Cloud Security Weaknesses

A bluedog Whitepaper

bluedog
SECURITY MONITORING

Cloud Security Weaknesses

Executive Summary

More and more data and operations are moved to the cloud every day. With increased cloud adoption come increased threats.

Even more significantly, these are brand new threats to match the brand new cloud solutions that we use.

Cloud computing has transformed the way organizations use, store, and share their data and their application. There is an unparalleled amount of data going in and out of the cloud today (and especially in and out of the public cloud). Cloud-stored data is a precious resource – for both its owners and for attackers.

Contrary to popular belief, the responsibility to protect cloud-stored corporate data doesn't lie with the cloud provider, but mostly with the data owner – the companies using cloud services.

This whitepaper analyzes the current state of cloud security and the top weaknesses in this field so that corporate data owners know what to look for when choosing a cloud provider. The next chapter will shed some light on the current industry standards for cloud security. This will help you make better decisions when it comes to your data and it will also explain what you can do to make sure it is secure.

Table of Contents

The State of Cloud Security

By the end of 2020, 67% of enterprise architecture will be cloud-based and so will 82% of the workload. This will result in over 40 zettabytes of data flying more or less freely in the cloud[1].

The incredible growth spur of the cloud industry prompted the birth of additional sub-industries, the so-called "as-a-services/aaS" ones. SaaS, iPaaS, NaaS are just a few of them. And, unsurprisingly, they also grow at an accelerated pace.

Table 1. Worldwide Public Cloud Service Revenue Forecast (Millions of US Dollars)

	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	45,212	43,438	46,287	49,509
Cloud Application Infrastructure Services (PaaS)	37,512	43,498	57,337	72,022
Cloud Application Services (SaaS)	102,064	104,672	120,990	140,629
Cloud Management and Security Services	12,836	14,663	16,089	18,387
Cloud System Infrastructure Services (IaaS)	44,457	50,393	64,294	80,980
Desktop as a Service (DaaS)	616	1,203	1,951	2,535
Total Market	**242,697**	**257,867**	**306,948**	**364,062**

= infrastructure as a service; PaaS = platform as a service; SaaS = software as a service

Note: Totals may not add up due to rounding.

Image Source[2]

Of course, this amount of data couldn't have gone unnoticed by attackers.

This is why almost two thirds of organizations see security as the biggest hurdle in adopting cloud solutions[3]. At the same time, 75% of security experts say that managing data privacy and protection in the cloud is more complicated than on premises[4].

---

[1] https://techjury.net/blog/cloud-computing-statistics/, retrieved October 2020
[2] https://www.information-age.com/public-cloud-revenue-to-grow-6-3-in-2020-gartner-123490499/, retrieved October 2020
[3] https://hostingtribunal.com/blog/cloud-computing-statistics/#gref, retrieved October 2020

This difficulty in managing and mitigating security issues led to 70% of companies that adopted cloud solutions to experience a security incident. 44% of these companies state that data loss or data leakage is their top concern. However, 66% of them also leave backdoors open to attackers through misconfigured cloud services and settings[5].

Things aren't as bleak as they seem, though. Gartner predicts that, in the near future, IaaS (Infrastructure as a Service) will have 60% fewer security incidents than traditional data centers. At the same time, 95% of cloud security incidents will be caused by users by 2022[6]. Cloud providers already know what they need to do to ensure security. Their efforts grow more successful every day.

As stated before, it's mostly up to the users (the data-owning corporations or the individual end users to ensure that they uphold their end of the bargain in cloud security).

The following chapters discusses the most common cloud security threats – the ones all companies, irrespective of their size, should be aware of.

Top Cloud Security Weaknesses

As it happens with on-prem security threats, cloud security ones aren't all made equal. Depending on the type of data you store in the cloud, how you use it and what type of cloud services you use most often, your security weaknesses are different.

