Top Threats to Cloud Computing 2024

The permanent and official location for Cloud Security Alliance Top Threats research:
https://cloudsecurityalliance.org/research/working-groups/top-threats/

Acknowledgments

Co-chairs

Jon-Michael Brook
Alex Getsin
Vic Hargrave
Michael Roza

Contributors

Jon-Michael Brook
Randall Brooks
Alex Getsin
Vic Hargrave
Laura Kenner
Michael Morgenstern
Stephen Pieraldi
Michael Roza

Reviewers

Vishnu Guttha
Yuvaraj Madheswaran
Nishith Sinha

CSA Global Staff

Sean Heide
Claire Lehnert
Stephen Lumpe

Table of Contents

Executive Summary

The *Top Threats* report aims to raise awareness of cloud threats, vulnerabilities, and risks. In this installment, we surveyed over 500 industry experts on security issues in the cloud industry. Our respondents identified 11 important security issues in their cloud environments this year. The *Top Threats* Working Group used the survey results and its expertise to create the "*Top Threats* to Cloud Computing 2024" report.

The latest report highlights the 2024 *Top Threats* (ranked in order of significance per the survey described on page 8). The survey rankings for 2024 and 2022 are also shown.

2024		2022
Misconfiguration & Inadequate Change Control	1	Identity & Access Mgmt (IAM)
Identity & Access Mgmt (IAM)	2	Insecure Interfaces and APIs
Insecure Interfaces and APIs	3	Misconfiguration & Inadequate Change Control
Inadequate Selection/ Implementation of Cloud Security Strategy	4	Inadequate Selection/ Implementation of Cloud Security Strategy
Insecure Third-Party Resources	5	Insecure Software Development
Insecure Software Development	6	Insecure Third-Party Resources
Accidental Cloud Disclosure	7	System Vulnerabilities
System Vulnerabilities	8	Accidental Cloud Disclosure
Limited Cloud Visibility/ Observability	9	Misconfiguration & Exploitation of Serverless & Container Workloads*
Unauthenticated Resource Sharing	10	Advanced Persistent Threats
Advanced Persistent Threats	11	Cloud Storage Data Exfiltration*

**Security issues not in the top 11 for 2024*

Observations

The survey analysis shows a continuing drop in the ranking of traditional cloud security issues that are the responsibility of cloud service providers (CSPs). Concerns such as denial of service, shared technology vulnerabilities, and CSP data loss featured in the previous report were now rated low enough to be excluded from this report. These omissions continue the apparent trust in the cloud;

vintage cloud security issues in Infrastructure as a Service (IaaS) environments are less of a concern. Additionally, we observed that data breaches no longer dominate as the top cloud security concern.

As cloud business models and security tactics evolve, this report raises awareness of critical security issues such as:

- Misconfiguration & Inadequate Change Control
- Identity & Access Management (IAM)
- Insecure Interfaces & APIs
- Lack of Cloud Security Architecture and Strategy

Misconfiguration and Inadequate Change Control: Now holding the top spot in our 2024 *Top Threats* survey, up from third in the 2022 report. Configuration management has been a cornerstone of organizational capability maturity for decades. However, the transition to cloud computing has compounded the challenges, making it crucial for teams to adopt more robust cloud-specific configurations. Given a cloud's persistent network access and infinite capacity, misconfigurations can have wide-reaching impacts across an organization.

Identity and Access Management (IAM): Previously in the first spot, IAM now takes the second position. Challenges such as replay attacks, impersonation, and excessive permissions persist in cloud environments, similar to on-premise setups. However, the shift towards using self-signed certificates and poor cryptographic management raises significant security concerns. The focus on implementing Zero Trust architecture and software-defined perimeters (SDP) reflects these issues' prominence in our survey respondents' priorities.

Insecure Interfaces and APIs: Moving to third from second, adopting microservices highlights the critical importance of securing interfaces and APIs. Despite their pivotal role in cloud services, including SaaS and PaaS offerings, substantial challenges remain in securing these elements due to coder inefficiencies and the always-on nature of the cloud.

Inadequate Cloud Security Strategy: Remaining at the fourth position, this area continues to pose a question: Why do significant challenges in planning and architecting security solutions persist? Cloud computing has transcended its novelty status, necessitating a clearly defined and executed architectural strategy.

Target Audience

Cloud and security practitioners and enthusiasts would benefit from this report to gain up-to-date, valuable insights into cloud security threats and challenges, how they impact the industry, and what can be done to mitigate their consequences. Finally, this survey-based research will equip compliance, risk, technology, information security staff, and executive management with technology trends and high-priority cloud security considerations relevant to the present time.

The Survey

In creating the "*Top Threats* to Cloud Computing 2024" survey report, the CSA *Top Threats Working Group* conducted research in two stages. Both stages used surveys to gather the thoughts and opinions of cybersecurity professionals concerning the most relevant threats, vulnerabilities, and risks of security issues to cloud computing with the ultimate goal of identifying the *Top Threats* for 2024.

During the first research stage, the group aimed to create a shortlist of cloud security issues through an in-person survey of the working group's members. The group started with the previous report (*Top Threats* to Cloud Computing: Pandemic Eleven survey report 2022) of 11 *Top Threats* (security issues) and then added 19 issues through discussion. The group then reviewed the 30 issues in a series of meetings, asking working group members to indicate the importance of each matter to their respective organizations and their knowledge of organizations familiar to themselves. This resulted in 28 issues presented in the survey.

In the second stage of the research, the group's main goal was to rank—by importance—the list of 28 security issues using an online survey of 500+ security professionals. The group chose a 10-point sliding scale to reflect the importance of each issue. The survey participants were instructed to rate each cloud security issue on a scale of 1 to 10, with 1 being "Not very important" and 10 being "Most important." The points for each category were totaled and then averaged. The security issues were then ranked according to their mean. The working group then arrived at the Top 11 Threats below.

Survey Results Rank	Survey Average Score	Issue Name
1	8.282331	Misconfiguration & Inadequate Change Control
2	8.070780	Identity & Access Management (IAM)
3	7.987272	Insecure Interfaces & APIs
4	7.620689	Inadequate Selection/Implementation of Cloud Security Strategy
5	7.582061	Insecure Third-Party Resources
6	7.545801	Insecure Software Development
7	7.506641	Accidental Cloud Data Disclosure
8	7.462794	System Vulnerabilities
9	7.389799	Limited Cloud Visibility/Observability
10	7.379310	Unauthenticated Resource Sharing
11	7.364326	Advanced Persistent Threats

With the 11 *Top Threats* identified, the working group analyzed each issue. Each analysis describes the issue, business impacts, key takeaways, anecdotes, and real-world examples, as well as a reference to the relevant section of CSA's Security Guidance for Critical Areas of Focus in Cloud Computing v5 domain guides and the relevant mitigating controls in CSA's Cloud Controls Matrix (CCM) and CAIQ v4 controls. Finally, the overall methodology is representative of the Top Threats methodology presented in CSA's Certificate of Cloud Auditing Knowledge Study Guide v1.

Security Issue 1

MISCONFIGURATION & INADEQUATE CHANGE CONTROL

Misconfigurations are the incorrect or sub-optimal setup of cloud computing assets that can leave them vulnerable to unintended damage or external/internal malicious activity. Lack of cloud system knowledge or understanding of cloud security settings and nefarious intentions can result in misconfigurations. Some common misconfigurations [1] are: 1. secrets management, 2. disabled monitoring and logging, 3. ICMP left open, 4. insecure automated backups, 5. storage access, 6. lack of validation, 7. unlimited access to non-HTTPS/HTTP ports, 8. overly permissive access to virtual machines, containers, and hosts, 9. enabling too many cloud access permissions (least privilege), 10. subdomain hijacking (aka dangling DNS), 11. misconfigurations specific to your cloud provider(s) like AWS S3 buckets. Misconfiguration of cloud resources is a leading cause of security issues in the cloud that can result in severe damage, as shown in the Business Impact section below. [2]

Inadequate change control practices in cloud environments can lead to improper configurations that remain undetected, posing a significant security risk. Cloud environments differ significantly from traditional IT infrastructure, making change control more challenging. Traditional change processes typically involve multiple roles and approvals, often taking days or weeks to complete before reaching production. Cloud computing methodologies, on the other hand, emphasize automation, broad access, and rapid change, often abstracting static infrastructure elements into code. Additionally, utilizing multiple cloud providers introduces further complexity due to their unique capabilities and frequent updates. This dynamic environment demands an agile and proactive approach to change control and remediation, which many organizations strive to achieve.

Business Impact

The impact of misconfigurations/inadequate change controls on cloud systems can be severe depending on the nature of the misconfiguration/improper change and how quickly it is detected and mitigated. The following are the impacts that can result from cloud misconfigurations and inadequate change controls:

Technical Impact:

- *Disclosure of Data:* Unauthorized cloud access to sensitive data compromises confidentiality.
- *Loss of Data:* Permanent or temporary erasure of critical data from cloud systems affects availability.
- *Destruction of Data:* Physical or logical damage to data in cloud systems jeopardizes integrity.

Operational Impact:

- *System Performance:* Degraded performance of cloud resources impacts user experience and productivity.
- *System Outage:* Complete or partial shutdown of cloud services disrupts business operations.

Financial Impact:

- *Ransom Demands:* Payment may be required to restore compromised cloud data or systems access.
- *Non-compliance and Fines:* Failure to adhere to regulatory requirements can result in fines and penalties.
- *Lost Revenue:* Financial losses can occur due to cloud service disruptions, customer dissatisfaction, or legal actions.
- *Reduction in Stock Price:* Breaches and public disclosure can damage market perception and the company's valuation.

Reputational Impact:

- *Company Reputation:* Breaches and public disclosure can damage the organization's public image and brand value.

Key Takeaways

1. **Cloud configuration monitoring, audits, and assessments** - [3]: By leveraging machine learning, organizations can automate the regular detection of cloud system security misconfigurations, reducing the reliance on manual inspections/audits/assessments and increasing efficiency.
2. **Cloud system, change management approaches** - [4]: The unceasing and dynamic nature of continuous business transformations and security challenges requires ensuring that approved changes are made properly using real-time automated verification.

