CLOUD COMPUTING SECURITY

PROTECTING YOUR ONLINE DATA

An Overview, Guide to Protecting your Cloud Data with LIFARS and Avanan.

LIFARS
your digital world, **secured**

CONTENTS

OVERVIEW

Cloud Computing Defined

As technology continues to advance and transform business functions, more companies are choosing to transfer their data into the cloud. With having easy accessibility to servers, databases and application services, cloud computing removes the responsibility of managing, storing and sharing data; handing it to a third-party cloud provider. The cloud provides businesses flexibility allowing for easy access to data anytime and anywhere.

A cloud provider will offer customized services, depending on an enterprise's regulations and organizational needs. However, with any provider, the benefits of cloud computing will provide you with flexibility and scalability, cost efficiency, increased speed, automatic updates, and disaster recovery.

Benefits of Cloud Computing

1. **Flexibility/Scalability:** Cloud computing grows with your company. As your demands increase, it will become easier to scale up your cloud space. You have the capability to scale up or down, while only paying for your needs.
2. **Cost Efficiency:** Moving to cloud computing may decrease the cost of maintaining your networks. You can reduce your costs of purchasing expensive equipment and systems with cloud computing depending on your cloud provider.
3. **Increased Speed:** Resources are a click away. Companies with cloud computing can now respond quickly and efficiently to any changes that may arise.
4. **Automatic Updates:** It's not in your hands anymore. Most cloud providers update your networks automatically.
5. **Disaster Recovery:** Your data does not vanish. With natural disasters, like fires, tornadoes, or storms, your information can be destroyed, if it was stored on your computer or USB drives. With cloud computing, your information stays saved in the internet.

MOVING TO THE CLOUD

Top 3 Considerations

1. Business Functions
Evaluate your business functions to see if they are appropriately in line with your systems and applications.

2. Choosing a Provider
Find a vendor that can meet your data security, accessibility, and portability requirements.

3. Define Responsibilities
Understand and determine your relationship with a cloud service provider.

1. Business Functions

When deciding to move data into the cloud, there is a lot to take into consideration. First, it is essential to look into your business continuity and disaster recovery plan, focusing specifically on the business impact analysis to ensure that it is up to date with current regulations and standards. Understanding your performance and capacity reports to avoid an overload on your system will help when choosing the appropriate cloud provider. Assigning recovery time objectives not only for the business, but also for clients and compliance perspectives will help to avoid the consequences associated with a disruption in business continuity. Evaluating your business functions to see if they are appropriately in line with your systems and applications when moving to the cloud is also highly recommended. Since most cloud providers do not accept older operating systems, make sure your organization's systems are updated before choosing to migrate to the cloud.

MOVING TO THE CLOUD

2. Choosing a Provider

When considering which cloud provider would suit your organization the best, it is important to make sure that the vendor can meet data security, accessibility, and portability expectations and requirements. Your policies and standards should be set to meet the level of security required by your organization. Some of your policies may need to be changed before moving to the cloud, hardening or softening rules. You may have to change virtual or physical applications to ensure high security is maintained when moving to the cloud.

User Experience

Accessibility to the user device and the cloud interface, whether app based or by a web browser, is important to a business. The cloud interface should provide ease and simplicity to the user, providing a positive user experience. It is best to also look at the ease of data portability, which can determine how your data is transferred. Your goal is to be able to easily transfer data through the cloud without having to re-enter data each time. There should be a capacity of retrieving data from one cloud service and transferring it to your target cloud service.

Data Backup & Recovery

Along with these requirements, it is critical that vendors meet both your data backup and recovery requirements. Having the proper backup and recovery in place is extremely important in the case of a compromise. Knowing how a vendor handles moving data from physical to virtual, along with its accessibility and ability to recover data in a new infrastructure is crucial. Understanding how exactly data is transferred will help with determining the security posture of the cloud provider.

MOVING TO THE CLOUD

3. Define Responsibilities

Be sure to examine each party's responsibilities. Typically, most vendors will have standard Service Level Agreements (SLAs) describing their responsibilities, such as uptime, recovery, and redundancy. Having defined roles and knowing what exactly the responsibilities of your vendor and your business are will help to ensure a smooth and functional operation.

