The Top Cyberthreats To The Cloud

Written for KAMIND, IT, Inc.

By Ravi Das

Introduction

With the Remote Workforce now an almost guarantee that will continue well into 2021, many business in Corporate America are now scrambling fast to deploy their entire IT and Network Infrastructures into a Cloud based Platform, such as that of the Amazon Web Services (AWS) or Microsoft Azure. This trend has been catalyzed by two notable events:

- The Cybersecurity lessons that have been learned when COVID 19 originally hit earlier this year;
- The advantages of using the Cloud for remote workers, especially when it comes to accessibility, scalability, and affordability.

But even though the Cloud has many huge advantages, the Cyberattacker is now paying attention to this trend, and are now targeting these types of platforms as a result. In this whitepaper, we address some of the top Cyberthreats to the Cloud, and some solutions that can be used to mitigate them.

The Threats

1) Denial of Service Attacks:

These are also known as "DoS" based attacks, and in fact is, considered to the parent to the Distributed Denial of Service ("DDoS") attacks. But the DoS based ones are slightly different. For example, it is only used to target either one Web based application at a time, unlike the DDoS which targets multiple applications all at once. But the bottom line of these kinds of attacks is that they are designed to literally choke the load times of the Web application on the client side, making them nearly impossible to access, just because it takes so long. In other words, the Cyberattacker is taxing the very limits of the processing power of the Web server that is hosting the particular application. In fact, it is very analogous to a traffic jam, which is nicely summarized in this quote: "It is like being caught in rush-hour traffic gridlock: there is no way to get to your destination, and there is nothing you can do about it except sit and wait."

(SOURCE: 1).

What are some of the ways that you can mitigate this from happening?

- Implement Advanced Intrusion Detection Systems:

  These are also known as "IDSs". With this, anomalous behavior can be detected quickly and easily, and from that, you can cut off the flow of network communications from the point of origination.

- Deploy Firewalls that have Traffic Inspection functionalities:

  Most Firewalls simply just check for the behavior of most network traffic. But with this kind of Firewall, it does a much more granular inspection of the data packets and can immediately terminate those that are deemed to be nefarious in nature.

- Blacklist IP Addresses:

  This is something that your Cloud Solutions Provider can do for you, this is a particular functionality that you may be able to initiate. With this, any known or potential malicious IP addresses are blacklisted, so that your Web application (if you have created one for your customers) will be blacklisted, and thus, cannot be served any of the requested web pages.

2) The usage of Shared Environments:

One of the main reasons of the why the Cloud can offer so many strategic advantages to its tenants is that it makes use of shared resources. For example, when you log into web portal in Azure, you have the look and feel as if it's your own server. To a certain degree, this is true. But it is important to keep in mind that there are many of these Virtual Servers that are spun off and hosted from just one primary, physical server. Because of that, these Virtual Servers share both the computational and processing resources of this one physical server. For the most part, what happens in one tenant should not impact your infrastructure, but there are times that it can, especially if this physical server has not been configured properly.

What can be done to fix this?

Unfortunately, you are being the tenant, there is not much that you can do on your own powers. This is something that only your Cloud Service Provider can fix, so therefore, if you suspect something is happening in this regard, notify them immediately so that they can resolve the issue in just a short period of time.

3) The Advanced Persistent Threat:

This is one of the newest threat variants that is starting to emerge in Cloud based Platforms. These are also known as APTs, and a technical definition of it is as follows:

"An advanced persistent threat is an attack in which an unauthorized user gains access to a system or network and remains there for an extended period of time without being detected."

(SOURCE: 2).

In other words, the Cyberattacker finds locates an unknown backdoor into your Virtual Machine (VM – these are also used synonymously with "Virtual Servers" and mean literally the same thing), and from there, can stay in for a very long period of time, without going noticed. The ultimate goal is to try and steal as much confidential information and data as possible over this extended duration.

What can be done to mitigate this kind of risk?

- Limit access:

  It is very important to remember that your Cloud based Platform will be one of your company's most prized permissions. You don't want each and every employee to have access it, so limit it those individuals that need access to it the most, which is namely your IT Security Team. Your Cloud Service Provider should be able to initiate all of the required protocols that are needed in order to avoid the mishap of malicious account takeover.

- Implement different Subnets:

Rather than deploying everything into one Cloud Infrastructure, you can actually divide it out into different segments which are also known as "Subnets". By doing this, you are putting a database into one segment, the other in a different one, etc. The idea of this is twofold:

*It will help to further eliminate the risk of shared resources spilling over into your platform from the different tenants;

*If by chance a Cyberattacker does break into one Subnet, the chances of them breaking into others is statistically diminished, which will help to contain any damage that has already been created.