Anecdotes and Examples

Recent incidents resulting from misconfiguration and inadequate change control include:

- **(May 2023)** It was reported that Toyota Motor Corp. had acknowledged a significant vehicle data leak affecting approximately 2.15 million users in Japan. The affected users constitute nearly the entire customer base who signed up for Toyota's major cloud service platform, T-Connect, and users of G-Link, a similar service for Lexus vehicle owners. The data was publicly accessible for a decade, from November 2013 to mid-April 2023. The cause of this breach was attributed to human error. Although the leaked data included details such as vehicle locations and identification numbers, no reports of malicious use have been reported. In response to this incident, Toyota has taken measures to block access to data from the outside. It has initiated an investigation into all cloud environments managed by Toyota Connected Corp. Additionally, the company has committed to implementing a system to audit cloud settings, establishing continuous monitoring procedures, and providing comprehensive training for employees on data handling rules. [5]
- **(September 2023)** It was reported that DarkBeam, a managed cloud service provider and digital risk protection firm, inadvertently left an Elasticsearch and Kibana interface unprotected, exposing records from reported and unreported data breaches. The leaked (downloaded) data included user emails and passwords, totaling over 3.8 billion records. DarkBeam had been collecting this information to alert its customers in case of a data breach. The incident is likely to impact more than just DarkBeam users. The leak was discovered on September 18th and was promptly closed after being reported. Data leaks often occur due to human error, such as forgetting to password-protect the instance after maintenance. Among the leaked data were 16 collections named "email 0-9" and "email A-F," each containing 239,635,000 records. This extensive and organized compilation of data poses a significant threat to individuals whose credentials have been disclosed. Threat actors could target affected users with phishing campaigns using their personal information. Users must change their passwords across online accounts, use strong password generators, and enable two-factor authentication to protect their accounts. [6]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 2: Cloud Governance
Domain 3: Risk, Audit, & Compliance
Domain 5: Identity & Access Management
Domain 7: Infrastructure & Networking
Domain 9: Data Security
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

A&A **Audit and Assurance**
A&A-02: Independent Assessments
A&A-03: Risk-Based Planning Assessment

AIS **Application and Interface Security**
AIS-02: Application Security Baseline Requirements
AIS-04: Secure Application Design and Development
AIS-05: Automated Application Security Testing

BCR **Business Continuity Mgt & Op. Resilience**
BCR-02: Risk Assessment and Impact Analysis
BCR-08: Backup

CCC **Change Control and Configuration Mgt**
CCC-02: Quality Testing
CCC-04: Unauthorized Change Protection
CCC-09: Change Restoration

CEK **Cryptography, Encryption, and Key Mgt**
CEK-03: Data Encryption
CEK-05: Encryption Change Management

DSP **Data Security & Privacy Lifecycle Mgt**
DSP-07: Data Protection by Design and Default
DSP-08: Data Privacy by Design and Default
DSP-17: Sensitive Data Protection

GRC **Governance, Risk Mgt, and Compliance**
GRC-02: Risk Management Program
GRC-05: Information Security Program

HRS **Human Resources**
HRS-09: Personnel Roles and Responsibilities
HRS-11: Security Training / Awareness

IAM **Identity and Access Management**
IAM-03: Identity Inventory
IAM-08: User Access Review

IVS **Infrastructure and Virtualization Security**
IVS-02: Capacity and Resource Planning
IVS-03: Network Security
IVS-04: OS Hardening and Base Controls

LOG **Logging and Monitoring**
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response
LOG-12: Access Control Logs

SEF **Security Incident Management, E-Discovery, & Cloud Forensics**
SEF-03: Incident Response Plans
SEF-04: Incident Response Testing
SEF-06: Event Triage Processes

TVM **Threat & Vulnerability Management**
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting

References

1. Common Cloud Misconfigurations and How to Avoid Them
   https://www.upguard.com/blog/cloud-misconfiguration
2. 13 Most Common Misconfigurations on the Cloud
   https://www.clouddefense.ai/common-misconfigurations-on-the-cloud/
3. Safeguarding Against Security Misconfigurations with the Power of Machine Learning
   https://securityboulevard.com/2023/11/safeguarding-against-security-misconfigurations-with-the-power-of-machine-learning/
4. Change execution monitoring
   https://www.versio.io/solution-change-request-management.html
5. More than 2 million Toyota users face the risk of vehicle data leak in Japan
   https://www.reuters.com/business/autos-transportation/toyota-flags-possible-leak-more-than-2-mln-users-vehicle-data-japan-2023-05-12/?ref=thestack.technology
   Apology & Notice Concerning Newly Discovered Potential Data Leakage of Customer Info Due to Cloud Settings
   https://global.toyota/en/newsroom/corporate/39241625.html
   Yet Another Toyota Cloud Data Breach Jeopardizes Thousands of Customers
   https://www.darkreading.com/ics-ot-security/toyota-cloud-data-breach-jeopardizes-thousands-customers
   Toyota spewed vehicle location data for millions onto unsecured cloud databases for 10 years
   https://www.thestack.technology/toyota-data-breach-2023-t-connect-cloud/
6. DarkBeam leaks billions of email and password combinations
   https://securityaffairs.com/151566/security/darkbeam-data-leak
   DarkBeam's Alarming Data Breach Exposes 3.8 Billion Records
   https://techreport.com/news/darkbeams-alarming-data-breach-exposes-3-8-billion-records/
   More than 3.8 billion records exposed in DarkBeam data leak
   https://www.cshub.com/data/news/darkbeam-data-leak

Security Issue 2

IDENTITY & ACCESS MANAGEMENT

Identity & Access Management (IAM) ensures individuals only get access to resources they are allowed (authorized) to after proving who they say they are. This system is pivotal in defining and managing user roles, access privileges, and the specific conditions under which these privileges are allocated or rescinded. Despite its critical role, IAM presents ongoing challenges in cybersecurity due to its complexity and the evolving nature of cyber threats. Key components like user authentication, authorization, single sign-on (SSO), multi-factor authentication (MFA), and activity monitoring are integral to IAM's effectiveness. However, the intricacies and dynamism of these features can introduce vulnerabilities, especially if not implemented, configured, updated, and monitored correctly. As cyber threats become more sophisticated, securing sensitive information against unauthorized access becomes increasingly daunting, making the robust implementation and continual refinement of IAM strategies indispensable to fortifying cybersecurity defenses.

Managing identities and access in cloud environments can be complex and risky. Different cloud providers have unique systems, which can lead to mistakes and security gaps. When users can create and manage their accounts and resources, it can result in excessive permissions and misconfigured settings, increasing security risks. Each vendor incorporates distinct IAM frameworks and nuanced fine-grained permissions. Without a deep understanding and management strategy for multiple systems, the risk of misconfigurations and inconsistent security policies is significant. With a centralized IAM system monitoring, issue response is easier, while inconsistent policies further complicate security efforts. The dynamic nature of cloud resources, like short-lived resources and automated scaling, adds to management complexity. Integrating cloud and on-premises systems can be challenging, especially with hybrid environments and the need for single sign-on. Compliance with various regulations is another hurdle. Mitigating these risks involves 1. adopting unified IAM solutions with strong authentication like single sign-on and phishing-resistant multi-factor

authentication (MFA), 2. enforcing the principle of least privilege, 3. automating provisioning and de-provisioning processes, 4. conducting activity monitoring, and 5. providing continuous training and awareness programs for users and administrators. Proper implementation and continual refinement of IAM strategies protect sensitive information and maintain cybersecurity defenses' effectiveness.

Business Impact

Inadequate Identity and Access Management (IAM) can lead to unauthorized access, data breaches, and regulatory non-compliance, causing significant financial and reputational damage. Effective IAM strategies are essential to protect sensitive information and maintain robust cybersecurity defenses.

Technical Impact:

- *System Access:* Weak authentication may lead to the exploitation of confidential data from backend systems.
- *Data Disclosure:* Outside parties may access business data due to communication weaknesses, system access, or credential reuse.
- *Data Loss:* MOVEit campaigns demonstrate how exfiltrated data can provide leverage in negotiating ransoms.

Operational Impact:

- *System Outage:* Complete or partial shutdown of cloud services can disrupt business operations.
- *Feature Delay:* Feature updates may be delayed due to the need to remediate software exploits.

Financial Impact:

- L*ost Revenue:* Financial losses can occur due to service disruptions, service restoration, customer dissatisfaction, or legal actions.
- *Non-compliance:* Failure to adequately secure identity and access controls can lead to non-compliance with regulatory requirements such as GDPR, CCPA, and industry-specific regulations like PCI DSS. Regulatory breaches can result in significant fines and legal actions.

Reputational Impact:

- *Company Reputation:* Damage to the cloud service organization's public image, business, and brand value.
- *Customer Reputation:* Clients relying on weakly secured API cloud services can experience data breaches and service interruptions, negatively impacting their reputations.

Key Takeaways

- **Unify IAM Solutions:** Use IAM solutions that provide strong authentication, centralized management, and visibility across multiple cloud providers.
- **Adhere to the Principle of Least Privilege:** Ensure users have only the access rights needed to perform their tasks. Controlling the blast radius helps mitigate potential breaches.
- **Automate Provisioning and De-provisioning:** Implement automated tools to manage the lifecycle of accounts and permissions, ensuring timely updates and removal of unnecessary access.
- **Access evaluation and monitoring:** Implement automated tools to manage the lifecycle of

accounts and permissions, ensuring timely updates and removal of unnecessary access. Deploy tools to detect, alert, and prevent unauthorized access attempts through continuous security monitoring.

