SECURITY COMPASS WHITEPAPER

What Are the Top Security Risks During Cloud Migration?

Copyright © 2020 Security Compass. Updated June 2020.

Security Compass

Over the last decade, cloud computing has taken organizations by storm — most of them are moving their applications to the cloud. The benefits of cloud migration are clear, some want to scale up fast while others are migrating to reduce the cost of maintaining an in-house infrastructure. For smaller, high-growth organizations, cloud offers enterprise-class technology while staying nimble.

But cloud services expose organizations to new vulnerabilities because of the increased attack surface. It is also important to note that when organizations select a cloud service provider, they work under a "shared responsibility model" for application development. This means it is ultimately an organization's responsibility to protect their data in the cloud environment.

The European Network and Information Security Agency (ENISA) publication lists almost two dozen discrete cloud security risks across policy and organizational, technical, and legal categories.

Considering all the risks associated with cloud computing before making the move can prevent security breaches later. These breaches are not only expensive in terms of the remediation costs involved but can also severely damage an organization's reputation.

In fact, the fear of breaches is quite high as evident from a survey by Cybersecurity Insider where 29 percent of the responders said that data security, loss, and leakage risks are holding them from cloud adoption while 28 percent are concerned about general security risks.

In this white paper, we will talk about some of these risks ranked as "very high" and "high" by ENISA, along with recommendations to prevent these that you can use in your cloud migration strategy. We have also included a few recommendations for risk mitigation from the Cloud Security Alliance's (CSA) Security Guidance document.

1

Reliance on a single cloud service provider

HIGH PROBABILITY	MEDIUM IMPACT	HIGH RISK

When moving applications to the cloud, it is critical to understand the security requirements, applicable regulatory standards, architecture-based threats, and controls available to mitigate threats. In the cloud's "shared responsibility" model, each cloud vendor may offer different levels of management and security controls.

In a SaaS environment, the vendor may provide a custom database schema. In an IaaS or PaaS environment, tools, frameworks, operating systems, and other environments may not be easily replicated. In the event of difficulties, switching between cloud providers could result in delays, downtime, and an inability to meet SLAs.

Recommendation: Include engineering and security in the evaluation of providers and their terms of service to mitigate risk. Build and test contingency plans for back-up hosting. The CSA further recommends that users evaluate the financial stability of providers and avoid proprietary authentication services, opting instead for standards-based solutions such as OATH.

2

Ceding control to the cloud service provider

VERY HIGH PROBABILITY	VERY HIGH IMPACT	VERY HIGH RISK

One of the benefits of cloud migration is efficiency; it eliminates many of the systems and personnel required to manage and maintain a data center. This means the cloud customer is totally dependent on the policies, procedures, monitoring, and reporting of the cloud provider.

Smart cloud customers will understand the threats and regulatory requirements for each application when selecting a cloud provider. If a provider's service prohibits penetration testing, vulnerability assessments, or other security assessments, it may not be viable for an application subject to PCI-DSS.

Recommendation: As part of the migration strategy for each application, identify which internal and external policies apply to the application, and which controls are required. Examine the shared responsibility model to ensure that the cloud provider can offer and validate the required controls. The CSA also recommends evaluating a provider's third-party attestations and the scope of its assessments and certifications.

3

Access to other tenants' resources or data

HIGH PROBABILITY	HIGH IMPACT	HIGH RISK

Two defining features of the cloud environment are shared resources and multi-tenancy. By sharing computing resources across multiple users, cloud providers maintain the capacity for rapid scaling without requiring users to maintain permanent computing resources for peak capacity.

These features also present varying levels of risk, depending on the deployment model selected. Private clouds with well-considered security models present less risk than public clouds sharing storage, networks, and tenants using less diligent security where "guest-hopping" attacks may be a factor. In addition, the actions of each tenant such as spamming or port scanning can affect the reputation of all tenants, leading to blocked IP addresses and the deterioration of services.

Recommendation: The "shared responsibility" model will differ between providers and deployment models. The CSA security guidance includes a simple process model where teams first identify security and compliance requirements and an architecture and deployment model, then use these to identify gaps in controls.

4

Malicious activities by insiders

MEDIUM	VERY HIGH	HIGH
PROBABILITY	IMPACT	RISK

A recent Verizon Data Breach Investigations Report found that "20 percent of all cybersecurity incidents and nearly 15 percent of all data breaches" involved insider and privilege misuse patterns. According to a Fortinet study, 56 percent of respondents believe that the "shift to cloud computing is making the detection of insider attacks more difficult."

Whether in a company-owned data center or cloud setting, privileged users such as system administrators require root access to devices and systems for patching, upgrades, and general administration. In addition, depending on the model, cloud providers may offer network security, web application firewalls, security monitoring, and incident response. When unscrupulous insiders choose to compromise security, the actions might be particularly difficult to detect, especially when resulting from shared or compromised credentials.