Depending on the cloud service you choose, the shared responsibilities between you and the cloud provider will differ. It is your responsibility to choose the services that best fit your content, systems, and networks. In most cases, depending on the service you use, physical security, host infrastructure, and network controls are dependent on the provider. Accountability, client management, and end point protection are your responsibility. Other responsibilities, such as application controls or access management are shared responsibilities with your organization and vendor.

CLOUD SERVICES

Three Main Types of Cloud Services

Cloud providers offer cloud services that you can choose to best fit your needs.

1. Software-as-a-Service (SaaS):

This service is a software that is stored and used via the cloud. It offers users the simplicity of clicking an icon on the desktop that then connects to an application or web-browser; such as Microsoft 360. SaaS is the most widely accepted service by organizations because of its several advantages. SaaS offers an inexpensive method of connecting to the cloud. Many providers offer a subscription based cloud, so your organization can buy more or less depending on the number of connections needed/required. SaaS also takes away the inconvenience of storing and managing data because the software is stored and used in the cloud.

2. Infrastructure-as-a-Service (IaaS):

This service provides a virtual platform for remote connection and use, hosted by the cloud provider. Users connect to the virtual platform using the Remote Desktop Protocol (RDP) or another secure remote connection protocol. The users are then able to run applications, process data, create content, or perform other tasks using the virtual machine. Most organizations use IaaS as virtual servers because the responsibility of managing and maintaining server farms is turned to the provider.

3. Platform-as-a-Service (PaaS):

This service provides a computing platform, such as a web application server that can offer services internally and to customers via the internet. It can be used to give services both to the users and the customers over the internet. This service is usually used by online stores because it eliminates the need to maintain infrastructure such as, physical servers, databases, websites, or applications.

CLOUD SECURITY

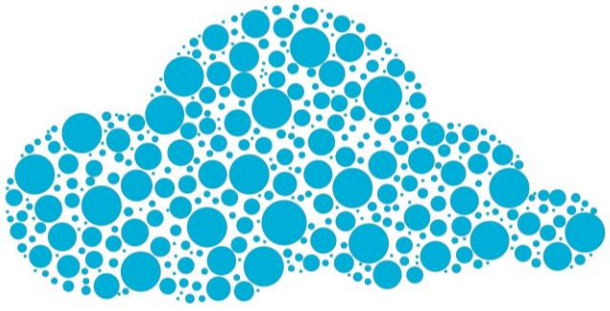
Security Concerns

Your clients, customers, partners, and associates are relying on you to ensure their information is safe. The complexity of today's systems is ever-increasing and the threats to your assets are real. Regular and continuous penetration testing and security reviews are best practice recommendations for any organization to meet a high-quality standard. As more companies select different SaaS, IaaS and PaaS platforms for their corporate environment, the security and compliance with regulatory requirements has become a major reason for transitioning to a cloud platform.

Vulnerabilities in cloud

Unlike traditional systems, cloud environments present a few security concerns. Many of the popular cloud providers, such as Amazon, Microsoft, Google, undoubtedly have a solid security in place - but it's important to remember that they are not infallible. In one scenario, multiple cloud-based applications that were each secure on their own, had to interact with each other, and this interaction caused user data to be exposed in the process.

Some of the most common vulnerabilities observed in cloud deployments are broken authentications and session management. Data needs to be secured both in transit and at rest and ensure that session identifiers are always protected. Other common vulnerabilities are insecure direct object references, security misconfiguration, sensitive data exposure, and missing function level access control. When conducting a penetration test in the cloud, these should be your primary targets.



THREATS IN THE CLOUD

Top ten threats and preventative measures

Although the cloud provides many advantages, it does come with some security concerns. OWASP has outlined the top ten threats found in the cloud. Recognizing and acting upon these threats can help minimize the security risks.

1. Cross Site Scripting (XSS)

XSS is considered as the most common weakness in web applications. It allows an attacker to inject client-side code, usually HTML or JavaScript into a web application. The script can look like this: <script> alert(1) </script>. XSS takes advantage of the trust between the user and the web application to inject the malicious code. The attacker sends a malicious code to the end user, the end user's browser executes the script because it believes the script is coming from a legitimate source. Allowing the XSS payloads to access cookies, session tokens, or other information. Turning off active scripting in your web browser can reduce risk of XSS, however this limits your ability to use dynamic websites.

