CLOUD DATA BREACHES

HOW THEY HAPPEN AND HOW TO AVOID THEM

MOTOROLA SOLUTIONS

EXECUTIVE SUMMARY

The cloud movement is rapidly transforming today's business landscape and most organizations now manage environments in a combination of on-premise, cloud infrastructure and software-as-a-service (SaaS) models. Not surprisingly, this has led to an increasing number of security incidents and data breaches. In this white paper, we'll look at some of the biggest cloud breaches in recent history, how they happened and how you can avoid making similar mistakes.

INTRODUCTION

The cloud movement is rapidly transforming today's business landscape. With the growing popularity of Amazon Web Services (AWS), Office 365, Google Cloud and Microsoft Azure, information technology environments now run in a combination of cloud infrastructure and software-as-a-service (SaaS) models. In many cases, organizations are running multiple AWS or Azure accounts.

While there are real benefits of shifting workloads offsite and increasing scalability, security complexities have emerged. With so many cloud environments to manage, it's difficult for security teams to know which resources are running across various cloud accounts and if these accounts are configured securely.

To further add to the complexity, there's often confusion around who is responsible for cloud security. Is it the cloud service provider (CSP)? The organization using these services? Or a combination of both? The reality is that cloud security is a shared responsibility. However, many organizations have failed to take this to heart or to take advantage of even the most basic security tools offered by cloud infrastructure and SaaS providers.

Not surprisingly, this has led to an increasing number of security incidents and data breaches. In the 2020 Cloud Security Report, published by Cybersecurity Insiders, 94 percent of cybersecurity professionals said they are at least moderately concerned about public cloud security, a small increase from last year's survey. The top challenges include protecting against data loss and leakage (69 percent) and threats to data privacy and confidentiality (66 percent).

In this white paper, we'll look at some of the biggest cloud breaches in recent history, how they happened and how you can avoid making similar mistakes.

DOW JONES 2019 DATA EXPOSURE

Incident #1

WHAT HAPPENED

In 2017, Dow Jones made headlines in a case that involved an exposed Amazon AWS S3 bucket, which was misconfigured to allow any AWS Authenticated Users to download the personal and financial information of 2.2 million subscribers of The Wall Street Journal and Barron's.

Unfortunately, Dow Jones was in the news again in 2019 as a result of a data exposure that the company attributed to an unnamed third-party vendor. An independent security researcher, Bob Diachenko, discovered the immense Dow Jones Watchlist dataset on a public Elasticsearch cluster. The dataset was 4.4GB and was accessible by anyone who knew where to look, Diachenko said.

The database, which has since been secured, had 2.4 million records with extremely sensitive information on current and former political figures, their relatives, close associates and associated companies; national and international companies under government sanction; people officially linked to, or convicted of, high-profile crimes; and profile notes from Dow Jones that cited federal agencies and law enforcement sources.

LESSONS LEARNED

First and foremost, it is crucial that corporate information security policies are applied to cloud environments. On a regular basis, examine which policies require a refresh to match up with your current cloud environments and usage. Make sure that cloud storage is secured and not left as world-readable and that it has strong password protection requirements.

Of course, it also helps to apply certain change management processes and proper security settings. For instance, if Dow Jones employees, contractors and third-party vendors had to go through a quality assurance process before creating storage buckets or Elastic search clusters, someone could have caught the problem earlier.

CYBERSECURITY PROFESSIONALS THAT SAID THEY ARE AT LEAST MODERATELY CONCERNED ABOUT PUBLIC CLOUD SECURITY, A SMALL INCREASE FROM LAST YEAR'S SURVEY.

94%

2020 Cloud Security Report, Cybersecurity Insiders

ACCENTURE DATA EXPOSURE

Incident #2

WHAT HAPPENED

In Accenture's case, four AWS S3 storage buckets were left unsecured and world-readable. All these buckets contained sensitive information, including API data, authentication credentials, VPN keys and customer data.

The credentials exposure did not directly open the gate for criminals to access Accenture's critical information. However, given Accenture's large roster of Fortune 100 and Fortune 500 clients, those exposed credentials could easily lead to secondary attacks, creating the potential for liability issues.

LESSONS LEARNED

There are similar questions that arose from the Dow Jones case: How did those S3 buckets get created? Why weren't they secured in the first place? Did the lack of a reliable change management process lead to a less proactive approach? These are all questions that needed to be addressed early to minimize or prevent breaches in this environment.

This is also a case that illustrates why cloud security training — some form of "Cloud Security 101" — should be part of standard operating procedure now for security and DevOps teams. Whether they're novices or more experienced, everyone involved with cloud deployment and management should be educated on the ground rules and risks.