Recommendation: Establishing and practicing an incident response plan for privileged account takeovers will help mitigate damage from a breach. The CSA offers extensive guidance for identity and access control, including controls for privileged accounts.

5

Accessibility of customer management interfaces

MEDIUM PROBABILITY	VERY HIGH IMPACT	HIGH RISK

Cloud providers offer an internet-facing management interface which allows cloud users access to their resources and is shared by all cloud users. The management interface is therefore an attractive target for attackers and like all software may include vulnerabilities, including remote access and browser vulnerabilities.

Recommendation: The process of selecting a cloud provider should include an assessment of the provider's internal security controls. The risk from management interface compromises can be mitigated by a strong internal application security program at the cloud provider, including threat modeling, security requirements, and validation of controls such as penetration testing and vulnerability management programs.

6

Deletion of data

MEDIUM PROBABILITY	VERY HIGH IMPACT	HIGH RISK

Shared resources can include disks, database, and other storage devices. When resources are scaled down or decommissioned, it may not be possible to delete or "wipe" the data stored on those devices.

Recommendation: Users should account for these risks as part of the security requirements for any project. Strong encryption will mitigate risk of data being disclosed, assuming the decryption keys are also not stored locally. Some cloud providers may allow full deletion through special procedures.

7

Service engine compromises

LOW PROBABILITY	VERY HIGH IMPACT	HIGH RISK

In any cloud platform, the service engine sits above all resources and abstracts the resources across all users. Vulnerabilities or design flaws in the service engine are an attractive target for hackers, as they may allow access to multiple user environments, exploit weaknesses in a single environment to access other environments, modify data, and reduce resources resulting in a denial of service to applications.

Recommendation: When selecting a cloud provider for a deployment, understand clearly the shared responsibilities and identify controls for all gaps between requirements, architecture, and deployment models.

8

Risk of data disclosure in civil lawsuits

HIGH PROBABILITY	MEDIUM IMPACT	HIGH RISK

While security risks dominate discussions in cloud migrations, legal risks are also present. Should a cloud provider be subpoenaed for a client's data, multiple cloud users can be affected. If hardware is part of the subpoena, the risk of data disclosure increases.

Recommendation: The CSA recommends that cloud customers should understand the relevant legal and regulatory frameworks, as well as contractual requirements and restrictions that apply to the handling of their data or data in their custody, and the conduct of their operations, before moving systems and data to the cloud.

In addition, users should review provider agreements to ensure they are able to put legal holds on disclosures while pursuing alternatives. Strong encryption of data at rest in the cloud and storing trade secrets and other company IP locally can mitigate the risk of unauthorized disclosure of sensitive information.

9

Location of data centers

HIGH PROBABILITY	HIGH IMPACT	HIGH RISK

Many cloud providers operate in varied geographical regions to reduce risk from outages, speed content delivery, and provide disaster recovery options. When information is stored on these data centers, it is subject to the privacy laws and data disclosure regulations of those jurisdictions.

While North America, Europe, and parts of Asia have well established data privacy laws, other regions may present unpredictable legal protections and enforcements. ENISA cites the example of the "national security interests of the hosting country [being] cited as a reason for seizing data" or hardware.

Recommendation: ENISA and CSA stress that not all law enforcement measures are unacceptable. Instead, ensure as part of any requirements that teams understand where cloud resources are hosted and how that may affect risk.

10

Compliance with local regulations

HIGH PROBABILITY	HIGH IMPACT	HIGH RISK

Using a cloud provider does not exempt cloud users from complying with local data protection and breach disclosure regulations. If shared resources are in multiple jurisdictions, it may be possible to move personally identifiable information or other protected data between these jurisdictions. Failure to comply with local data protection regulations, including breach notification, can result in substantial penalties.

Recommendation: As with the Risk of Changes of Jurisdictions, teams should require providers to disclose the locations of all data centers, local data protection and breach disclosure requirements.

In conclusion

The risks highlighted in this document comprise less than half of those cited by ENISA. Others include policy risks concerning supply chains and hardening procedures, technical risks regarding a cloud provider's ability to scale to meet demand, defend against Denial of Service attacks, or loss of backups, and the legal risk posed by software licensing agreements.

When used with a cloud migration plan like that of the CSA, the ENISA risks will help development and security teams address a broader set of threats to software as it moves to the cloud. As we mentioned earlier, ensuring the security of your organization's data in the cloud environment is more important than ever because of the ever-rising threat landscape. You can make cybersecurity a competitive differentiator by making your business resilient.

Learn about our industry-leading solution, SD Elements, that can improve your security posture in the cloud and protect your customer data.

SecurityCompass

Go Fast. Stay Safe.™

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
995 Market Street
2nd Floor
San Francisco, CA
USA 94103

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001

Copyright © 2020 Security Compass. Updated June 2020.