Anecdotes and Examples

Here are some recent examples of this security issue's cloud incidents:

- **(May 2023) MOVEit Campaign:** A series of breaches linked to the MOVEit file transfer tool impacted several organizations, including government agencies and healthcare providers. For example, the Oregon Department of Transportation experienced a breach affecting approximately 3.5 million individuals, with attackers gaining access to sensitive personal information due to over-permissioned accounts and poor separation of duties. Robust logging, auditing, and traffic-based anomaly detection are required to capture traffic that results from account compromises. These incidents underscore the emerging trend of data extortion attacks, where cybercriminals pressure victims to pay to prevent the release of stolen data rather than to decrypt it. [1]
- **(June 2023) JumpCloud Data Breach:** JumpCloud, an Identity and Access Management firm, suffered a breach due to a sophisticated nation-state actor. The attack targeted specific customer accounts by injecting data into JumpCloud's commands framework. The breach was initially traced back to a spear-phishing campaign and non-expiring credentials, emphasizing the risks associated with sophisticated cyber-attacks and the importance of robust security measures, including credential strength review, forced timed resets, and log reviews. [2]
- **(October 2023) Okta Data Breach:** Okta, a provider of identity services and authentication management, experienced a data breach where an unauthorized actor accessed its support case management system using stolen credentials. This incident compromised customer support case information, highlighting the risks of storing service accounts and sensitive information within accessible systems. Continuous monitoring and systematic review processes are critical. [3]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 2: Cloud Governance
Domain 3: Risk, Audit, & Compliance
Domain 5: Identity & Access Management
Domain 6: Security Monitoring
Domain 9: Data Security
Domain 10: Application Security
Domain 12: Related Technologies & Strategies

CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: App. & Interface Sec. Policy & Procedures
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics

CCC Change Control and Configuration Mgt
CCC-07: Detection of Baseline Deviation
CCC-08: Exemption Management

DSP Data Security & Privacy Lifecycle Mgt
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-07: Data Protection by Design and Default
DSP-17: Sensitive Data Protection
DSP-19: Data Location

GRC Governance, Risk Mgt, and Compliance
GRC-02: Risk Management Program
GRC-05: Information Security Program
GRC-06: Governance Responsibility Model

IAM Identity and Access Management
IAM-01: Identity & Access Mgt Policy & Procedures
IAM-03: Identity Inventory
IAM-05: Least Privilege
IAM-08: User Access Review

LOG Logging and Monitoring
LOG-10: Encryption Monitoring and Reporting

IVS Infrastructure and Virtualization Security
IVS-03: Network Security
IVS-06: Segmentation and Segregation

TVM Threat & Vulnerability Management
TVM-08: Vulnerability Prioritization

References

1. MOVEit cyberattacks: keeping tabs on the biggest data theft of 2023 https://www.theverge.com/23892245/moveit-cyberattacks-clop-ransomware-government-business
2. JumpCloud: June 20 Incident Details and Remediation https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation
3. Okta hit by third-party data breach exposing employee information https://www.bleepingcomputer.com/news/security/okta-hit-by-third-party-data-breach-exposing-employee-information/
4. The 10 Biggest Data Breaches of 2023 (so far) https://www.crn.com/news/security/the-10-biggest-data-breaches-of-2023-so-far
5. DOJ-Collected Information Exposed in Data Breach Affecting 340,000 https://www.securityweek.com/doj-collected-information-exposed-in-data-breach-affecting-340000/

Security Issue 3

INSECURE INTERFACES & APIs

Cloud Service Providers (CSPs), enterprise vendors, and internal developers offer machine-to-machine application programming interfaces (APIs) or comprehensive suites of human user interfaces (UIs), typically for system controls. Initial design requirements often don't align with long-term utilization. Changing leadership, corporate strategy direction, or third-party partner access needs exposures, creating deadlines with a race to deploy. Previous decisions, undocumented assumptions, legacy support requirements, poor architectural design, or On-Premise/IaaS/SaaS product parity expectations will impact corporations' ongoing transition to the cloud.

APIs and UIs become vulnerable for various reasons, including: 1. inadequate authentication mechanisms, 2. lack of encryption, 3. improper session management, 4. insufficient input validation, 5. poor logging and monitoring, 6. outdated or unpatched software, 7. assumed protection parity during cloud conversion, 8. overly permissive access controls, 9. lack of rate limiting. An Akamai 2024 report documented, "29% of web attacks targeted APIs over 12 months (January through December 2023), indicating that APIs are a focus area for cybercriminals." [1] Human portal authentication methods add risks, such as weak or reused passwords, which can be easily compromised. Attackers can exploit these vulnerabilities with impacts ranging from unauthorized access, sensitive data theft, or service disruption. In 2023, OWASP pointed to the importance of securing interfaces, augmenting their popular web list with the new API Security Top 10. [2]

Business Impact

The impact of insecure interfaces on cloud systems can be severe depending on the nature of the system and what other safeguards or mitigations exist. The risk of an insecure interface or API varies depending on the usage and data associated with the API and how quickly the vulnerability is detected and mitigated. The most commonly reported business impact is the unintended exposure of sensitive or private data left unsecured by the API. When examining the impacts that can result from insecure interfaces, consider the following:

Technical Impact:

- *System Access:* Poor authentication may result in the exploitation of backend systems.
- *Data Disclosure:* Outside parties may access business data due to communication weaknesses, system access, or credential reuse.

Operational Impact:

- *System Outage:* Complete or partial shutdown of cloud services can disrupt business operations.
- *Feature Delay:* Feature updates may be delayed due to the need to remediate software exploits.

Financial Impact:

- *Lost Revenue:* Financial losses can occur due to service disruptions, service restoration, customer dissatisfaction, or legal actions.
- *Non-compliance and Fines:* Failure to adhere to regulatory requirements for vulnerability management can result in penalties.

Reputational Impact:

- *Company Reputation:* Damage to the cloud service organization's public image and brand value.
- *Customer Reputation:* Clients relying on weakly secured API cloud services can experience data breaches and service interruptions, negatively impacting their reputations.

Key Takeaways

- The attack surface provided by APIs should be monitored and secured in accordance with best practices.
- Rate limiting and throttling should be implemented to protect against Denial of Service (DoS) attacks and credential stuffing.
- Traditional security control approaches and change management policies must be updated to keep pace with cloud-based API growth and change. Instead of bearer tokens or usernames/passwords, examine shorter-duration credentials with automatic time-based rotation. Human-accessible user interfaces with MFA factors will raise security. All tokens related to authentication events should follow standards with the ability to inspect the time when they were issued.
- Confirm product and service parity when moving capabilities. The vendor's on-premise interface solutions may operate substantially differently in the vendor's SaaS configuration or when moved between hyperscaler CSPs.
- Investigate credential lifecycle automation and technologies that continuously monitor for anomalous API traffic. Incorporate intelligence feeds for augmented detection. These tools correctively remediate problems in near real-time.

Anecdotes and Examples

Recent examples of issues related to insecure interfaces and APIs include:

- **(January 2024)** Security researcher Troy Hunt identified an API vulnerability in Spoutible, a Twitter alternative. The exploit allowed access to user account information, including email addresses and bcrypt hashed passwords, simply by using an API URL with a Spoutible username. This breach exposed data for 207,000 records. [3]
- **(January 2024)** Over 15 million Trello accounts were leaked due to a public API matching an existing email database with Trello accounts. This incident highlighted poor API security and led to the exposure of user data, which was later offered for sale on the Dark Web. [4]
- **(January 2024)** In 2024, a significant API leak at Mercedes Benz gave hackers access to the company's GitHub Enterprise, exposing source code, cloud keys, and internal documents. The breach was traced back to an employee's GitHub token without a timestamp, found in a public repository the year before. [5]
- **(February 2024)** Australian ISP Tangerine was breached, exposing over 200,000 records. The breach was traced to the login credentials of a single contractor. Stolen data included personal information such as names, dates of birth, phone numbers, and email addresses. [6]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 3: Risk, Audit, & Compliance
Domain 4: Organization Management
Domain 5: Identity & Access Management
Domain 6: Security Monitoring
Domain 7: Infrastructure & Networking
Domain 8: Cloud Workload Security
Domain 9: Data Security
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

AIS **Application & Interface Security**
AIS-01: App. & Interface Sec. Policy & Procedures
AIS-04: Secure Application Design and Development
AIS-06: Automated Secure Application Deployment

CEK **Cryptography, Encryption, and Key Mgt**
CEK-03: Data Encryption
CEK-04: Encryption Algorithm

CCC **Change Control and Configuration Mgt**
CCC-01: Change Management Policies and Proc.
CCC-02: Quality Testing
CCC-05: Change Agreements

DSP **Data Security & Privacy Lifecycle Mgt**
DSP-01: Security and Privacy Policy and Procedures
DSP-03: Data Inventory
DSP-04: Data Classification
DSP-05: Data Flow Documentation

IVS **Infrastructure and Virtualization Security**
IVS-03: Network Security
IVS-04: OS Hardening and Base Controls
IVS-09: Network Defense

References

1. 2024 State of the Internet Report on API Security: Shining a Light on API Threats
   https://www.akamai.com/lp/soti/lurking-in-the-shadows
2. OWASP API Security Project
   https://owasp.org/www-project-api-security/
3. Twitter rival Spoutible alleges smear campaign amid security breach controversy
   https://techcrunch.com/2024/02/12/twitter-alternative-spoutible-clashes-with-critics-over-security-breach/
4. Massive Trello User Data Leak: Hacker Lists 15 Million Records on a Dark Web Hacking Forum
   https://www.cpomagazine.com/cyber-security/massive-trello-user-data-leak-hacker-lists-15-million-records-on-a-dark-web-hacking-forum/
5. Mercedes Source Code Exposed by Leaked GitHub Token
   https://www.securityweek.com/leaked-github-token-exposed-mercedes-source-code/
6. 230k Individuals Impacted by Data Breach at Australian Telco Tangerine
   https://www.securityweek.com/230k-individuals-impacted-by-data-breach-at-australian-telco-tangerine/

Security Issue 4

INADEQUATE CLOUD SECURITY STRATEGY

Cloud security strategy encompasses considering external factors, existing implementation, and selection of cloud technologies, priorities, and trends toward creating a high-level plan or approach. These insights help organizations achieve cloud security goals and support business objectives. A strategy can include cloud architecture and design of cloud deployment models, cloud service models, cloud service providers (CSPs), service region availability zone, specific cloud services, and general principles, such as preference for CSPs based on impact (national and environmental or social), or tolerance or avoidance of on-demand service consumption and billing models. Cloud security strategizing may consider existing vendor lock-ins, business intentions to expand in a particular region that requires local data residency, and a company-wide preference for a certain CSP or model. Furthermore, a strategy may affect or dictate a forward-looking design of IAM, networking, and security controls across different cloud accounts, vendors, services, and environments.