2. Injections Flaws

Injection Flaws come as a close second. Anytime an application uses an interpreter, there is a risk of introducing an injection vulnerability into the system. Injection flaws spread malicious code through an application to other connected systems. An attacker can inject malicious commands or characters into the information that the web application is receiving, and pass on the infected information onto the external system that is then executed. These attacks target the operating system through system calls and the use of external programs using shell commands.

THREATS IN THE CLOUD

Top ten threats and preventative measures

3. Malicious File Execution

When a user uploads or inputs information on a webpage that is not administered correctly, it gives attackers the ability to bypass authorization and get access into the system. The attacker can remotely execute the code, install root kits, and compromise an entire system. All web applications that accept file names or files from the user are vulnerable to this type of attack. Additionally, if the compromised local user has administrator permissions on other system, the company's internal network could be easily compromised. To avoid malicious file execution the process begins in the design phase of the application. Make sure you have a well-written application that does not allow user input of any type images or XML and have firewall rules in place.

4. Insecure Direct Object Reference (IDOR)

IDOR occurs when an application exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. An attacker can manipulate direct object references to access other objects without authorization, unless an access control check is in place. Preventing IDOR depends on fixing the design of the web application by including access control and per user or session indirect references.

5. Cross Site Request Forgery (CSRF)

CSRF is a malicious attack that exploits web applications; an attacker forces the user of a web application to perform an unauthorized action. The "user" inputs unauthorized commands to trusted web application. This is quite similar to identity theft, as the attacker pretends to be the user and uses the user's identity to perform certain actions. To execute this attack, the user needs to already be authenticated to the secure site. To prevent CSRF, you can use a cryptographically generated token for the user session, so malicious web sites cannot obtain the user's credentials. Also, always encourage users to log out of secure web sites when they are done and to never save authentication information on the browser.

THREATS IN THE CLOUD

Top ten threats and preventative measures

6. Information Leakage and Error Handling

Web applications can accidently leak private information about the application, such as the configuration, data structures, or filenames. Information is generally leaked through error messages. You should disable or limit error handling and secure paths should have multiple outcomes that return similar error messages. Also, check and configure errors from all layers to prevent exploitations. Create a default error handler that return a sanitized error message.

7. Broken Authentication and Session Management

If session tokens or authentication functions are not managed properly, it will allow attackers to compromise passwords or session IDs. An attacker who has bypassed the authentication could view sensitive content provided by the application. Appropriate use of an authentication and session management mechanism can help lessen the problem. You should place restrictions on passwords which require a minimum size and complexity. There should also be a set number of times the user can attempt to log in. When users attempt to change their password, the system should require both the old and new password. Sessions should be protected with SSL and session IDs should be long and complicated.

8. Insecure Cryptographic Storage

Insecure cryptographic storage occurs when sensitive data is not properly secured. Attackers can break the keys and find cleartext copies or access data. It is important to encrypt all sensitive data. Ensure all offsite backups are encrypted and that the keys are backed separately. Key management policies should be maintained and use strong algorithms and keys. Strong algorithms should be used to hash passwords with a proper salt.

THREATS IN THE CLOUD

Top ten threats and preventative measures

9. Insecure Communications

Having insecure communications allows an attacker to sniff a network and gain access to the conversations, credentials, or transfer of private information. Properly encrypting all authenticated and sensitive communications is important. Without encrypting the channel, the developer can't guarantee the integrity of the data. Use SSL for all authenticated connections and those that are transmitting sensitive data. This applies to client to server, server to server, server to database communication, and any network communication where the Man in the Middle could listen to the communication.

10. Failure to Restrict URL Access

This vulnerability happens when application fails to have correct access control policies in place. Attackers can bypass security by accessing files or following direct links, allowing the attacker to get data source files directly. Also, use ACLs to forbid anonymous readings and do not let random web visitors have permission to read or gain access to any sensitive files. You should also define the file types for remote reading on the server and remove irrelevant files in the directory.