- Make use of Multifactor Authentication:

This is also known as "MFA". With this particular strategy, you are implementing at least three or more layers of authentication mechanisms, in order to 100% guarantee the legitimacy of the individual that is trying to access your Cloud based Platform. This is a great strategy to use in conjunction with limiting access, as reviewed earlier in this whitepaper. In fact, Microsoft Azure comes with a great set of MFA tools, that you can install and use in a very short period of time.

4) Data Loss:

This is a topic that has made news headlines this year and will continue even well into 2021. This happens when the Cyberattacker covertly hijacks the Personal Identifiable Information (PII) datasets from your Cloud Infrastructure and sells them onto the Dark Wed to make a lucrative profit. Or they can be used to launch Identity Theft Attacks.

What can be done to help avoid this?

Really, there is no way in which you can prevent this from happening. This kind of breach can occur even to those businesses that are deemed to have the best lines of defenses at hand. In this situation, the only thing you can do is to keep make backups of your databases on a regular basis. But it is also important that you make multiple copies of these backups and store them into different locations. In this regard, a very nice feature of Microsoft Azure is that you can create separate VMs in geographically different Data Centers. This is technically known as also as "Geodiversity". You can use this method in addition to creating different Subnets. By doing this, you can keep your database backups in different Data Centers.

5) Ensuring strong levels of Due Diligence and Compliance:

Although the Cloud based Platforms can be easy to configure and deploy, there is very often a rush by businesses to move their entire IT/Network Infrastructures all at once, in the shortest time possible. This tactic will now only leave grave security holes, but you are also exposing the Personal Identifiable Information (PII) datasets at grave risk to accidental or even malicious leakage.

What can be done to prevent this?

- Establish a clear plan of action:

If you have a lot to migrate over, you first need to come up with a comprehensive plan as to how it will be done. It is very important that you break down this down into various phases, taking a "one step at a time" approach. In way, it is like developing source code for Web application. After each module is created, you need to test it first before you can move to the next one. Like this, after you have migrated the components that are included in the first phase, make sure all is working well, and completely enable all of the security features that are needed in this regard. Once everything looks good, then move onto the second phase, etc. True, it may take quite some to this until you reach completion, but it is better to make sure each and every piece is working the way it should be. This is especially pertinent as you migrate databases as well. With this approach, also make sure that the components in each phase has been configured properly as well. Although your Cloud Service Provider can help you by providing the tools that are needed to this, you have the ultimate responsibility for actually doing this right in the first place.

- Making sure you come into compliance:

  By taking this phased in approach, you will also be in a much better position to handle the issues of compliance, especially when it comes to both the GDPR and the CCPA. If you wait until the very end to check for compliance, the chances are greater that you could miss something, and at a subsequent point in time, because of this, you could potentially face an audit and steep financial penalties.

6) Future system weaknesses and vulnerabilities:

Even though you may have taken great care to make sure that your Cloud deployment into Microsoft Azure has been as safe and smooth as possible, there is still the potential of some mishap occurring into the future. In other words, what worked well initially has no guarantee of holding up into the future, given the dynamic nature of the Cyber Threat Landscape. Probably one of the biggest vulnerabilities here is the uploading and storage of insecure API software libraries for Wed application that you are hosting. For example, many software development teams, in an effort to deliver the project in time and under budget to the client, often fail to test for the security vulnerabilities of the APIs that are using. As a result, not only does this put your Web application at risk, but any failures here can have an unintended, cascading negative effect on the other parts of your VMs.

How can mitigate this risk?

- Test everything:

  In this regard, you will not only want to test the security of the APIs that you have used, but also the source code that you have compiled as well. A great way to do this is to conduct an exhaustive Penetration Test of all of the software modules involved. This will uncover both the known and the unknown vulnerabilities that may residing. Once all of these have been remediated, you can proceed to upload all of this to your VMs and even the databases that you have set up and configured as well. By taking these extra steps now, you are greatly curbing the statistical chances that your Cloud based Platform will be the victim of a large scale Cyberattack.

7) Account Heisting:

Although this is one of the oldest threat variants to date, it is still one of the most widely used ones as well. There are many ways that a Cyberattacker can hijack one of your accounts, and this can stem from the result that you could still be using a legacy-based authentication method, such as using just one password, and letting your employee create it. Because passwords can be so easily guessed these days, this can allow not only non-authorized entry into your Cloud based Platform, but it can also lead to the creation of other phony accounts, in which hackers can use in order to look like that they are legitimate employees.