Strategy should precede and dictate design, but it is common to see that cloud technologies demand an incremental and agile approach to planning, strategizing, and improving. Sound cloud security strategy enables secure operation of workloads and productivity in cloud accounts, networks, and services. Furthermore, this will serve an organization by overcoming (or avoiding) security challenges and risks, supporting decision-making, and gaining meaningful benefits, even given business, technology, and risk uncertainties.

Business Impact

The absence of a cloud security strategy and architecture hampers the implementation of effective and efficient infrastructure security efforts and designs. Recurring security failures can be attributed to inadequate strategy and design and result in various impacts.

Technical Impact:

- *Data Disclosure:* Failures to design or implement a sound cloud security strategy may lead to recurring security incidents and breaches, resulting in significant confidentiality issues.

Operational Impact:

- *Deployment:* An inadequate strategic approach to cloud security can result in misallocated efforts, blockers to deployment and engineering, duplicate work or licensed solutions, scope creep, and ineffective patches and fixes, where design-level measures would be more effective.

Financial Impact:

- *Financial Costs:* Recurring security incidents and breaches caused by failures to design or implement a sound cloud security strategy may lead to significant containment expenses.
- *Non-compliance and Fines:* Penalties and fines can result from regulatory non-compliance due to improperly designed and implemented cloud security strategies.

Reputational Impact:

- *Company Reputation:* Negative media coverage and word of mouth are common outcomes of cloud security failures, even when no breach or malicious intent is involved. These will negatively affect client acquisition, collaborations, and stock valuation, particularly in the short term. Security and cloud vendors are particularly reliant on their brand trust and susceptible to security failures.

Key Takeaways

- Devise a cloud security strategy or key guiding principles with defined goals or objectives.
- When designing and implementing cloud services and security measures, consider business objectives, risk, efficiency, security threats, and legal compliance.
- Consider likely human error, persistent threat actors working against your cloud resilience, and failure to activate a core protective or baseline control (e.g., defense in-depth, prioritization of configuration-lean cloud deployment models) in your cloud strategy and security.
- Design appropriate and best-practice cloud networks, accounts, data, identity management, and boundaries, focusing on defined cloud strategy and goals.

Anecdotes and Examples

Recent examples of issues related to a lack of cloud security architecture and strategy include:

- **(June 2023)** JumpCloud, a cloud-based Identity and Access Management (IAM) service integrating the assets and identity systems of tens of thousands of enterprise customers, experienced a security breach involving unauthorized access via spear phishing of an engineer. The advanced and persistent attack and resulting investigation, containment, and breach takeaways spanned API keys, user awareness, source-code management and integration, service deployment models and controls, endpoint and identity security measures, infrastructure and container technologies design, customer and authorities engagement, and communication. Building effective resilience to thwart advanced attacks in a complex cloud-based and security-sensitive technology service takes competency and grit. Still, it also takes foresight and profound consideration of security and related domains planning and delivering across technology and service. [2]
- **(2022 and 2023)** In January 2022, the LAPSUS$ hacking group accessed Okta's internal administrative systems by compromising a third-party customer support engineer's account. The attacker was able to navigate Okta's systems, customer administration, data portals, and some confidential information. In 2023, Okta was alerted to an additional breach by several prominent customers, including BeyondTrust and 1Password. This second breach showed persisting gaps in the cloud-based identity company's IAM, detection, and overall resilience. [3]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 1: Cloud Computing Concepts and Architectures
Domain 2: Cloud Governance
Domain 3: Risk, Audit, & Compliance
Domain 12: Related Technologies & Strategies

CSA CCM Controls Version 4.0

A&A Audit and Assurance
A&A-03: Risk-Based Planning Assessment
A&A-04: Requirements Compliance

BCR Business Continuity Mgt & Op. Resilience
BCR-03: Business Continuity Strategy
BCR-04: Business Continuity Planning

DCS Datacenter Security
DCS-06: Assets Cataloguing and Tracking

DSP Data Security & Privacy Lifecycle Mgt
DSP-01: Security and Privacy Policy and Procedures
DSP-03: Data Inventory
DSP-07: Data Protection by Design and Default

GRC Governance, Risk Mgt, and Compliance
GRC-02: Risk Management Program
GRC-06: Governance Responsibility Model
GRC-08: Special Interest Groups

HRS Human Resources
HRS-02: Acceptable Use of Technology Policy and Procedures

IAM Identity and Access Management
IAM-01: Identity & Access Mgt Policy & Procedures
IAM-04: Separation of Duties
IAM-09: Segregation of Privileged Access Roles

IPY Interoperability & Portability
IPY-01: Interoperability and Portability Policy and Procedures

IVS Infrastructure and Virtualization Security
IVS-06: Segmentation and Segregation
IVS-07: Migration to Cloud Environments
IVS-08: Network Architecture Documentation

STA Supply Chain Management, Transparency and Accountability
STA-04: SSRM Control Ownership
STA-08: Supply Chain Risk Management

TVM Threat & Vulnerability Management
TVM-01: Threat and Vulnerability Management Policy and Procedures

References

1. IBM Security. (2023). *IBM X-Force Cloud Threat Landscape 2023 Report - Section 3, Recommendations and best practices.* https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/09/13/x-force-cloud-threat-landscape-2023
2. [Security Update] June 20 Incident Details and Remediation https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation
3. Okta, with a bruised reputation, rethinks security from the top down https://www.cybersecuritydive.com/news/okta-security-revival/708636/

Security Issue 5

INSECURE THIRD-PARTY RESOURCES

Cloud computing adoption is increasing rapidly, and a third-party resource could mean different things from externally written code through open-source libraries to SaaS products, or as noted in Security Issue 2, Insecure Interfaces and APIs. Risks stemming from third-party resources are also considered supply chain vulnerabilities as they are part of delivering your cloud service or application to your customers. This is also called Cybersecurity Supply Chain Risk Management (C-CSRM) and focuses on the supply chain cybersecurity risk imposed on one's cloud service or application. Additionally, according to research from Colorado State University, two-thirds of breaches result from supplier or third-party vulnerabilities. [1]

Because a product or service is the sum of all the other products or services it uses, the exploit can start because of any component (e.g., a single line of code) integrated within the application. For the malicious hacker, this means that to achieve their goal, they "only" need to look for the weakest link as an entry point. This weakest link can often be a small supplier to a large business.

Business Impact

Issues resulting from utilizing an insecure third-party resource will have a business impact focusing on the technical, operational, financial, and reputational impacts. Listed below is a starting point to consider how these impact an organization:

Technical Impact:

- *Data Disclosure:* Compromised third-party access can result in unauthorized cloud access to sensitive data, compromising confidentiality.
- *Data Destruction:* Improper code refactoring can result in unauthorized access, allowing data to be compromised.

Operational Impact:

- *Production System Outage:* Delays or unpatched vulnerabilities in third-party resources can result in access that compromises the production system.

Financial Impact:

- *Non-compliance and Fines:* If a third party does not comply, the company can be held responsible for damages, penalties, and fines.

Reputational Impact:

- *Company Confidence:* Publicly disclosed breaches caused by insecure third-party resources can cause customers to lose trust in the company's ability to protect sensitive information.

Key Takeaways

- Software cannot be completely secured, especially code or products you didn't create. An organization can still make informed decisions about which products to use. Utilize third-party resources that are officially supported. Check for any appropriate compliance certifications, transparency about security efforts, bug bounty programs, and a responsible approach to addressing security issues and delivering timely fixes.
- Identify third-party resources through Software Composition Analysis (SCA) and develop a Software Bill of Materials (SBOM) or a SaaS Bill of Materials (SaaSBOM).
- Track the SBOM or SaaSBOM and the third parties your organization is using. An organization doesn't want to discover it's been using a vulnerable product only when the list of victims is published. This includes open source, SaaS products, cloud providers and managed services, and other integrations you may have added to your application.
- Perform periodic automatic and manual reviews of the third-party resources. If your process detects a product you don't need or uses an outdated version with security issues, it should be remediated via appropriate mechanisms. This includes looking at access grants provided to critical components such as code repositories, infrastructure, or high-impact individual applications.
- Work with your suppliers to ensure they have the training and tools to perform automated application security testing.

Anecdotes and Examples

Recent third-party-related issues include:

- **(February 2024)** According to IBM, the cost of a data breach typically averages $4.45 million globally for the year 2023. Additionally, in April 2023, 3CX, an internet telephony company, notified its customers about a supply chain-focused attack. Cybercriminals targeted one or more of 3CX's source code repositories and embedded malware into the company's desktop application. [2]
- **(March 2024)** Listed as CVE-2024-3094, a malicious backdoor was discovered in xz Utils, a widely used data compression utility. This utility is found on almost all Linux and Unix Operating Systems. The xz Utils provides lossless data compression. The backdoor was intentionally planted in versions 5.6.0 and 5.6.1 by one of the two main xz Utils developers with years of contributions to the project. [3]
- **(April 2024)** According to an updated 2024 report, Cyberint notes that supply chain attacks can take several forms, which include credential theft, software or firmware tampering, data theft, and denial of service. They note that there has been a recent spike in breaches to suppliers. Additionally, attempts have been made to tamper with a vendor's product or service to other organizations. [4]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 1: Cloud Computing Concepts and Architectures
Domain 2: Cloud Governance
Domain 5: Identity & Access Management
Domain 7: Infrastructure & Networking
Domain 10: Application Security

CSA CCM Controls Version 4.0

BCR Business Continuity Mgt & Op. Resilience
BCR-01: Business Continuity Mgt Policy & Procedures
BCR-02: Risk Assessment and Impact Analysis
BCR-03: Business Continuity Strategy

CCC Change Control and Configuration Mgt
CCC-04: Unauthorized Change Protection
CCC-05: Change Agreements

DCS Datacenter Security
DCS-05: Assets Classification
DCS-06: Assets Cataloging and Tracking
DCS-07: Controlled Access Points

DSP Data Security & Privacy Lifecycle Mgt
DSP-03: Data Inventory
DSP-05: Data Flow Documentation
DSP-06: Data Ownership and Stewardship
DSP-08: Data Privacy by Design and Default
DSP-10: Sensitive Data Transfer
DSP-16: Data Retention and Deletion