CLOUD PENETRATION TESTING

Defining the Scope

Defining the scope of the penetration test is essential. For example, if it is a public cloud, it is necessary to understand the precise point where the tenant and provider are separating from each other, while with a private cloud, it might be possible to do a full stack penetration testing. When conducting a penetration test in a cloud environment, it's essential to stay within the boundaries of their respective domains and cloud service model. A pentester also needs to evaluate the cloud stack starting from the facility that hosts the hardware, to the network, computer and storage, hypervisor, virtual machine, solution stack, the application, and the API or GUI. Based on all of the factors mentioned above, the pentester should be able to determine the precise scope of the test in terms of the various layers that are to be included.

Coordination

This is a very important step as most Cloud Service Providers (CSPs) do have different requirements and processes. Amazon, for example, makes it relatively easy to coordinate tests through an online tool. Others may have a more complicated process in place and can take longer - LIFARS recommends having an extra week added to your plan for this. The next step is to ensure that the tests you are planning to perform are in line with the CSP's policies. Due to the multitenant nature of cloud platforms, many CSPs do not allow tenants to perform certain types of attacks - such as DoS and other exploits and scans that use up a lot of shared resources.

Pivoting

Advanced pentests often include the exploitation of one application or system and using it to perform other attacks against other systems or applications. This is called pivoting. Pivoting is allowed by CSPs most of the time, but most do not allow pivoting out of the cloud to perform an attack on an outside system.

OTHER CONSIDERATIONS

Multi-vendor approach

A multi-vendor network provides the ability to select the best solution to align an organization's infrastructure strategy with its business requirements based upon open standards. Having a wider range of options allows the user the flexibility to be selective when choosing which solution to deploy. Since the network is a major aspect of an organization's business strategy, organizations should not have to settle for a solution that does not meet all their requirements due to vendor limitations. A multi-vendor strategy enables a best-of-breed solution, allowing for a sustainable and high performing network environment.

A benefit to networks built upon open standards is that they can adopt new solutions as an organization continues to grow or as new and improved solutions are released. Since a multi-vendor strategy is essentially an open standards strategy, vendors must continue to create new advances to maintain a competitive edge.

Increasingly, businesses continue to outsource network security functions because it is less costly than having an onsite staff of security personnel to provide incident detection and response. Not only will outsourcing reduce business expenses, it will also free up existing IT resources to focus on other business functions.

Having multi-vendor, defense-in-depth approach can further secure an organization's operations by supporting mission critical applications, improving upon operational efficiencies and increasing business productivity.

THE LIFARS DIFFERENCE

Customized Solutions

LIFARS' experienced team will assess your existing environments and will help select the right solutions and configurations to align with the same level of security in the cloud as expected in your data center.

Configuration

After scanning for security gaps, vulnerabilities, and data leakage, LIFARS will review and communicate the recommended configuration of your SaaS, IaaS and PaaS to create a secure environment and improve the overall security posture.

Malware Risk

Each platform is a new channel into your configuration that could allow hackers the ability to gain access and exploit. It is crucial that your loads in IaaS and PaaS have the right security measures set in place.

Data Protection

The cloud makes it too easy for information that was either uploaded or shared, to fall into the wrong hands. Scanning your cloud and flagging sensitive information is part of what we do to ensure quality monitoring and data protection.

Compliance

Classifying your data and your users is the first part of building a compliant cloud. The second half is to tie them into a policy that includes auditing and reporting of incidents and a workflow to remediate or mitigate those incidents. LIFARS will provide turn-key policies specifically tailored to your compliance requirements and will work with you to adjust and implement them into your organization.

Manage Security as a Service

LIFARS can also assist your organization with continued managed services of these solutions. Our team can work as an extension of your team, implementing security solutions, auditing, and reporting the workflows – manual or automatic in a time-limited process.

FROM STRATEGY TO INCIDENT RESPONSE

LIFARS & Avanan

Assessing your own systems for security gaps and vulnerabilities is essential for any organization operating (even partially) in the digital realm. As a result, many cloud providers now offer cloud security services. This is why LIFARS leverages cloud security specialist, Avanan, to provide a cohesive, joint cloud security service to ensure oversight and instant response in the case of a compromise. Avanan knows that “Data can be more secure in the cloud than it is on the network.”