---

[4] Ibidem
[5] https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx, retrieved October 2020
[6] https://hostingtribunal.com/blog/cloud-computing-statistics/#gref, retrieved October 2020

However, there are a few types of cloud security issues that are common and frequent[7] in most cloud-reliant organizations.

Let's review them!

Data Breaches

An average of 4800 websites are compromised every month with formjacking code[8]. The number of health data breaches alone increased by 70% from 2017 to 2019[9].

A data breach is incredibly dangerous as it takes an average of 209 days to identify and 73 days to contain[10]. During this time, the financial and reputation losses are hard to measure.

The key elements of preparing for a data breach are:

- Define the value of your data and the impact its loss can have on your business. Remember than attackers are after data!
- Clearly specify who has access to the data. This is the most important aspect of protecting it.
- Internet-facing or internet-available data is the most accessible to breaches and misconfigurations, so always start there!
- You can use encryption to protect your data, but that usually comes at the cost of usability.
- The best way to avoid data breaches or to contain them rapidly is a robust incident response plan that takes your cloud provider into account

Misconfiguration and/or Improper Change Control

The Exactis incident leaked the personal information of more than 340 million records[11]. This huge database was left publicly accessible due to a misconfiguration error.

---

[7] https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven, retrieved October 2020

[8] https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf, retrieved October 2020

[9] https://www.statista.com/statistics/798564/number-of-us-residents-affected-by-data-breaches/, retrieved October 2020

[10] https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260, retrieved October 2020

[11] https://www.wired.com/story/exactis-database-leak-340-million-records/, retrieved October 2020

The loss of data is not the only thing to worry about here. More harmful attacks can also alter or delete data records with the explicit intent of causing disruptions to your business.

What can you do?

- Understand that the complexity of cloud solutions makes it impossible to use traditional control and change management methods.
- Use cloud-appropriate technologies that continuously scan for misconfigured items.

Inadequately Protected Credentials, Identity, and Key Management

IAM (Identity and Access Management) gets tricky when you can't access the physical server room. This makes it all the more important.

Think about your email account: having a strong password means nothing if you share it with a lot of people, especially online, or if you store it improperly.

The same goes for cloud IAM.

Cloud security weaknesses stem from insufficient identity and credential protection, lack of automated rotation of cryptographic keys, passwords, and certificates, lack of multi-factor authentication, weak passwords, and so on.

How can you mitigate these risks?

- Always use two-factor authentication.
- Limit the number of root accounts and their use.
- Segment and separate your accounts based on business needs and the principle of the least privileged.
- Always remove obsolete or unused credentials and privileges.
- Approach key rotation in a centralized manner.

Account Hijacking

22% of the breaches in 2020 involved phishing[12]. As phishing attacks get more targeted and more sophisticated, accounts get hijacked easier.

Of course, phishing is not the only way an attacker can gain access to a corporate account. They can also acquire the credentials by compromising the cloud service or by other means. Whatever the means of entry, as soon as the attacker has a legitimate corporate account to use, the damage they can cause is huge: disruption of business, financial fraud, data theft, and data destruction are just a few of the things you can expect.

Here's how to avoid this:

- A password reset is not enough when the credentials have been stolen. Investigate and address the root causes.
- Invest in and actively monitor IAM controls.

Insider Threats

66% of organizations think that malicious or accidental insider threats are more likely to happen than outsider ones. Two out of three such threats are caused by negligence. In the past two years, such threats have grown by 47%[13].

Insider threats can come from current or former employees, business partners, contractors, suppliers, or any other stakeholder that doesn't need to break through a company's defenses to gain access. It is worth to note, though, that, as the statistics above show, an insider doesn't need to have malicious intent to cause a threat.

Quite the opposite, in fact. Most often, an employee or a business partner doesn't want to expose your data or information to public access. They do it out of neglect or lack of knowledge of security best practices.

Here's how to mitigate insider threats:

- Make employee training and education on best security practices a regular and ongoing process.
- Restrict access to critical systems on a need basis.
- Regularly review, audit, and repair misconfigured cloud servers.