IAM **Identity and Access Management**

IAM-05: Least Privilege
IAM-10: Management of Privileged Access Roles
IAM-11: CSCs Approval for Agreed Privileged Access Roles
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

IPY **Interoperability & Portability**

IPY-01: Interoperability and Portability Policy and Procedures
IPY-02: Application Interface Availability
IPY-03: Secure Interoperability and Portability Management
IPY-04: Data Portability Contractual Obligations

SEF **Security Incident Management, E-Discovery, & Cloud Forensics**

SEF-01: Security Incident Management Policy and Procedures
SEF-03: Incident Response Plans
SEF-07: Security Breach Notification

STA **Supply Chain Management, Transparency and Accountability**

STA-01: SSRM Policy and Procedures
STA-02: SSRM Supply Chain
STA-03: SSRM Guidance
STA-04: SSRM Control Ownership
STA-05: SSRM Documentation Review
STA-06: SSRM Control Implementation
STA-07: Supply Chain Inventory
STA-08: Supply Chain Risk Management
STA-09: Primary Service and Contractual Agreement
STA-10: Supply Chain Agreement Review
STA-11: Internal Compliance Testing
STA-12: Supply Chain Service Agreement Compliance
STA-13: Supply Chain Governance Review
STA-14: Supply Chain Data Security Assessment

References

1. Hackers Putting Global Supply Chain at Risk
   https://www.nationaldefensemagazine.org/articles/2020/7/2/hackers-putting-global-supply-chain-at-risk
2. Rising Threat: Understanding Software Supply Chain Cyberattacks And Protecting Against Them
   https://www.forbes.com/sites/forbestechcouncil/2024/02/06/rising-threat-understanding-software-supply-chain-cyberattacks-and-protecting-against-them/?sh=4e0f3fd16907
3. Backdoor found in widely used Linux utility targets encrypted SSH connections
   https://arstechnica.com/security/2024/03/backdoor-found-in-widely-used-linux-utility-breaks-encrypted-ssh-connections/
4. The Weak Link: Recent Supply Chain Attacks Examined
   https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

Security Issue 6

INSECURE SOFTWARE DEVELOPMENT

Although developers do not intentionally create insecure software, the complexity of software and cloud technologies can inadvertently introduce vulnerabilities. When such insecure software is deployed, threat actors can exploit these weaknesses to compromise cloud applications. By focusing on a cloud-first approach, organizations can facilitate the creation of DevOps pipelines, enabling Continuous Integration/Continuous Deployment (CI/CD) pipelines. Cloud service providers (CSPs) may also offer secure development features, such as guardrails or automated application security testing. Additionally, CSPs provide IAM features, which can enforce least privilege in developer environments and support repudiation.

Ensuring each developer understands the company's shared responsibility assumptions with the CSP requires continuous education. For instance, if a zero-day exploit is reported in the developer's software, the developer is responsible for remediating the issue. Conversely, if the CSP provides the software development or operational environment, it is the CSP's responsibility to implement patches to remediate the issue.

Embracing cloud technologies allows companies to focus on what is unique to their business while letting the CSP own and manage everything that may be commoditized. As stated by the Cloud Controls Matrix 4.0, organizations should: "Define and implement a (Secure Development Lifecycle) SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization." By implementing an SDLC, the focus will be on delivering a more secure cloud application.

Business Impact

Insecure software development will have a business impact that focuses on technical, operational, financial, and reputational aspects. Listed below are starting points to consider how these impacts can affect one's organization:

Technical Impact:

- *Data Disclosure:* Insecure software can result in unauthorized cloud access to sensitive data, compromising confidentiality.
- *Data Destruction:* Unauthorized access resulting from insecure software development can compromise data.

Operational Impact:

- *Feature Delay:* Insecure software development can result in delayed feature updates.
- *System Outage:* Insecure software can cause a complete or partial shutdown of cloud services.

Financial Impact:

- *Non-compliance and Fines:* Companies that do not comply with regulatory requirements can be held responsible for damages, penalties, and fines.

Reputational Impact:

- *Customer Confidence:* Publicly disclosed breaches caused by insecure software development can cause consumers to lose trust in the company's ability to protect sensitive information.

Key Takeaways

- Define and implement a Secure Development Lifecycle (SDLC) process that includes scanning for weaknesses and vulnerabilities during design, development, and operations.
- No software application can be truly secure. An organization's developers can utilize cloud technologies to develop a more secure cloud application and deploy mechanisms to enable resiliency.
- Using cloud technologies prevents reinventing existing solutions. Developers utilize guardrails and other APIs to focus on issues unique to the business.
- Understanding the shared responsibility model, items like patching vulnerabilities in CSP services or developers' applications can ensure timely remediation.
- CSPs value security and will offer guidance, such as a "Well-Architected Framework" or secure design patterns, on implementing services securely. [1]

Anecdotes and Examples

Recent issues related to account hijacking include:

- **(April 2024)** A vulnerability hit a WordPress plugin. As identified as CVE-2024-27956 and a CVSS score of 9.9/10 (Critical), this vulnerability allows attackers to create user accounts with administrative privileges and to plant backdoors for long-term access. The root issue is a common weakness affecting SQL. The attack is a SQL injection issue and affects WP Automatic versions before 3.9.2.0. This vulnerability affects 30,000 websites. [2]
- **(April 2024)** The hacking group Fancy Bear, APT28, has been utilizing a vulnerability in the Windows Print Spooler to escalate privileges, obtain credentials, and exfiltrate data. This actor utilizes a previously undisclosed hacking tool named GooseEgg. The GooseEgg tool has been identified as being used by APT28 since at least June 2020. [3]
- **(April 2024)** Cybersecurity researchers identified a dependency confusion vulnerability impacting a deprecated Apache project called Cordova App Harness. This attack targets the tendency for package managers to check the public repositories before private registries. A threat actor can publish a malicious package with the same name to a public-package repository. It is noted that dependencies are potential weaknesses in the software development factory. [4]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 1: Cloud Computing Concepts and Architecture
Domain 5: Identity & Access Management
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: App. & Interface Sec. Policy & Procedures
AIS-02: Application Security Baseline Requirements
AIS-03: Application Security Metrics
AIS-04: Secure Application Design and Development
AIS-05: Automated Application Security Testing
AIS-06: Automated Secure Application Deployment
AIS-07: Application Vulnerability Remediation

CCC Change Control and Configuration Mgt
CCC-02: Quality Testing

IAM Identity and Access Management
IAM-01: Identity & Access Mgt Policy & Procedures
IAM-04: Segregation of Duties
IAM-05: Least Privilege
IAM-14: Strong Authentication
IAM-16: Authorization Mechanisms

TVM Threat & Vulnerability Management
TVM-03: Vulnerability Remediation Schedule

References

1. AWS Well-Architected Framework
   https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html
2. WP Automatic WordPress plugin hit by millions of SQL injection attacks
   https://www.bleepingcomputer.com/news/security/wp-automatic-wordpress-plugin-hit-by-millions-of-sql-injection-attacks/
3. Microsoft: APT28 hackers exploit Windows flaw reported by NSA
   https://www.bleepingcomputer.com/news/security/microsoft-russian-apt28-hackers-exploit-windows-flaw-reported-by-nsa-using-gooseegg-tool/
4. Apache Cordova App Harness Targeted in Dependency Confusion Attack
   https://thehackernews.com/2024/04/apache-cordova-app-harness-targeted-in.html

Security Issue 7

ACCIDENTAL DATA DISCLOSURE

The risk of accidental data disclosure (often due to misconfiguration) grows yearly. [1] Free public search tools can assist in finding public repositories of data. [2] These risks exist across Amazon (S3 buckets, Elastic Container Registry, Elastic Block Storage), Azure Blob, GCP Storage, Docker Hub, Elasticsearch, Redis, and GitHub. [3] Though the problems have been known and discussed widely over the past two years, Elasticsearch and S3 breaches often occur within 24 hours of exposure. The Cloud Security Alliance published a study in April 2024 indicating that 21.1% of public buckets contained sensitive data. In the past year alone, in addition to the standard fare of full name, nationality, date of birth, and gender, accidental disclosures have included a trove of other sensitive data such as passport info, passwords, educational data, driver licenses, automobile information, medical records, and biometrics. Many of these accidental disclosures are preventable and occur due to oversight and insufficient controls.

For example, when creating an S3 bucket, the user or administration decides whether to enable public read access, and when data is added, the user is usually offered the same choice. The default settings are universally private and must be manually changed to public. While some historical settings still exist on older buckets, this security issue occurs due to choosing convenience over security.

Business Impacts

Accidental data disclosure can be both a threat and a result – it's an insider threat of unwitting employees attempting to make their lives easier without considering security implications. It's a result of breaches and other threats. The results are clear and in the monthly news.

Technical Impact:

- *Data Exposure:* When sensitive company or personal data is exfiltrated due to misconfiguration or other error, it is exposed to people who are not authorized to have or use the data.

Operational Impact:

- *Business Disruption:* Within minutes, attackers could find and compromise unsecured storage and containers, preventing the system from operating.

Financial Impact:

- *Non-compliance:* The California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR) provide hefty fines for breaches.

Reputational Impact:

- *Company Reputation:* The publicity from breaches could affect consumer and business perceptions of company integrity and the ability to govern, control, and manage the business.

Key Takeaways

- All cloud platforms are susceptible to misconfiguration/user error, with limited technology solutions – these are most often process challenges that require robust education programs, IT auditing initiatives, legal planning, etc.
- Some basic configuration steps can dramatically help reduce the likelihood of the 'accidental' part of this issue. Ensure proper configuration of buckets to minimize access (maintain private settings, encrypt content, use strong passwords with Multi-Factor Authentication (MFA). Each major cloud provider (Amazon, Google, Microsoft) provides a step-by-step guide to secure configurations. [5]
- To significantly reduce exposure, implement a least-privilege Identity and Access Management (IAM) policy for databases. Ensure assignments to this policy are strictly controlled and monitored. Disable/do not use Access Control Lists (ACLs) in favor of IAM for more sophisticated security. Continue progressing toward a Zero Trust architecture.
- To ensure compliance, data owners must periodically identify and audit data buckets and their permissions. If configured, Cloud Security Posture Management (CSPM) tools can auto-remediate.