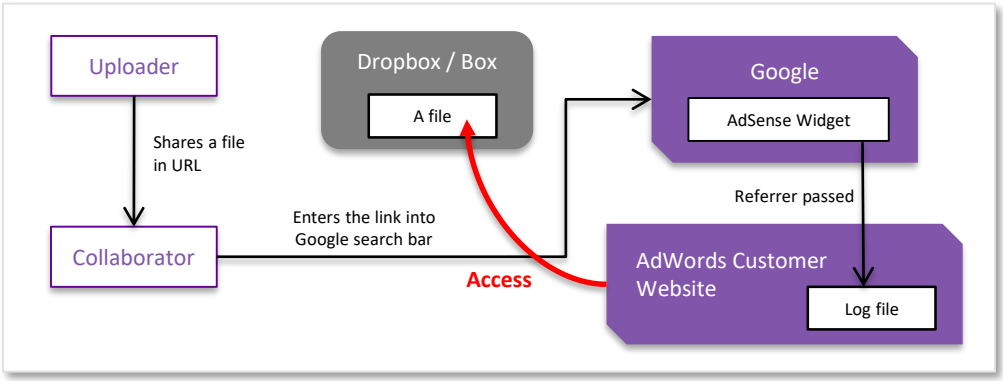
CASE STUDY

Background

In 2014, LIFARS learned that file storage cloud services, such as Dropbox and Box, can put customers' security at risk as users can unintentionally leak their own files. Using Google Analytics to review a number of campaigns, LIFARS team inadvertently discovered that users' links were being exposed, making personal or business information accessible.

LIFARS Research

LIFARS team found that a Google Adwords Campaign originator can capture shared links pointed to stored data on Dropbox or Box. Google allows these campaign originators to have access to what users have previously searched for advertising purposes. This means that if a user enters the shared URL into Google search bar, companies with Google' advertising service will be able to access the shared files and folders.



[Figure 1] Vulnerabilities of shared file in file sharing applications

Tips on using cloud file sharing applications

LIFARS recommends a few helpful tips for those who use cloud file sharing applications.

- Ensure the application provides privacy setting options, only allows those you specifically invite, to have access to files you are sharing
- Make sure the system has an authentication that requires users to identify themselves
- Delete old files that you no longer need. If your file sharing application is not security enabled, we recommend you to create a new account with security enabled
- Don't combine your work and personal files in a single account. Losing company data can have severe consequences: lost reputation, legal issues, and fines

CASE STUDY

ServiceSource Safely Secured

As of December, 2016, ServiceSource has secured their cloud with Avanan. ServiceSourse is a life-cycle company that provides outsourced customer adoption and expansion for subscription-based businesses. Kip James, ServiceSource's Chief Information Security Officer and Data Privacy Officer, realized that there were limitations to the data center security products they were using to protect their information in the cloud. Previously, they used security products such as antivirus, malware protection, sandboxing, and data leakage prevention, but they needed more protection.

Solutions

Kip selected Avanan's platform because Avanan is one of the few companies that offers a product that understands the security status of all the information stored in the cloud. With Avanan, Kip was able to:

- See who was sharing what with whom and events across all security products
- Understand the status of SaaS application and cloud storage information
- Alerts to determine if there are attempts to share sensitive information outside the organization
- Try new security products with a click of a mouse in the Platform

Results

"I turned on everything with just a simple click in Avanan just to see what it would do– antivirus, malware sandboxing, DLP, anomaly detection, you name it." Kip said.

Today, ServiceSource is fully equipped with data loss prevention mechanism and top-notch visibility into when sensitive data is being shared, and any risks that may be associated with it. With Avanan, the organization can try new products to identify those that best suit their organizational needs before making a commitment to any.

LIFARS

your digital world, **secured**

Contact Us to Learn More

www.lifars.com | 212.222.7061 | info@lifars.com | Twitter: @LIFARSLLC

LIFARS is an Elite Cybersecurity Intelligence firm based in New York City specializing in: Incident Response, Digital Forensics, and Cybersecurity Intelligence.