IDERA® | Cloud Whitepaper

THE COMPLICATIONS OF CYBER-SECURITY IN THE CLOUD

THE COMPLICATIONS OF CYBERSECURITY IN THE CLOUD

Cloud computing services offer many advantages for companies or organizations that make use of them. There are often financial incentives involved in cloud migrations, as the provider's ability to use an economy of scale solution results in cost savings for their customers. Enterprises can engage cloud providers to enhance their computing capabilities with technologies such as artificial intelligence (AI) or machine learning (ML) that in-house resources cannot attain. The flexibility inherent in the virtualization underlying the cloud computing paradigm allows companies to fine-tune their requirements and only pay for the resources that they need.

Along with these benefits come the challenges introduced by having enterprise computing resources in multiple locations. It is not uncommon for an organization to have an on-premises data center and cloud instances housed by multiple providers. This puts additional stress on an Information Technology (IT) team trying to maintain high levels of availability and performance. They need to divide their attention between the various platforms used to deliver their solutions. It can be a hard balancing act to keep going.

Security is an area that demands a laser-like focus in any computing environment. Lack of cybersecurity can cause degraded availability and performance with the associated negative impacts on business. It also opens the gate for an organization's data assets to be compromised. Security can be seen as the most important aspect of an organization's computing resources. Without it, everything else is just a house of cards at risk of collapsing at any moment.

The factors that complicate security are the same as the factors that impact managing enterprise computing resources in the cloud. The split-screen nature of keeping tabs on multiple platforms and providers introduces additional possibilities for mistakes.

SECURITY RISKS OF CLOUD COMPUTING

Many security risks can afflict customers making use of cloud services. The Cloud Security Alliance (CSA) published its most recent guide to the top threats in cloud computing in August 2019. It spells out the range of risks that needs to be addressed when making use of the cloud.

DATA BREACHES

A data breach is perhaps the most feared type of security issue that an organization can face. At the very least, valuable corporate or business data may be at risk. In the worst-case scenario, personally identifiable information on customers and employees is compromised. Both cases can cause serious financial damage to the affected entities. A company can have their reputation tarnished following a data breach with a loss of future business that is hard to quantify and harder to repair.

Data breaches can occur for many reasons, ranging from inadequate network protection to credentials compromised through a phishing attack. The additional connections required to facilitate a cloud infrastructure and introducing personnel not under the control of the customer result in the need for a greater emphasis on guarding against a data breach.

MISCONFIGURATION AND INADEQUATE CLOUD SECURITY ARCHITECTURE

A single mis-configured system can cause an open door that allows the total infrastructure to be compromised. Cloud-based resources are complex and prone to configuration errors. Enhanced change management processes are required to verify changes made to cloud instances.

Containers are lightweight virtual machines with a low overhead that are replacing traditional virtualization techniques. They are used extensively in cloud computing as vehicles to streamline the deployment of new systems and instances. Mis-configured containers can quickly be replicated throughout an environment, making it essential that they are thoroughly verified before being reused.

INSUFFICIENT ACCESS CONTROL AND MANAGEMENT

Migrating computing resources to the cloud exposes an organization's environment to entities outside of their direct control. A modified approach to identity and access management (IAM) is required to address the increased risk of unauthorized access or data breaches.

The principles of IAM are the same when used with cloud resources as when used in more traditional settings. Specifically, issues that can cause weakened cybersecurity include failing to implement multi-factor authentication and inadequately protecting credentials. The absence of an automated rotation process designed to safeguard passwords and keys allows unauthorized personnel to access systems and data inappropriately. Failure to implement a policy that demands strong passwords for anyone accessing enterprise systems is another issue resulting from lax IAM standards.

HIJACKED ACCOUNTS AND INSIDER THREATS

Account hijacking and the inappropriate use of authorized privileges are two related threats that can affect systems in the cloud and those in on-premises data centers. Attackers hijack accounts when they get privileged user credentials. This can be done by various means including email phishing or compromising the cloud service and stealing the required information.

Insider threats can either be malicious or negligent. Systems are exposed to additional personnel when involving cloud service providers. This introduces more hands that can purposely or accidentally cause problems or access sensitive data that they are not authorized to handle.

INSECURE INTERFACES AND APIS

Interfaces and application programming interfaces (APIs) are necessary evils that allow valid users to access enterprise computing resources. They are also commonly used to attack computer systems. These components represent the most exposed parts of a system and offer hackers an avenue for stealing credentials that can be used for further exploitation of the environment. Security must be considered during their design.

LIMITED VISIBILITY INTO CLOUD USAGE

The inability to gain full visibility into how the resources in the cloud environment are being used is a problem that can lead to two types of security issues. One problem is the use of unsanctioned applications running on the cloud infrastructure. This issue gives rise to the concept of shadow IT,

where employees use applications that do not meet corporate standards for legitimate support purposes. The inability to meet the organizational guidelines makes the use of these applications a security risk to the whole environment.

In a similar vein, authorized personnel can misuse valid applications or valid applications can be misused through the use of stolen credentials. Uncovering the misuse of computing resources requires a deep understanding of the accepted user behavior and a process for identifying and addressing anomalies. It can be a fine line between acceptable and inappropriate usage that can be difficult to detect.

CRYPTOJACKING

Cryptojacking is a recent addition to the hacker arsenal and is seen as an easier way to extract financial gain from an enterprise than using ransomware. It works by hijacking some of an organization's computing resources, which are then used to mine for cryptocurrency. This infection results in fewer central processing unit (CPU) cycles available to approved applications.

It can be difficult to identify systems that are affected by cryptojacking since they continue to operate, although with degraded performance. In a complex cloud infrastructure, many factors can impact performance. Sometimes, the degradation may be blamed on a slow network or faulty upgrade. Cryptojacking is a specific example of unsanctioned apps wielded by unknown entities outside the control of the client or cloud provider.

SHARED SECURITY RESPONSIBILITIES IN THE CLOUD

The customer and the provider perform cloud security through a collaboration. It is not an equitable partnership, as the customer is often responsible for securing most of the components in the environment. With a data breach, it will be the customer who needs to clean up the mess no matter who was ultimately at fault for the issue. Therefore, the customer needs to take the necessary steps to ensure that security is fully implemented throughout their infrastructure.

The delineation of duties varies based on the cloud delivery model in use. All major cloud vendors use the same method of dividing the responsibilities for securing an organization's computing resources. The degree of responsibility placed on the customer is directly proportional to the amount of flexibility and control they exert over the environment.

- Infrastructure as a Service (IaaS) is the cloud computing model that affords customers the greatest level of control over resources procured from a cloud provider. The provider is responsible for the networking, storage, servers, and virtualization that defines the foundation of the infrastructure. Customers are tasked with providing security for the operating systems, middleware, runtime, applications, and data that are used to extract value from the infrastructure.

- Platform as a Service (PaaS) presents a more fully formed computing environment in which customers run their applications. The cloud service provider is responsible for the same aspects of security as in the IaaS model and has to lock down the network, storage devices, and physical and virtual servers. Responsibility for runtime, middleware, and operating system security is transferred from the customer to the provider. The client maintains responsibility for securing the applications and data that make use of the platform provided by the cloud vendor.

- Software as a Service (SaaS) is the model that puts most responsibility for security with the cloud provider. This means that all aspects of the environment except for customer data is expected to be secured by the cloud service. Since a software application is part of the provider's offering, they are the ones who need to keep it secure, removing this aspect of security from the customer.

Organizations must understand where the lines are drawn with their cloud providers regarding security responsibilities. The general outlines that apply to the different cloud models need to be codified in the agreements signed between the two parties. This process needs to be repeated as new services are migrated to the cloud infrastructure. It is never safe to assume that the same level of protection will be provided without verification from the vendor.

BEST PRACTICES TO ENSURE SECURE CLOUD ENVIRONMENTS

The risks involved with using cloud service providers demand a set of best practices to maintain vigilant cybersecurity and keep enterprise computing and data resources protected and available. Many of these methods also apply to on-premises environments but are even more important with the complexity of cloud infrastructures and the additional opportunities they present for attack.

UNDERSTANDING SHARED SECURITY RESPONSIBILITIES

Knowledge is power, and this is true when implementing cloud security. It is critically important for an enterprise to know exactly where the responsibility for securing various aspects of the environment lies. This is not an issue where guesswork or assumptions are sufficient. The well-being of an organization depends on a thorough understanding of the differences between who is responsible for which parts of the computing environment.

DATA PROTECTION

The common responsibility in all cloud models is application data. In all cases, the customer is tasked with securing their data. This should be done by implementing policies that ensure the data is encrypted when at rest and in transit. There are situations where encrypting data may lead to performance degradation, but in the grand scheme of things customers need to accept this tradeoff.

When choosing between the security of data and the performance of the systems that use it, security must be emphasized. The customer should control the keys that are required to unlock the encrypted data. Encryption should also be mandated for backups to further protect the data from unauthorized entities. Fully encrypted backups of all customer data should be part of any cloud implementation.

ENHANCED ACCESS MANAGEMENT

Two related ideas any organization should practice with a cloud computing presence are the concept of zero trust and the principle of least privilege. They are the building blocks used to develop identity and access management controls that provide enhanced cloud security to the infrastructure and its data.

The zero trust model of security mandates that there are no trusted entities. It demands authorization throughout a user engagement with a computing environment. What this means in practice is that merely gaining access to an infrastructure does not enable a user to use its resources indiscriminately. Authorization must be verified at each step of the engagement through a more granular approach to access management that uses technologies like multi-factor authentication and analytics.

The principle of least privilege complements the zero trust security model by minimizing the level of access enjoyed by a particular user. It limits user privileges to the bare necessities required to perform their role in the organization. Higher levels of access can be provided for specific tasks and then immediately revoked according to organizational policies.

Frequent audits of user privileges are highly recommended to enforce robust access management. This includes modifications that are required as individual roles within an organization change. It also extends to the timely removal of accounts that are no longer needed because of employees leaving the enterprise. Keeping dormant credentials should never be tolerated as they present a dangerous entry-point into otherwise secure systems.

MONITORING STRATEGY

An all-encompassing monitoring strategy can be one of the best defenses of cloud computing implementations. Many of the issues that are difficult to identify can be addressed through a strong monitoring policy. At its most basic level, monitoring will alert organizations to attempts by unauthorized entities to gain access to their resources. Networks, systems, and applications should all be in scope for monitoring whether the responsibility for securing them falls to the customer or the cloud provider. There is no harm and there can be potentially significant gains for clients who monitor all aspects of the infrastructure, regardless of who is providing security.

Problems such as cryptojacking or identifying the use of unsanctioned applications can be addressed through the use of historical monitoring where baselines are constantly compared to current usage patterns. Using these tactics, anomalies that otherwise escape notice can be discovered and promptly addressed. This strengthens security and ensures that customers are not paying for resources that are being used for unapproved purposes.

The challenge of maintaining cybersecurity in the cloud is a multi-faceted process that requires the cooperation of the customer and cloud provider. Organizations should never lose sight of the fact that they are responsible for the security of their systems and data. There can never be too great an emphasis put on securing the cloud systems they use.