Anecdotes and Examples

Recent examples of a variety of flavors of accidental cloud data disclosure issues include:

- **(June 2023) Passwords:** A publicly accessible link enabled access to a 38TB Azure storage bucket containing Microsoft passwords, Teams messages, and files. Amazon and CSA both advise strongly against using such links. [4, 5, 6]
- **(June 2023) Passport Information:** A misconfigured World Baseball Softball Federation S3 bucket exposed 48,000 records, including 4,600 passports. See Security Issue 3 (Misconfiguration and Inadequate Change Control) as well as Amazon and CSA recommendations. [4, 5, 7]
- **(May 2023) Educational Data:** CaptainU (a college recruitment organization) exposed nearly 1M high school student academic records with pictures and private messages (including students between the ages of 13 and 18). This example demonstrates that not only are user attributes getting stored and leaked, but full conversations, images, etc., are attached to those records and stored in the same places. [8]
- **(May 2023) Biometrics:** U.S. Government AI contractor Veritone AI exposed 550GB of audio, video, and biometric image media, employee PII, police body camera footage, Freedom of Information Act (FOIA) requests and related documents, employee credentials, and system logs with authorization tokens. Some of this data could be combined to create deepfakes to further increase the value to a fraudster. [9]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 2: Cloud Governance
Domain 5: Identity & Access Management
Domain 7: Infrastructure & Networking
Domain 9: Data Security
Domain 10: Application Security

CSA CCM Controls Version 4.0

AIS **Application and Interface Security**
AIS-02: Application Security Baseline Requirements
AIS-04: Secure Application Design and Development

BCR **Business Continuity Mgt & Op. Resilience**
BCR-05: Documentation

DSP **Data Security & Privacy Lifecycle Mgt**
DSP-01: Security and Privacy Policy and Procedures
DSP-02: Secure Disposal
DSP-03: Data Inventory
DSP-05: Segmentation and Segregation
DSP-06: Data Ownership and Stewardship
DSP-07: Data Protection by Design and Default
DSP-09: Data Protection Impact Assessment
DSP-10: Sensitive Data Transfer
DSP-11: Personal Data Access, Reversal, Rectification and Deletion
DSP-13: Personal Data Sub-processing
DSP-14: Disclosure of Data Sub-processors
DSP-16: Data Retention and Deletion
DSP-17: Sensitive Data Protection

GRC **Governance, Risk Mgt, and Compliance**
GRC-01: Governance Program Policy and Procedures
GRC-02: Risk Management Program

IAM **Identity and Access Management**
IAM-01: Identity & Access Mgt Policy & Procedures
IAM-03: Identity Inventory
IAM-05: Least Privilege

IVS **Infrastructure and Virtualization Security**
IVS-01: Infrastructure and Virtualization Security Policy and Procedures
IVS-03: Network Security
IVS-06: Segmentation And Segregation

References

1. Code42 Annual Data Exposure Report 2024
   https://www.code42.com/resources/reports/2024-data-exposure
2. Bucket Search Tool
   https://buckets.grayhatwarfare.com/
3. 2023 Honeypotting in the Cloud Report
   https://orca.security/resources/blog/2023-honeypotting-in-the-cloud-report/
4. Cloud Security Alliance - The Data on the Danger of Publicly Exposed S3 Buckets (and how to remediate)
   https://cloudsecurityalliance.org/blog/2023/04/06/the-data-on-the-danger-of-publicly-exposed-s3-buckets
5. Security Best Practices for Amazon S3
   https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
6. Microsoft Azure Data Leak Exposes Dangers of File-Sharing Links
   https://www.darkreading.com/cloud-security/microsoft-azure-data-leak-exposes-dangers-of-file-sharing-links
7. Misconfigured WBSC server leaks thousands of passports
   https://cybernews.com/security/wbsc-data-leak-passports/
8. College recruitment database leaking nearly 1 million students' GPAs, SAT scores, IDs, and other personal data
   https://cybernews.com/security/college-recruitment-database-leaking-nearly-1-million-students-gpas-sat-scores-ids-and-other-personal-data/
9. AI firm with ties to U.S. government exposes billions of documents in breach
   https://www.biometricupdate.com/202405/ai-firm-with-ties-to-u-s-government-exposes-of-billions-of-documents-in-breach

Security Issue 8

SYSTEM VULNERABILITIES

System vulnerabilities are flaws in cloud service platforms that can be exploited to compromise confidentiality, integrity, and availability of data and potentially disrupt service operations. Cloud services are usually built from custom software, third-party libraries and services, and operating systems. Vulnerabilities in any of these components leave a cloud service more susceptible to cyberattacks. There are four main categories of system vulnerabilities:

- **Misconfiguration** - Vulnerabilities arise when a cloud service is deployed with default or incorrect configuration settings. According to the NSA, misconfiguration of cloud resources is the most prevalent cloud vulnerability. [4] As noted earlier, misconfiguration is the number one security issue identified by this publication's Top Threats survey responders.
- **Zero-day vulnerabilities** - These are vulnerabilities discovered and exploited by threat actors but are unknown to cloud service providers and software vendors.
- **Unpatched software** - Software that contains known security weaknesses that have not been fixed despite the availability of patches for the issues.
- **Weak or default credentials** - Lack of strong authentication increases the chance of threat actors gaining unauthorized access to sensitive data and systems.

Dealing with system vulnerabilities requires continuous monitoring of system and network activities combined with regular vulnerability scanning to uncover security issues before hackers find them. Patch management systems should be used regularly to find out about, acquire, test, and deploy software updates or patches to fix known security vulnerabilities in applications and systems. Deploying Zero Trust architecture can help resist attacks by limiting access to vital system resources through continuous authentication and enforcement of least privilege access.

Business Impact

System vulnerabilities negatively affect the performance and operation of cloud services in several ways. Their effects on cloud services are felt as long as they remain unpatched. Here are some of the impacts that can result from system vulnerabilities:

Technical Impact:

- *Weakened Security:* Cloud services that fail to address system vulnerabilities are more susceptible to attack and compromise.
- *Data Loss:* Sensitive and mission-critical data can be more easily stolen from or exposed in systems that have unpatched vulnerabilities.

Operational Impact:

- *Business Disruption:* Data loss can prevent organizations from fulfilling business obligations to partners and customers.
- *System Performance:* Cloud services that are attacked can experience degradation of system performance and even system outages.

Financial Impact:

- *Lost Revenue:* Financial losses due to service disruptions, restoration, customer dissatisfaction, or legal actions.
- *Non-compliance and Fines:* Failure to adhere to regulatory requirements for vulnerability management and associated penalties.

Reputational Impact:

- *Company Reputation:* Damage to the cloud service organization's public image and brand value.
- *Customer Reputation:* Clients relying on compromised third-party cloud services can experience data breaches and service interruptions, negatively impacting their reputations.

Key Takeaways

- System vulnerabilities are flaws within cloud services that expand their attack surface.
- The NSA and the Top Threats survey respondents have identified misconfiguration as the most significant cloud service vulnerability.
- Continuous monitoring of systems and networks provides visibility into security vulnerabilities and other system integrity issues.
- Regular patch management ensures that the latest security patches are acquired and deployed, making systems more resistant to cyberattacks.
- Zero Trust architecture can limit potential damage by zero-day vulnerabilities by limiting access to critical cloud resources.

Anecdotes and Examples

Recent examples of issues related to system vulnerabilities in the cloud include:

- **(January 2023)** Fortra disclosed that a remote code execution (RCE) vulnerability in its GoAnywhere Managed File Transfer (MFT) was actively exploited. The vulnerability tracked as CVE-2023-0669 enabled the attacker to create unauthorized user accounts in some customer environments and download files from the MFT service. [3]
- **(March 2023)** OpenAI took its ChatGPT service offline to fix a bug the company introduced in its Redis cache client code. Redis is an open-source system that ChatGTP uses to cache user data to minimize direct database access. The bug exposed users' chat history and the first messages from newly created conversations. In addition, payment-related information belonging to 1.2% of ChatGPT Plus subscribers, including first and last name, email address, payment address, payment card expiration date, and the last four digits of the customer's card number, were also exposed. [1]
- **(May 2023)** The Russian-based Clop ransomware group compromised the MOVEit Managed File Transfer (MFT), which exploited 4 SQL injection vulnerabilities in the MFT system. The vulnerabilities are tracked as CVE-2023-34362, CVE-2023-35036, CVE-2023-35708, and CVE-2023-3693X. The attacks affected multiple MOVEit customers, including US government organizations and private sector companies. It is estimated that over 500 organizations and 34 million individuals were affected, with 72% of Clop's victim organizations in the US but many others in Europe and Asia. The Clop ransomware group's method of operation has shifted from encrypting data to threats of exposing sensitive data retrieved from their targets [6]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 5: Identity & Access Management
Domain 6: Security Monitoring
Domain 7: Infrastructure & Networking
Domain 9: Data Security
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

AIS Application and Interface Security
AIS-01: App. & Interface Sec. Policy & Procedures
AIS-02: Application Security Baseline Requirements
AIS-06: Automated Secure Application Deployment
AIS-07: Application Vulnerability Remediation

CEK Cryptography, Encryption & Key Mgt
CEK-03: Data Encryption
CEK-04: Encryption Algorithm

IAM Identity and Access Management
IAM-02: Strong Password Policy and Procedures
IAM-14: Strong Authentication
IAM-15: Passwords Management
IAM-16: Authorization Mechanisms

IVS Infrastructure and Virtualization Security
IVS-04: OS Hardening and Base Controls