Lastly, most security professionals are all too familiar with corporate security training programs for employees. Many organizations require staff to complete this training every year. It typically includes topics like email phishing, social engineering, malware, ransomware and related subjects. Adding a section or learning module on cloud security basics, as well as best practices for using cloud applications and services, should be a top priority for organizations in years to come.

TOP CLOUD CONCERNS

69%
Protecting against data loss and leakage

66%
Threats to data privacy

2020 Cloud Security Report, Cybersecurity Insiders

DEVFACTOR DATA BREACH

Incident #3

WHAT HAPPENED

While there are many well-documented cases in recent years of storage breaches, a company called DevFactor had an issue involving GitHub.

An employee inadvertently pushed AWS keys to their GitHub repository. Cyber criminals have bots that are continuously crawling GitHub to look for things like new repositories that go live, or changes to existing repositories. Once they spot activity, the bots automatically begin to go through the code to look specifically for things like AWS keys.

DevFactor quickly realized they'd pushed the AWS keys to GitHub and took them down, but by that point, it was already too late. The automated bots detected the keys and took the information. Then they automatically went to their AWS environment and through the API calls, creating 140 servers to mine for Bitcoins. Amazon noticed the activity and notified DevFactor within the day, but during the short time that the automated Bitcoin mining operation was live, it cost the company $2,300, which Amazon fortunately refunded.

LESSONS LEARNED

What are some of the lessons learned from this? Obviously, applications should be written to secure keys. Make sure that the lock and key are separated and separate the code as well, if possible.

If an organization is using public repositories like GitHub to store code, they should review their systems development lifecycle (SDLC) or application development lifecycle process to determine what they need to do to sanitize data before it gets pushed to the cloud. It may make sense to add a manual check as a failsafe to prevent problems like this.

While cloud providers may guarantee that their platform and their management of it is secure, once they've given an organization permission to work within a space, they don't have visibility into or control of that environment. Thus, it is up to each organization to monitor their own access and usage.

While many organizations are used to monitoring their local data center infrastructure, most are not monitoring the cloud as closely to look for unusual activity. If someone or something – whether an employee, malicious hacker or automated bot – is connecting to a cloud API interface from a new IP address or a different region of the world than usual, cloud access monitoring can quickly show that something uncommon is happening.

Monitoring can also include looking for new instances. Some organizations may only add a few instances a month from time to time. Others may be doing it on an hourly basis. Whatever an organization's baseline is, monitoring can alert them to these changes. In the case of DevFactor, spinning up 140 servers was anomalous enough that Amazon detected it and let them know, but organizations should be monitoring their own environment for activity like this, too.

AVIVA AND TESLA

Incident #4

WHAT HAPPENED

Aviva and Tesla were using open source Kubernetes administration consoles to manage multiple cloud environments through a centralized location. This environment was deployed in AWS. The attacks against Aviva and Tesla were similar but there were a few notable differences. Tesla's attack was more sophisticated and involved hackers employing evasion tactics like hiding the IP address of the mining pool server they used.

In the case of both Aviva and Tesla, the default deployment, whether intentionally or unintentionally, was not password protected. Cyber criminals discovered this and were able to get into the Kubernetes administration consoles, as well as the credentials for the firms' AWS and Azure environments. Since the platform was meant to manage the environment, having those keys then gave the criminals enough control to do whatever they wanted to within the environment and utilize the available computing power to mine cryptocurrency mining, all without the knowledge of the companies.

LESSONS LEARNED

These cases illustrate the need for access controls and password best practices for securing systems. Because Kubernetes was meant to manage multiple cloud environments, it operates like an internal-only system. This begs the question of why these kinds of systems were accessible from the Internet in the first place. If they were locked down or had their inbound access rules set such that either through a virtual private cloud interface (VPC) or a VPN, or only from corporate headquarters, those might have been the only systems that had access to get to the management portal.

Including cloud in annual penetration testing is another way to find anomalous behavior. An experienced penetration tester could have found this web interface. If a penetration tester sees new instances being activated, they can see what the default settings are and recommend changes as needed.

Filtering access controls and monitoring for connections to management interfaces from either IP addresses or parts of the world where they don't normally come from or aren't corporate owned could have quickly identified the problem.

DELOITTE EMAIL BREACH

Incident #5

WHAT HAPPENED

The last example is a case involving Deloitte, one of the world's largest accounting firms. The firm was the victim of a cybersecurity attack that reportedly went unnoticed for months. An email administrator had their account compromised while they were in the process of migrating to Office 365. This gave malicious hackers unrestricted access to the firm's global email server and left emails from nearly 250,000 global employees and 350 clients exposed. In addition, cyber criminals had potential access to sensitive data such as passwords, usernames, health information and architectural schematics.