How can this be avoided?

- Make use of Password Managers:

  Essentially, these are software based applications that can not only create those much needed long and complex passwords, but can reset them at time intervals that you prescribe, and can even alert you in case of any sort of malicious activity that are taking place against those passwords. You should make the usage of this tool mandatory for those employees that are accessing the VMs and any shared resources that reside form within them.

- Utilize Multifactor Authentication (MFA):

  Microsoft Azure has an entire portal that is dedicated to deploying all of the security tools you could ever imagine for your Cloud Infrastructure. One of these is MFA, in which at least three or more layers of authentication are used. This can be used quite efficiently to create and implement the Zero Trust Framework, in which all of your employees have to go through these layers of authentication, no matter what the circumstance might be.

8) Insider Threats:

Traditionally, these have been some of the most difficult threat variants to find. The only solace in this was that at least when employees were in the office before COVID19 hit, you could get some idea from somewhere if a Malicious Insider were brewing somewhere, especially that of a disgruntled employee or contractor. But with everything now virtual because of the Remote Workforce, it has become even much more difficult to detect the possibilities of an Insider Attack from occurring.

What are the steps one take to detect this in the "new normal"?

- Immediately terminate all levels of access:

  Probably the only best way to circumvent this from happening is to ***immediately delete all of the rights, privileges, and permissions of the employee*** after they have been terminated or leave on their own. This is also especially true of contractors.

- Keep an eye for anomalous activities:

  In this regard, you can make use of both Artificial Intelligence (AI) and Machine Learning (ML) tools to help track down any malicious or suspicious behavior on a real time basis. As a result, your IT Security Team will not have to waste any time in combing through all of the alerts and warnings that are coming through. You should also make use of what is known as a "Security Incident Event Management" (also known as "SIEM") package in this aspect. They can present all of this to information and data to you on a real time basis for an even quicker detection and response. The bottom line is that even though you may have revoked all of the login credentials of your ex-employee, it does not mean that they will still not try to break into your Cloud Infrastructure.

9) Data Breaches:

In the world of Cybersecurity today, there is very often confusion as to what a "Data Breach" is versus a "Data Leak". In reality, the two are very different. The technical definitions of both are as follows:

A Data Breach: "The existing controls were somehow broken or bypassed. This could have been accidental or malicious. Outside or inside people could breach controls. Hackers who manipulate a system to gain access to data they are not authorized to access is a data breach, as is an employee going against policy/procedure which exposes data."

A Data Leak: "This simply refers to the outcome that data was made available to unauthorized people."

(SOURCE FOR BOTH: 3).

In other words, with a Data Breach, there was a willful and deliberate attempt made in order to gain access to the confidential information and data. With a Data Leak, it is somehow made available to others, but it is very difficult to prove if trigger mechanism was intentional or just accidental. But whatever it is, the fact is that you have Personal Identifiable Information (PII) datasets that are now in the hands non authorized, third parties.

How can this be prevented from happening?

- Use Encryption:

  In the end, all businesses are prone to becoming a victim of both the above. The only thing that can be done is to mitigate that risk from occurring as much as possible. One of the best ways to do this is to Encrypt all of the information and data that reside in the databases that you have created. That way, if any of it does fall into the wrong hands, it will remain in a garbled state permanently, and with that, there is not much damage that can be done.

10) Cryptojacking:

To some degree or another, most of us have heard of the term of "Virtual Currency". One of the best-known examples of this is that of Bitcoin. In fact, this is what Cyberattackers very often want to be paid in when they launch an attack against a target, and before they will release the

Decryption Algorithms (this is at least the hope – but very few of them actually do this). Cryptojacking is yet another threat variant which prays upon the Virtual Currency market. A technical definition of it is as follows:

"It is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads Cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser."

(SOURCE: 4)

In other words, the unauthorized usage is simply the taking over of the victim's device's electrical and processing powers in order to illegally mine for these Virtual Currencies. Typically this has often been attributed to just and held devices, such as smartphones, tablets, etc. or other types of both hard wired and wired devices. But now, the Cyberattacker is getting away from this, and can actually harness these powers from your VMs as well, by any of the following methods:

1) Entering via a backdoor;
2) Duping the victim into clicking onto a malicious link or downloading an infected file;
3) Breaking into your Cloud based Platform through an account takeover or heisting attempt.

What can to do prevent this?

- Making use of Port Scanning:

  Another very popular way for the Cyberattacker to enter into your Cloud Infrastructure is via any open port that exists. A scan can quickly reveal to you any network ports that are open, and alert you to the ones that need to be closed immediately.