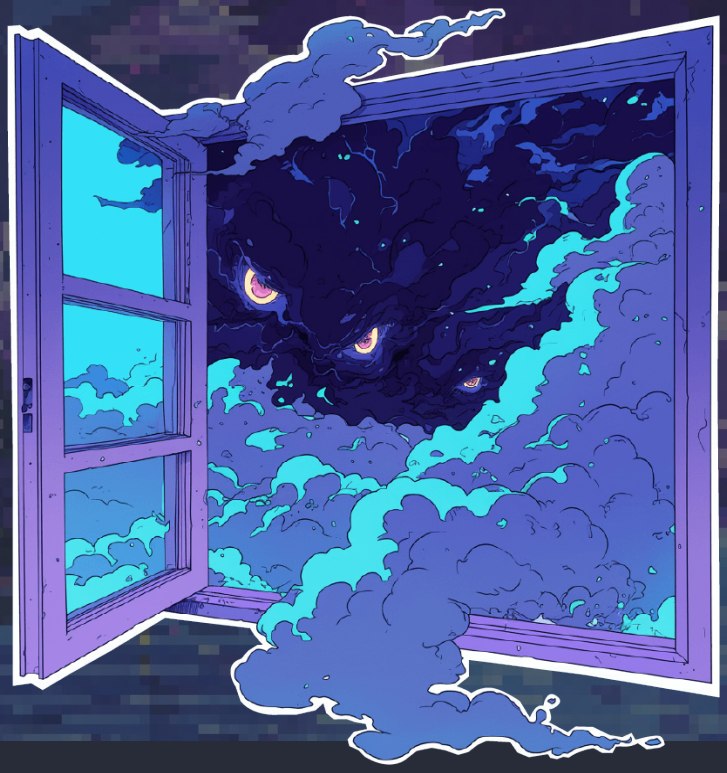
TVM Threat & Vulnerability Management
TVM-01: Threat and Vulnerability Management Policy and Procedures
TVM-02: Malware Protection Policy and Procedures
TVM-03: Vulnerability Remediation Schedule
TVM-04: Detection Updates
TVM-05: External Library Vulnerabilities
TVM-06: Penetration Testing
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting

References

1. ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation
   https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/
2. Cyber Security Vulnerabilities and Their Business Impacts
   https://www.verizon.com/business/resources/articles/s/cyber-security-vulnerabilities-and-their-business-impact/
3. Forta Sheds Light on GoAnywhere MFT Zero-Day Exploit Used in Ransomware Attacks
   https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html
4. Mitigating Cloud Vulnerabilities
   https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF
5. Most Common Types of CyberVulnerabilities
   https://www.crowdstrike.com/cybersecurity-101/types-of-cyber-vulnerabilities/
6. MOVEit Vulnerability Impact: Over 500 Organizations, 34M+ Individuals and Counting
   https://www.spiceworks.com/it-security/security-general/articles/moveit-vulnerability-impact-victims/
7. What is a zero-day exploit?
   https://www.ibm.com/topics/zero-day

Security Issue 9

LIMITED CLOUD VISIBILITY/ OBSERVABILITY



Limited cloud visibility occurs when an organization cannot effectively visualize and analyze whether cloud service usage is safe or malicious. This issue encompasses two key challenges: un-sanctioned app use and sanctioned app misuse. Un-sanctioned app use happens when employees utilize cloud applications and resources without corporate IT and security's specific permission and support, leading to Shadow IT. This scenario is particularly risky when sensitive corporate data is involved. Sanctioned app misuse occurs when organizations cannot monitor how their approved applications are being used by insiders or targeted by external threat actors, often through methods like credential theft, SQL injection, and DNS attacks. [1, 2, 3]

In 2023, several significant cloud breaches underscored the challenges of a lack of cloud visibility. Notable examples include:

- **Human Error Leading to Data Breaches:** Thales (2023) reported that more than a third (39%) of businesses experienced a data breach in their cloud environment, with human error being the leading cause for over half (55%) of these incidents. This highlights the critical need for better visibility and control over cloud environments to prevent such errors.
- **Undetected Security Breaches:** According to Gigamon (2023), nearly one-third of security breaches are going undetected by IT and security professionals. This lack of detection underscores the gap between perceived and actual security, emphasizing the need for improved visibility and monitoring tools.
- **Costs of Cloud Breaches:** Research by Illumio (2023) found that nearly half of all data breaches originated in the cloud, costing organizations an average of $4.1 million per breach. A significant contributor to these breaches was inadequate visibility into cloud connectivity and third-party software interactions.

- Misconfigurations and Access Issues: Expert Insights (2023) reported that many cloud breaches were due to misconfigured access permissions. Approximately 83% of organizations experienced at least one cloud data breach related to access misconfigurations, with many lacking visibility into user permissions and resource access.

Organizations are recognizing the importance of comprehensively monitoring robust access controls [3] and adopting advanced security practices such as Zero Trust Segmentation to mitigate these risks and enhance overall cloud security resilience. [4, 5]

Business Impacts

Limited cloud visibility can severely impact businesses through various technical, operational, financial, and reputational consequences. Here are the key impacts:

Technical Impact

- *Weakened Security:* Cloud services that do not mitigate visibility issues are more susceptible to attacks and compromises due to unmonitored vulnerabilities and misconfigurations.
- *Data Loss:* APT attacks often aim to steal or expose sensitive and mission-critical data, compromising business information integrity and confidentiality.

Operational Impact

- *Business Disruption:* Data loss can prevent organizations from fulfilling business obligations to partners and customers, leading to significant operational standstills.
- *System Performance:* Attacks on cloud services can degrade system performance or cause system outages, affecting overall productivity and service delivery.

Financial Impact

- *Lost Revenue:* Financial losses can result from service disruptions, restoration costs, customer dissatisfaction, or legal actions following a breach.
- *Non-compliance and Fines:* Failure to adhere to regulatory security requirements can result in hefty fines and penalties, which can impact the organization's financial stability.

Reputational Impact

- *Company Reputation:* Data breaches can damage the cloud service provider's public image and brand value, making it difficult to regain customer trust.
- *Customer Reputation:* Clients relying on compromised cloud services may also suffer from data breaches and service interruptions, which can negatively affect their reputations and customer relationships.

Key Takeaways

- **Develop comprehensive cloud visibility:** Start with a top-down approach, tasking a cloud security architect with creating a solution that integrates people, processes, and technology.
- **Mandate company-wide training:** Ensure all employees are trained on accepted cloud usage policies and their enforcement. [6]
- **Review and approve non-approved services:** Have the cloud security architect or third-party

risk management review and approve all non-approved cloud services.

- **Invest in cloud access security broker (CASB) and Zero Trust security (ZTS) solutions:** Use these tools to analyze outbound activities, discover cloud usage, and identify at-risk users and credentialed employee behavior anomalies.
- **Deploy a web application firewall (WAF):** Monitor all inbound connections for suspicious trends, malware, DDoS, and botnet risks.
- **Monitor key enterprise cloud applications:** Select solutions to control key applications and mitigate suspicious behavior.
- **Implement a Zero Trust model:** Adopt a Zero Trust approach across the organization to ensure robust security.

Anecdotes and Examples

Recent examples of issues related to limited cloud visibility include:

- **(September 2023 - October 2023)** The Okta breach, which lasted approximately 22 days, is another example highlighting the critical importance of cloud visibility. Okta's customer, 1Password, first detected the breach, and later, it was confirmed by BeyondTrust. The attackers gained access by compromising an Okta employee's personal Google account, which was used to save Okta service account credentials. This breach impacted all Okta Workforce Identity Cloud (WIC) and Customer Identity Solution (CIS) customers except those in FedRamp High and DoD IL4 environments. Sensitive data of hundreds of Okta's clients, including major companies like FedEx, Hewlett Packard, and T-Mobile, was potentially exposed. The breach underscored vulnerabilities in cloud service providers and the potential for widespread impact from such breaches, raising concerns about Okta's security practices and its ability to protect customer data. [7, 8]
- **(October 2023 - December 2023)** 23 and Me, a leading consumer genetics company, suffered a major data breach due to a misconfigured cloud storage bucket. The personal genomic data of over 5 million customers was compromised. This breach underscored the importance of maintaining rigorous visibility and access controls in cloud environments, especially those handling highly sensitive information. The exposure of such sensitive data not only compromised customer privacy but also raised significant concerns about data security practices within the company. The incident served as a stark reminder of the potential consequences of inadequate cloud visibility and the need for continuous monitoring and configuration management to safeguard sensitive data. [9, 10]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 1: Cloud Computing Concepts and Architecture
Domain 3: Risk, Audit, & Compliance
Domain 5: Identity & Access Management
Domain 8: Cloud Workload Security
Domain 9: Data Security
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

IAM Identity and Access Management
IAM-03: Identity Inventory
IAM-08: User Access Reviews

LOG Logging and Monitoring
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response

SEF Security Incident Management, E-Discovery, & Cloud Forensics
SEF-03: Incident Response Plans
SEF-04: Incident Response Testing

STA Supply Chain Management, Transparency, and Accountability
STA-08: Supply Chain Risk Management

TVM Threat & Vulnerability Management
TVM-01: Threat and Vulnerability Management Policy and Procedures
TVM-02: Malware Protection Policy and Procedure
TVM-03: Vulnerability Remediation Schedule
TVM-04: Detection Updates
TVM-05: External Library Vulnerabilities
TVM-06: Penetration Testing
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting
TVM-10: Vulnerability Management Metrics

References

1. Prisma Cloud by Palo Alto Networks: Cloud Discovery and Exposure Management
   https://start.paloaltonetworks.com/prisma-cloud-request-a-trial
2. Gigamon: Five Top Concerns in Private Cloud Visibility
   https://blog.gigamon.com/2024/03/05/five-top-concerns-in-private-cloud-visibility/
3. Thales: 2023 Cloud Security Study - Global Edition
   https://cpl.thalesgroup.com/cloud-security-research
4. Illumio: Cloud Security Index: Redefine Cloud Security with Zero Trust Segmentation
   https://www.illumio.com/resource-center/cloud-security-index-2023
5. CrowdStrike: 2023 Cloud Risk Report
   https://www.crowdstrike.com/cloud-risk-report/
6. 50 Cloud Security Stats You Should Know In 2024
   https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/
7. ManageEngine: Understanding the Okta Supply Chain Attack of 2023: A Comprehensive Analysis
   https://blogs.manageengine.com/it-security/2024/01/25/understanding-the-okta-supply-chain-attack-of-2023-a-comprehensive-analysis.html
8. BeyondTrust: Okta Support Unit Breach Update
   https://www.beyondtrust.com/blog/entry/okta-support-unit-breach-update
9. 23andMe's data hack went unnoticed for months
   https://www.engadget.com/23andmes-data-hack-went-unnoticed-for-months-081332978.html
10. 23andMe confirms hackers stole ancestry data on 6.9 million users
    https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/

Security Issue 10

UNAUTHENTICATED RESOURCE SHARING

Unauthenticated cloud resource sharing can pose a significant security risk for cloud services. Cloud resources can include virtual machines, storage buckets, and databases, all containing sensitive data and applications vital to business operations. Without proper user authentication or following the principle of least privilege, cloud resources are left open to compromise by threat actors who want to steal confidential data belonging to companies and private individuals.