[12] https://www.tessian.com/blog/phishing-statistics-2020/, retrieved October 2020
[13] https://techjury.net/blog/insider-threat-statistics/, retrieved October 2020

Insecure APIs or Interfaces

The 2018 Facebook breach was intensely discussed because it exposed the information of more than 50 million accounts[14]. Why did this happen?

From what we know, the security breach was caused by a vulnerability introduced by the social media service in its *View As* feature. Such vulnerabilities are extremely dangerous because, when associated with API ones, they give attackers and unobstructed path to stealing user or employee records.

This is to be expected, since both APIs and user interfaces are the most exposed parts of any system. This is why iron-clad security has to be built-in, from the design phase.

Other steps you can take to secure them include:

- Avoid the reuse of your API keys and always protect them.
- Always abide by good API practices. Ensure the oversight of key items like inventory, auditing, abnormal activity protection and testing.
- Consider using an open API framework for extra security.

Best Practices to Mitigate Cloud Security Weaknesses

Aside from the tips underlined in the previous chapter, there are a few general things you can do to mitigate the most common cloud security weaknesses.

[14] https://www.csoonline.com/article/3310041/facebook-50-million-accounts-impacted-by-security-flaw.html, retrieved October 2020

Identify Data that Is Very Sensitive or Regulated

The breach of certain data can lead to loss of intellectual property. When other types of data are breached, you stand to get regulatory penalties.

Data that falls under the GDPR European rule is something that should be heavily protected, for instance. Remember that the protection of your customers' and employees' data is your responsibility, not that of your cloud provider.

Are you compliant with international data privacy laws? Bluedog Security Monitoring has a dedicated Compliance service[15] to keep your sensitive data safe and make sure you don't stand to incur fines.

Make Sure You Understand How Your Data Is Being Used and Shared

Your data can be 100% safe in the cloud. But only if you regularly monitor who accesses it and how it is shared and used.

Make sure you perform regular assessments on permissions on your cloud-based files and folders. User roles and location along with the device types they used should be information you always have access to.

Uncover Unknown Cloud Use

Remember what we said about the dangers of insider threats and how they are not usually malicious? This is the safest gateway into your cloud data. Your employees typically don't ask IT before signing up for a cloud service or converting a PDF online.

This is why you need to run regular vulnerability scans[16] and phishing simulations[17] to uncover threats before they turn into real attacks. Your SIEM logs, firewall or proxy settings are also great at revealing what cloud services are being used without your knowledge and could potential signify risky online behavior.

---

[15] https://bluedog-security.com/compliance/, retrieved October 2020
[16] https://bluedog-security.com/vulnerability-scanning/, retrieved October 2020
[17] https://bluedog-security.com/phishing-simulations/, retrieved October 2020

Detect Malicious or Reckless User Behavior Early

Malicious use of cloud data can sometimes be associated with something as simple as a careless employee. Run regular UBA (User Behavior Analytics) to detect anomalies early on. This can help you prevent attacks before they happen.

A good way to identify your most vulnerable spots is penetration testing[18]. Through this procedure, you can find out which of your cloud and on-premise systems are at risk for insider and outsider attacks.

Protect Your Microsoft Office 365 Credentials

Microsoft Office 365 comes with a ton of benefits to your business (ease of file access, easy version control, and so on), but also with brand-new security challenges.

The login credentials can be easily stolen in a data breach. Once the attacker has access to an Office 365 account, they can wreak havoc on your company's extended network.

Make sure you protect every access gateway. The Bluedog Microsoft® Office 365™ Monitoring Service[19] is designed to render the use of such a powerful cloud-based tool stress-free.

About Bluedog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

[18] https://bluedog-security.com/penetration-testing/, retrieved October 2020
[19] https://bluedog-security.com/microsoftoffice365securitymonitoring/, retrieved October 2020

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254