In this case, the company did not have appropriate controls in place. Multi-factor authentication was not enabled until after the migration was completed. Had that been enabled, it might have prevented the credentials being compromised.

LESSONS LEARNED

This case illustrates the importance of including security at every step of the way when organizations are migrating to the cloud, or for example, during mergers and acquisitions. Enabling multi-factor authentication as soon as it's absolutely viable is just one example of this. Monitoring for unusual activity would have also enabled the firm to see the administrative account being logged into from somewhere unexpected could have also alerted the firm to problems sooner rather than months later.

Looking at core fundamentals, this also speaks to the need for not only having corporate policies but making sure that cloud is considered and that policies are used and enforced. For instance, when looking at access controls, making sure that cloud storage is covered is critical. Security professionals and DevOps teams should also understand and implement best practice recommendations from cloud vendors.

> When looking at access controls, making sure that cloud storage is covered is critical. Security professionals and DevOps teams should also understand and implement best practice recommendations from cloud vendors.

SUMMARY

What all these incidents have in common is human error. Consider doing a Cloud Security 101 training so that anyone who has access to cloud applications and infrastructure understands the risks and how data breaches like those just discussed have happened and what to look for if and when corporate policies and procedures aren't in place yet.

Make sure that cloud environments are assessed against the same standards or processes as on-premise data centers, including in pen testing exercises. If an organization is using cloud services, make sure that cloud is in scope for testing. Finally, ensure that basics like strong passwords and access controls are in place and enable multi-factor as soon possible.

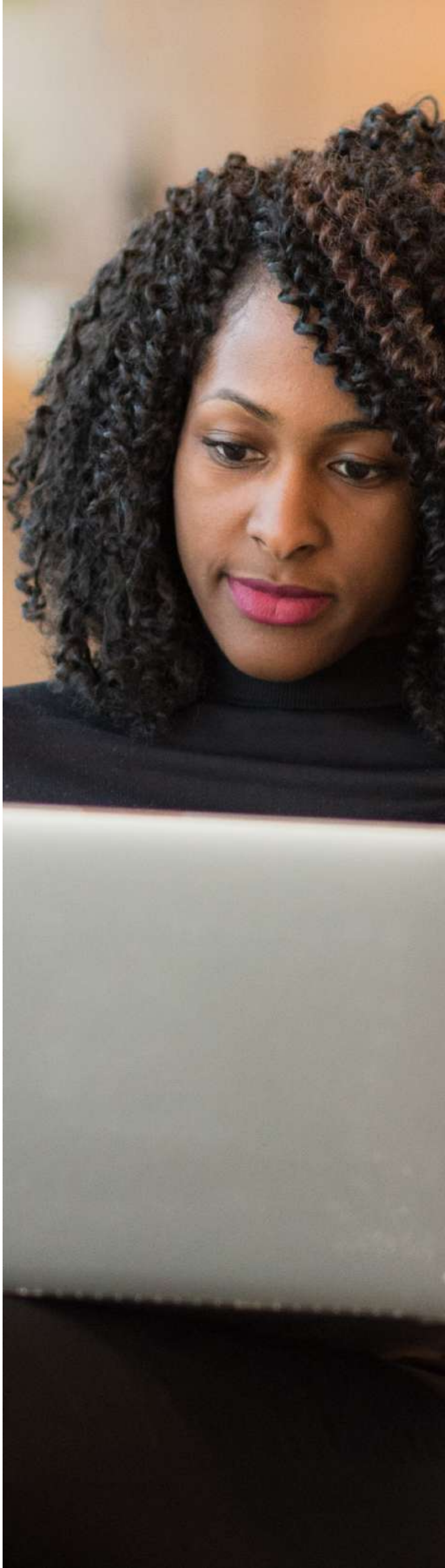
TRUSTED CYBERSECURITY SERVICES

Motorola Solutions Cybersecurity Services bring together an integrated portfolio aligned to the National Institute of Standards and Technology (NIST). As a trusted business partner, we help you develop roadmaps to safeguard your information, employees and systems.

With more than 90 years of experience managing mission-critical technologies and more than 20 years of developing cybersecurity solutions, Motorola Solutions is well-positioned to be the 'one service provider' for your cybersecurity needs.

With best-in-class people, process and technology we bring scalable operations that can help organizations manage cyber risk awareness, detection, response and recovery. Our cutting edge security automation and orchestration platform delivers 24/7 insights on security management, system performance and service delivery, enabling a 100 percent co-managed approach to security management.

We provide a purpose-built and integrated approach to end-to-end resilience.



Learn more at: motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**