CLOUD SECURITY THREATS

D. NOUR DANDAN | NETWORK BOX USA

NETWORKBOXUSA.COM

CONTENTS

When it comes to adopting and moving to the cloud, **security** is often cited as **one of the top concerns** with 77% of organizations recognizing its importance. This is amplified by the accessibility of data and applications from outside a company's network. Something which potentially grants threat actors visibility and access to an organization's infrastructure, if security is not properly configured and implemented consistently.

In traditional networking environments, the perimeter is arguably more straightforward and parameters regarding protecting a network are, more or less, easily identifiable. While the cloud is a different type of landscape, it does not necessarily introduce new threats. Rather, it magnifies existing threats and facilitates the need to adapt security techniques to a revised deployment model.

Let's take a look at some of the top cloud security threats.

DATA BREACHES

Data breaches are a legitimate security threat for both traditional and cloud environments. Ideally, security is at the forefront of deployment and maintenance in either environment, but the cloud does present additional challenges.

For instance, databases are no longer confined to an organization's physical network (i.e. local servers); they are accessible through a web browser via a web application. And, if access to those databases is not secure, it leaves an organization's databases vulnerable to a cyber attack.

ADVANCED PERSISTEN THREATS

Advanced persistent threat (APTs) are sophisticated threats that enter a network and use various techniques to launch additional attacks by going undetected for an extended period of time. In a survey conducted by Netscout, 15% of respondents had experienced an APT, while more than half cited APTs as one of their top concerns for the year.

In 2009, the Ghostnet operation was a cyberespionage campaign targeting workstations as well as users in over 100 countries via spear-phishing emails. These emails contained a malicious attachment that downloaded a Trojan, enabling hackers to remotely access and control infected devices.

SYSTEM VULNERABILITIES

Patching vulnerabilities is one of the most important aspects of any cybersecurity solution. A recent study analyzing over 316 million security incidents found that it takes organizations an average of 38 days to patch a vulnerability. 38 days. That is simply not fast enough.

The 2017 Equifax data breach is a prime example of why patching system vulnerabilities as soon as a patch is available is absolutely critical. Equifax hackers exploited a known vulnerability (CVE-2017-5638) in Apache Struts, for which a patch was available. To give you a timeline, Apache released a patch for that vulnerability on March 8th, hackers first exploited the vulnerability in May, and Equifax didn't patch it until July 30th. While it wasn't the only point of failure, the breach affected over 147 million individuals in the United States.

INSECURE INTERFACES/APIS

Interfaces and APIs are the front doors leading to data stored in the cloud. Since the cloud is heavily reliant on interfaces and APIs, the ones that are not sufficiently protected are a definite concern. Cue the iCloud breach of 2014. Hackers took advantage of a glitch in the iCloud interface that allowed them unlimited password guesses.

ACCOUNT HIJACKING

User access to data is based on permissions. Account hijacking is a real threat and can be particularly devastating if the account credentials stolen were those of someone with access to sensitive data. How do hackers hijack accounts, or, even, get their hands on login credentials?

Social engineering, for one, is a lucrative tactic that remains a huge problem in cybersecurity across organizations, as it taps into the human element of the security chain. (The Ghostnet operation mentioned earlier is one prime example of social engineering executed via targeted phishing emails.)

MALICIOUS INSIDERS

Malicious insiders can be a difficult threat to prevent, regardless of the network environment (e.g. physical or cloud). According to the 2018 Verizon Data Breach Incident's Report, 28% of data breaches involved insiders; however, not all insiders are intentionally malicious. Verizon found that 17% of breaches were because of human error, whether clicking on a malicious link, improperly disposing of sensitive documents/data, or being a social engineering target and unintentionally offering up information.

POOR ACCESS MANAGEMENT

Access management is crucial to protecting your data and clients, especially when it comes to the cloud. Poor access management can easily result in a breach, as seen with Reddit earlier this year, where hackers used legitimate admin credentials to gain access to an old database backup, as well as some users' emails.

Interestingly, Reddit had already implemented SMS-based two-factor authentication (2FA), but the hackers were able to intercept said SMS to authenticate the login. In response, Reddit quickly rolled out token-based 2FA for its employees, as well as users.

INSUFFICIENT DUE DILIGENCE

Technology is constantly evolving and, in turn, so is cybersecurity (and, subsequently, cybersecurity strategies). When protecting your cloud infrastructure is at stake, insufficient due diligence can present a serious security issue. This includes, but is not limited to, reviewing contracts with third party vendors (i.e. what steps are they taking to ensure that their cloud offering is secure?), identifying what you are doing to ensure your own cybersecurity, defining and implementing processes for incident response, as well as when employees are hired or leave the company, cybersecurity training, etc.

DATA LOSS

Regardless of how often we are told to back-up our data, data loss happens and can be a serious threat in cloud environments. Data loss could be a result of a malicious attack, or even purely accidental. Forrester Research released a report that discussed the 6 leading causes of data loss in the cloud:

1. Accidental Deletion
2. Departing Employees
3. Hackers
4. Malicious Insiders
5. Rogue Applications
6. SaaS (Software-as-a-Service) Providers' Prolonged Outage

Accidental deletion is, by far, the most common. For instance, in 2011, the Alzheimer's Association had an employee leave their organization. Prior to doing so, the employee deleted their emails. While he/she may have merely wanted to delete all personal emails, some of the deleted emails contained important information regarding an upcoming fundraiser.

WHO IS RESPONSIBLE FOR WHAT?

One of the biggest challenges when it comes to cloud security is determining who is responsible for what part of the cloud. After all, the cloud is a shared responsibility between cloud provider and client. Amazon Web Service's (AWS) illustrated their Shared Responsibility Model in this diagram. Simply put, AWS is responsible for the security OF the cloud, while clients assume responsibility for security in the cloud.

Even so, when it comes down to it, the bulk of the responsibility and impact is going to fall on your organization's shoulders because it was your data that was impacted.

As with anything, there is a learning curve and cloud security isn't any different. While the threats are similar to those affecting traditionally deployed networks, the cloud magnifies the threat and risk factors, and is a stark reminder of the importance of approaching the cloud with security top of mind.

CLOUD SECURITY THREATS

FACEBOOK	/NetworkBoxUSA
TWITTER	/NetworkBoxUSA
LINKEDIN	/NetworkBoxUSA
YOUTUBE	/NetworkBoxUSA
INSTAGRAM	/NetworkBoxUSA
BLOG	networkboxusa.com/blog
WEBSITE	networkboxusa.com

NETWORK BOX USA
cybersecurity done right

2825 Wilcrest Drive
Suite 259
Houston, TX 77042

832.242.5757

info@networkboxusa.com