IDENTIFYING THREATS (CONTINUED)

3. INSECURE INTERFACES AND APPLICATION PROGRAMMING INTERFACES

Application programming interfaces (APIs) and user interfaces are generally the most exposed part of a system by having an IP address available outside the trusted organizational boundary. Management, monitoring, provisioning and other cloud services are usually performed with these interfaces.

Due to the open nature of cloud services, interfaces and APIs often use anonymous access, cleartext authentication or content transmission. These assets will be the target of heavy attacks. Insecure APIs can pose risks related to confidentiality, integrity, availability and accountability.

4. ACCOUNT HIJACKING

Attackers using social engineering, phishing, fraud or vulnerability exploits to compromise confidentiality, integrity and availability is not new. However, threats to cloud services present an entirely new challenge.

If attackers gain access to a user's credentials, they can manipulate data, eavesdrop on sessions and redirect clients to illegitimate sites, to name a few ways. With stolen credentials, attackers often can access critical areas of cloud services, allowing them to compromise the confidentiality, integrity and availability of those services.

IDENTIFYING THREATS (CONTINUED)

5. DENIAL OF SERVICE

A distributed denial of service (DDoS) attack is another common attack vector used to adversely affect cloud services on the internet and online services. DDoS consumes all of a target's cloud resources, making those resources unavailable to other general users. DDoS attacks can target any cloud service or website by using all of its CPU, RAM, disk space or network bandwidth.

6. INADEQUATE MONITORING, COMPLIANCE AND AUDITING

If an organization migrates to the cloud, its previous investment in security certification and controls assurance may be endangered if the cloud customer cannot identify the controls for which it is solely or partially responsible for. It must also provide audit evidence to validate compliance with its security requirements.

Furthermore, it may be difficult to evaluate how cloud computing aspects comply with the organization's existing security policies if those policies don't account for cloud capabilities.

7. INSUFFICIENT DUE DILIGENCE

When executives create business strategies, they frequently take cloud technologies and providers into consideration. Developing a good roadmap and checklist for due diligence when evaluating technologies and providers is essential for the greatest chance of success.

Executives who rush to adopt cloud technologies and choose providers without performing due diligence expose their organizations to multiple risks.

IDENTIFYING THREATS (CONTINUED)

8. ABUSE AND NEFARIOUS USE OF CLOUD SERVICES

Because weak registration systems are present in the cloud computing environment, anyone with a valid credit card can register and use the service. This facilitates anonymity, which can incite spammers, malicious code authors and criminals to attack the system.

Common examples of misuse include launching distributed DDoS attacks, email spam and phishing campaigns.

9. MALICIOUS INSIDERS

Employees of a cloud provider could have complete access to company resources without effective operating controls. Cloud providers must have proper security measures in place to track employee actions, such as viewing a customer's data.

Cloud providers also should have their own hiring processes, but the challenge is vetting their procedures to match the organization's standards for meeting legal and regulatory compliance requirements.

10. SHARED TECHNOLOGY VULNERABILITIES

Cloud providers deliver services by sharing infrastructure, platforms or applications in a multi-tenant environment. However, there is always a risk that one tenant could deliberately or inadvertently interface with the security or performance of another tenant.

Sharing computing resources may result in outages throughout the network, degraded performance or denied access for users in certain geographies. In other words, by sharing space with the target of an attack, you could become collateral damage.

CONCLUSION

In summary, it is important for cloud providers to apply a shared responsibility model for security. The cloud provider accepts responsibility for some aspects of security, while the customer must be responsible for other aspects.

And, just as there are best practices for dividing and implementing cloud security responsibilities, there also are cloud network security best practices that can help simplify a cloud customer's strategic approach to securing their network.

While the cloud has many advantages, it also introduces new or advanced security threats, as we have just seen in the top 10 security concerns. Your organization may only realize the security benefits of cloud, and even increased security, when you thoughtfully choose the cloud services you need, embrace cloud-native features, and adjust your architectures and controls to appropriately secure the environment.

ABOUT THE AUTHOR

David Lefever | Vice President, Partner
Cybersecurity Practice

Since 2010, I guided a company formerly known as The Mako Group (now part of Centric Consulting) through growth and cyber strategies. As CEO at Mako, I was able to witness and assist in our team establishing a brand representing quality and family values.

My frequent client interactions largely focused on sharing industry perspectives, developing strategies and assisting in solving complex cyber problems across four key areas: cyber risk management, IT audits, penetration testing and virtual CISO.

Want to keep your brand reputation and financial impact safe? Our Cybersecurity team can help address your security concerns.

Talk to an expert

((CENTRIC))

ABOUT US

Centric Consulting is an international management consulting firm with unmatched expertise in business transformation, AI strategy, cyber risk management, technology implementation and adoption. Founded in 1999 with a remote workforce, the company has established a reputation for solving its clients' toughest problems, delivering tailored solutions, and bringing in deeply experienced consultants centered on what's best for your business. In every project, you get a trusted advisor averaging over 15 years of experience and the best talent from across the United States and India. Centric deliberately builds teams that can scale up or down quickly based on client needs, industry and desired outcome.

Headquartered in Ohio, with 1,400 employees and 14 locations, Centric has been honored over the years with over 100 awards for its commitment to employees, clients and communities. Most recently, it was recognized by Forbes, for the eighth consecutive year, as one of America's Best Management Consulting Firms.

Visit http://www.centricconsulting.com to learn more.