- Be on the lookout for resource consumption:

  Many times IT Security Teams think that a slow responding VM is the result of a slow network connectivity. But this could also be the first telltale sign that you have become a victim of a Cryptojacking Attack. Also be on the lookout for sudden vCPU usage spikes, or anything else related to that seems out of the ordinary to you.

Conclusions - The Tools From Microsoft

Overall, this whitepaper has examined some of the most prevalent Cyber related threats that have occurred this year to Cloud based Platforms and are even expected to continue well into 2021. But of course, there will be much newer and different variants that will emerge from them. As also discussed earlier in this whitepaper, Microsoft Azure has an entire array of security tools that you can start to use almost immediately from your administrative console.

Here are some key ones to keep in mind:

1) The Azure Security Center:

This is the main security management portal, and it has been designed to be a unified infrastructure. It can be used to not only further enhance the defense of all of your VMs, but it can also be used to beef up the lines of defenses for any On Premise assets that you may have, such as servers and workstations. Some of the many things that you can do with this are:

- Manage and enforce all of your security and compliance policies;
- Conduct continual assessments of your Cloud Infrastructure on a real time basis, especially when it comes to detecting and tracking suspicious like network behavior;
- Create and deploy network maps across all of your VMs in all of the Azure data centers that you are using so that you get a clear and succinct view of the network topology that as been created. With this, you can even pinpoint network bottlenecks and other choke points that may be slowing down your network infrastructure;
- Implement recommendations easily that are provided to you to further protect Cloud assets;
- Even deploy security mechanisms for any instances that you have which are IoT based;
- Institute security mechanisms for Hybrid based Cloud platforms.

2) The Azure Advanced Threat Protection (ATP):

This is a service for Azure which has been designed primarily to further enhance he security posture of Active Directory (AD), whether it has been deployed in the Cloud, On Premises, or even a combination of both. Here is a sampling of what you can do with it:

- Quickly identify and monitor any types of user and device behavior which are deemed to be rogue in nature. It makes use of both existing attack signatures and possible future ones by making use of AI, focusing upon Behavioral Analytics;
- Implement Threat Intelligence feeds both for your Cloud and On Premises based assets;
- Protect all of the Personal Identifiable Information (PII) datasets and their associated profiles/groups that are stored in AD;
- Get a timeline of when potential threat variants could be making their way into your Cloud Infrastructure so you can fend them off even quicker;
- Monitor on a real time basis each and every access point into your VMs so that you can immediately cut off any unauthorized attempts to access them.

3) The Azure Identity Manager:

This is also an Azure based service that essentially allows you to create and securely manage the identity profiles (as well as their associated rights, permissions, and privileges) for all of your employees. For example, you can do the following:

- Can create just one identity profile for an employee that needs access to multiple areas in your Cloud Infrastructure (but can implement different authentication mechanisms);
- Implement a Single Sign On (SSO) based regime for both the internal and external Web applications that you create;

- Create MFA authentication tools that are based on certain heuristics and rules. These can be deployed for both your VMs and On Premises servers/workstations;
- Implement even greater security layers that you can add onto your existing Virtual Private Network to mitigate the risk of malicious interception of the data packets substantially further.

4) The Azure Site Recovery:

This is yet another service that has created for Azure. It has been created and designed to keep not only your VMs but all of other Cloud based assets running all of the time, without any disruption to service. Here are some of the key features of it:

- You can deploy replication mechanisms so that you can reproduce a same instance of another VM that may have been impacted by a security breach;
- You can restore your VMs from their primary location to another Azure data center if the need arises;
- You can also replicate On Premises servers;
- If a specific process or workload from within a Windows or Linux VM needs to be replicated, you can do that as well;
- Conduct real time Incident Response/Disaster Recovery/Business Continuity drills without causing any disruption to service for your VMs.

Sources

1) https://www.whoa.com/fighting-the-top-12-threats-to-cloud-cyber-security-threats-10-12/
2) https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition
3) https://security.stackexchange.com/questions/229388/what-is-the-difference-between-a-data-leak-and-a-data-breach
4) https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
5) https://searchcloudsecurity.techtarget.com/tip/How-to-prevent-cloud-cryptojacking-attacks-on-your-enterprise
6) https://blogs.infoblox.com/security/what-you-need-to-know-about-cryptojacking-and-how-to-protect/
7) https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction
8) https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/#features
9) https://www.insight.com/content/dam/insight-web/en_US/article-images/datasheets/Microsoft-Azure-IAM-DS.pdf
10) https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview