**Misconfiguration**

Misconfigurations of cloud security settings are a leading cause of cloud data breaches. Many organizations’ cloud security posture management strategies are inadequate for protecting their cloud-based infrastructure.

Several factors contribute to this. Cloud infrastructure is designed to be easily usable and to enable easy data sharing, making it difficult for organizations to ensure that data is only accessible to authorized parties. Also, organizations using cloud-based infrastructure also do not have complete visibility and control over their infrastructure, meaning that they need to rely upon security controls provided by their cloud service provider (CSP) to configure and secure their cloud deployments. Since many organizations are unfamiliar with securing cloud infrastructure and often have multi-cloud deployments – each with a different array of vendor-provided security controls – it is easy for a misconfiguration or security oversight to leave an organization’s cloud-based resources exposed to attackers.

**Unauthorized Access**

Unlike an organization’s on-premises infrastructure, their cloud-based deployments are outside the network perimeter and directly accessible from the public Internet. While this is an asset for the accessibility of this infrastructure to employees and customers, it also makes it easier for an attacker to gain unauthorized access to an organization’s cloud-based resources. Improperly-configured security or compromised credentials can enable an attacker to gain direct access, potentially without an organization’s knowledge.

Insecure Interfaces/APIs

CSPs often provide a number of application programming interfaces (APIs) and interfaces for their customers. In general, these interfaces are well-documented in an attempt to make them easily-usable for a CSP’s customers.

However, this creates potential issues if a customer has not properly secured the interfaces for their cloud-based infrastructure. The documentation designed for the customer can also be used by a cybercriminal to identify and exploit potential methods for accessing and exfiltrating sensitive data from an organization’s cloud environment.

**Hijacking of Accounts**

Many people have extremely weak password security, including password reuse and the use of weak passwords. This problem exacerbates the impact of phishing attacks and data breaches since it enables a single stolen password to be used on multiple different accounts.

Account hijacking is one of the more serious cloud security issues as organizations are increasingly reliant on cloud-based infrastructure and applications for core business functions. An attacker with an employee’s credentials can access sensitive data or functionality, and compromised customer credentials give full control over their online account. Additionally, in the cloud, organizations often lack the ability to identify and respond to these threats as effectively as for on-premises infrastructure.

**Lack of Visibility**

An organization’s cloud-based resources are located outside of the corporate network and run on infrastructure that the company does not own. As a result, many traditional tools for achieving network visibility are not effective for cloud environments, and some organizations lack cloud-focused security tools. This can limit an organization’s ability to monitor their cloud-based resources and protect them against attack.

**External Sharing of Data**

The cloud is designed to make data sharing easy. Many clouds provide the option to explicitly invite a collaborator via email or to share a link that enables anyone with the URL to access the shared resource.

While this easy data sharing is an asset, it can also be a major cloud security issue. The use of link-based sharing – a popular option since it is easier than explicitly inviting each intended collaborator – makes it difficult to control access to the shared resource. The shared link can be forwarded to someone else, stolen as part of a cyberattack, or guessed by a cybercriminal, providing unauthorized access to the shared resource. Additionally, link-based sharing makes it impossible to revoke access to only a single recipient of the shared link.

**Malicious Insiders**

Insider threats are a major security issue for any organization. A malicious insider already has authorized access to an organization’s network and some of the sensitive resources that it contains. Attempts to gain this level of access are what reveals most attackers to their target, making it hard for an unprepared organization to detect a malicious insider.

On the cloud, detection of a malicious insider is even more difficult. With cloud deployments, companies lack control over their underlying infrastructure, making many traditional security solutions less effective. This, along with the fact that cloud-based infrastructure is directly accessible from the public Internet and often suffers from security misconfigurations, makes it even more difficult to detect malicious insiders.

**Cyberattacks**

Cybercrime is a business, and cybercriminals select their targets based upon the expected profitability of their attacks. Cloud-based infrastructure is directly accessible from the public Internet, is often improperly secured, and contains a great deal of sensitive and valuable data. Additionally, the cloud is used by many different companies, meaning that a successful attack can likely be repeated many times with a high probability of success. As a result, organizations’ cloud deployments are a common target of cyberattacks.

**Denial of Service Attacks**

The cloud is essential to many organizations’ ability to do business. They use the cloud to store business-critical data and to run important internal and customer-facing applications.

This means that a successful Denial of Service (DoS) attack against cloud infrastructure is likely to have a major impact on a number of different companies. As a result, DoS attacks where the attacker demands a ransom to stop the attack pose a significant threat to an organization’s cloud-based resources.

Main Cloud Security Concerns in 2021

In the Cloud Security Report, organizations were asked about their major security concerns regarding cloud environments. Despite the fact that many organizations have decided to move sensitive data and important applications to the cloud, concerns about how they can protect it there abound.

**Data Loss/Leakage**

Cloud-based environments make it easy to share the data stored within them. These environments are accessible directly from the public Internet and include the ability to share data easily with other parties via direct email invitations or by sharing a public link to the data.

The ease of data sharing in the cloud – while a major asset and key to collaboration in the cloud – creates serious concerns regarding data loss or leakage. In fact, 69% of organizations point to this as their greatest cloud security concern. Data sharing using public links or setting a cloud-based repository to public makes it accessible to anyone with knowledge of the link, and tools exist specifically for searching the Internet for these unsecured cloud deployments.

**Data Privacy/Confidentiality**

Data privacy and confidentiality is a major concern for many organizations. Data protection regulations like the EU’s General Data Protection Regulation (GDPR), the Health Insurance Portability and Accessibility Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and many more mandate the protection of customer data and impose strict penalties for security failures. Additionally, organizations have a large amount of internal data that is essential to maintaining competitive advantage.

Placing this data on the cloud has its advantages but also has created major security concerns for 66% of organizations. Many organizations have adopted cloud computing but lack the knowledge to ensure that they and their employees are using it securely. As a result, sensitive data is at risk of exposure – as demonstrated by a massive number of cloud data breaches.

**Accidental Exposure of Credentials**

Phishers commonly use cloud applications and environments as a pretext in their phishing attacks. With the growing use of cloud-based email (G-Suite, Microsoft 365, etc.) and document sharing services (Google Drive, Dropbox, OneDrive), employees have become accustomed to receiving emails with links that might ask them to confirm their account credentials before gaining access to a particular document or website.

This makes it easy for cybercriminals to learn an employee’s credentials for cloud services. As a result, accidental exposure of cloud credentials is a major concern for 44% of organizations since it potentially compromises the privacy and security of their cloud-based data and other resources.

**Incident Response**

Many organizations have strategies in place for responding to internal cybersecurity incidents. Since the organization owns all of their internal network infrastructure and security personnel are on-site, it is possible to lock down the incident. Additionally, this ownership of their infrastructure means that the company likely has the visibility necessary to identify the scope of the incident and perform the appropriate remediation actions.

With cloud-based infrastructure, a company only has partial visibility and ownership of their infrastructure, making traditional processes and security tools ineffective. As a result, 44% of companies are concerned about their ability to perform incident response effectively in the cloud.

**Legal and Regulatory Compliance**

Data protection regulations like PCI DSS and HIPAA require organizations to demonstrate that they limit access to the protected information (credit card data, healthcare patient records, etc.). This could require creating a physically or logically isolated part of the organization’s network that is only accessible to employees with a legitimate need to access this data.

When moving data protected by these and similar regulations to the cloud, achieving and demonstrating regulatory compliance can be more difficult. With a cloud deployment, organizations only have visibility and control into some of the layers of their infrastructure. As a result, legal and regulatory compliance is considered a major cloud security issue by 42% of organizations and requires specialized cloud compliance solutions.

**Data Sovereignty/Residence/Control**

Most cloud providers have a number of geographically distributed data centers. This helps to improve the accessibility and performance of cloud-based resources and makes it easier for CSPs to ensure that they are capable of maintaining service level agreements in the face of business-disrupting events such as natural disasters, power outages, etc.

Organizations storing their data in the cloud often have no idea where their data is actually stored within a CSP’s array of data centers. This creates major concerns around data sovereignty, residence, and control for 37% of organizations. With data protection regulations such as the GDPR limiting where EU citizens data can be sent, the use of a cloud platform with data centers outside of the approved areas could place an organization in a state of regulatory non-compliance. Additionally, different jurisdictions have different laws regarding access to data for law enforcement and national security, which can impact the data privacy and security of an organization’s customers.

**Protecting the Cloud**

The cloud provides a number of advantages to organizations; however, it also comes with its own security threats and concerns. Cloud-based infrastructure is very different from an on-premises data center, and traditional security tools and strategies are not always able to secure it effectively. For more information about leading cloud security issues and threats, download the Cloud Security Report.

Source:

<https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/>