Among the best practices for securing cloud resources, basic authentication involving password entry, at a minimum, is essential. Yet, every year, major data breaches occur from cloud storage and database systems that do not have password protection. In the vast sea of data on today's Internet, it may seem like finding unsecured cloud resources is challenging, but the opposite is true. Publicly available IoT (Internet of Things) search tools such as Shodan, Binary Edge, and Grayhat Warfare have existed for years, making it relatively easy to find unprotected data repositories.

Beyond password protection, other security measures can be taken to protect critical data:

- **Multi-factor authentication (MFA):** When attempting to access data, MFA requires users to verify their identity through secondary verification, such as one-time access codes or biometric verification.
- **Third-party authentication platforms:** Using services dedicated to verifying user identity can help organizations reliably manage user authentication and provide user-friendly authentication schemes such as one-click or one-touch authorization.
- **Managing user access:** Users should only be granted access to data and applications they require.
- **Continual monitoring of activity:** It is important to continuously monitor users and track any irregular activity. Suspicious user activity can be a prelude to a data breach or indicate that a data breach is underway.

Security controls should be regularly audited for misconfiguration and subjected to security testing to identify weaknesses. Once vulnerabilities are discovered, they can be fixed before cybercriminals find and exploit them.

Business Impact

Here are some of the negative impacts that can result from unauthenticated cloud resources:

Technical Impact:

- *Data Breach:* Unauthorized threat actors can steal or expose sensitive and mission-critical data.
- *Loss of Data:* Unrestricted access to data can lead to partial or complete data destruction.

Operational Impact:

- *Business Disruption:* Data loss can prevent organizations from fulfilling business obligations to partners and customers.

Financial Impact:

- *Lost Revenue:* Financial losses due to service disruptions, service restoration, customer dissatisfaction, or legal actions.
- *Non-compliance and Fines:* Failure to adhere to regulatory requirements for vulnerability management and associated penalties.

Reputational Impact:

- *Company Reputation:* Damage to the cloud service organization's public image and brand value.
- *Customer Reputation:* Clients relying on compromised third-party cloud services can experience data breaches and service interruptions, negatively impacting their reputations.

Key Takeaways

- Cloud storage and database facilities are sometimes not password protected and are open for anyone to exploit easily. Basic user authentication with password enforcement is essential for limiting access to cloud resources.
- Authentication can be further improved by deploying MFA and using 3rd-party authorization services.
- Continual monitoring of users can help determine whether their activities are legitimate or malicious.

Anecdotes and Examples

Recent examples of issues related to unauthenticated resource sharing include:

- **(September 2023)** KidSecurity is a widely used parental control app that parents can use to track their children, listen to the sounds of a child, and set gaming limits. Researchers discovered the company failed to secure Elasticsearch and Logstash collections used by their service, exposing users' private data. KidSecurity logs were left open to anyone on the Internet for over a month. Over 300 million records with private user data were exposed, including 21,000 telephone and 31,000 email addresses. The app also exposed users' payment information, revealing the first six and last four digits of credit card numbers, the expiration month and year, and the issuing bank. [2, 4]
- **(October 2023)** The India state-owned National Logistics Portal-Marine website has sensitive and private data due to misconfigured Amazon S3 buckets. The website also conveyed a Javascript file that contained login credentials to browsers. The exposed data included full names, nationality, date of birth, gender, passport numbers, passport issuing authority, expiration date of ship, and other vessel crew members submitted for their travel. Invoices, shipping orders, and cargo bills were also sensitive data. [3]
- **(January 2024)** Researchers found that Tunefab converter - used to convert music from streaming systems such as Spotify, Amazon's Audible, and Apple Music - exposed users' private data. The platform exposed over 151 million records containing users' IP addresses, areas, IDs, email addresses, and device info. The data leak was caused by a misconfigured MongoDB database that did not have password-protected access and appeared on the public Internet. The database was found on September 26 with a publicly available IoT search engine. [4, 5]

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 3: Risk, Audit, & Compliance
Domain 5: Identity & Access Management
Domain 6: Security Monitoring
Domain 9: Data Security
Domain 10: Application Security

CSA CCM Controls Version 4.0

A&A Audit and Assurance
A&A-04: Requirements Compliance
A&A-05: Audit Management Process

DSP Data Security & Privacy Lifecycle Mgt
DSP-07: Data Protection by Design and Default
DSP-17: Sensitive Data Protection
DSP-19: Data Location

IAM Identity and Access Management
IAM-01: Identity & Access Mgt Policy & Procedures
IAM-02: Strong Password Policies and Procedures
IAM-07: User Access Changes and Revocation
IAM-08: User Access Review
IAM-14: Strong Authentication
IAM-15: Password Management
IAM-16: Authorization Mechanisms

LOG Logging and Monitoring
LOG-05: Audit Logs Monitoring and Response
LOG-12: Access Control Logs

TVM Threat & Vulnerability Management
TVM-06: Penetration Testing
TVM-07: Vulnerability Identification

References

1. Cloud Basics, Best Practices & Implementation
   https://www.okta.com/blog/2020/12/cloud-security-basics-best-practices-implementation/
2. KidSecurity's user data was compromised after the app failed to set the password
   https://cybernews.com/security/kidsecurity-parental-control-data-leak/
3. India's national logistics portal exposed sensitive personal data trade records
   https://techcrunch.com/2023/10/02/india-national-logistics-portal-marine-data-expose/
4. List of Data Breaches and Cyber Attacks in 2023 - 8,216,886,660 records breached
   https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
5. Spotify music converter puts users at risk
   https://cybernews.com/news/spotify-music-converter-puts-users-at-risk/

Security Issue 11

ADVANCED PERSISTENT THREATS

Advanced persistent threats (APTs) continue to pose a significant risk to cloud security. These sophisticated adversaries, including nation-state actors and organized criminal gangs, have the resources and expertise to carry out long-term attack campaigns targeting sensitive data and resources in the cloud. [1]

In 2022-2023, APT activities significantly threatened cloud environments through various tactics, including ransomware and extortion, exploitation of zero-day vulnerabilities, phishing, and credential theft, destructive wiper attacks, and supply chain compromises. [3] These methods highlight the persistent nature of APTs, necessitating robust security measures to safeguard cloud infrastructures against such advanced threats.

To defend against APTs in the cloud, organizations should monitor cyber threat intelligence to understand the most relevant APT groups and their tactics, techniques, and procedures (TTPs). Red team exercises can help test and improve detection and response capabilities against emulated APT attacks. Threat-hunting operations in cloud environments are also crucial for identifying the stealthy, persistent presence of APTs. A multilayered cloud security strategy, including strong access controls, encryption, monitoring, and incident response, is essential for countering these advanced adversaries.

Business Impacts

APTs can severely impact businesses through various channels, leading to significant technical, operational, financial, and reputational consequences.

Technical Impact

- *Weakened Security:* Cloud services that fail to address APT vulnerabilities are more susceptible to attacks and compromises.
- *Data Loss:* APT attacks often aim to steal or expose sensitive and mission-critical data, compromising the integrity and confidentiality of business information.

Operational Impact

- *Business Disruption:* Data loss can hinder an organization's ability to meet business obligations to partners and customers, leading to operational standstills.
- *System Performance:* Attacks on cloud services can degrade system performance or cause system outages, affecting overall productivity and service delivery.

Financial Impact

- *Lost Revenue:* Financial losses can result from service disruptions, restoration costs, customer dissatisfaction, or legal actions following a breach.
- *Non-compliance and Fines:* Failure to adhere to regulatory security requirements can result in hefty fines and penalties, which can impact the organization's financial stability.

Reputational Impact

- *Company Reputation:* APT breaches can damage the cloud service provider's public image and brand value, making it difficult to regain customer trust.
- *Customer Reputation:* Clients relying on compromised cloud services may also suffer from data breaches and service interruptions, which can negatively affect their reputations and customer relationships.

Key Takeaways

- **Business impact analysis:** Regularly analyze business impact to identify and understand your organization's critical information assets and potential vulnerabilities. This will help prioritize security efforts and resource allocation to protect the most valuable data from APT threats.
- **Cybersecurity information sharing:** Participate in cybersecurity information-sharing groups and forums to stay informed about relevant APT groups and their tactics, techniques, and procedures (TTPs). This collective knowledge can enhance your organization's preparedness and response capabilities.
- **Offensive security exercises:** Regularly simulate APT TTPs through red teaming and threat-hunting activities. These offensive security exercises help test and improve your detection and response capabilities, ensuring your security measures are effective against sophisticated threats.

Anecdotes and Examples

Recent examples of issues related to APTs, organized crime, and hackers:

- **(March 2023)** The North Korean APT group LABYRINTH CHOLLIMA targeted cloud resources of cryptocurrency and financial technology companies. This group employed ransomware and extortion tactics, showcasing their ability to operate across multiple platforms, including Windows, Linux, and macOS. The attack demonstrated the group's sophisticated capabilities and focus on high-value targets within the financial sector. The dual approach of ransomware and extortion is aimed at immediate financial gain and creating long-term disruptions and pressure on the affected organizations [2, 6].
- **(June 2023)** Iranian APT groups were observed using ransomware not solely for financial gain but as a cover for espionage activities. These groups deployed wipers to destroy evidence of intrusion, making their operations appear as typical ransomware attacks. This tactic allowed them to conduct espionage and other covert activities while obscuring their true intentions. Wipers indicate a strategic approach to eliminate traces of their presence and operations, complicating incident response and forensic investigations. This method of combining ransomware with wipers highlights APT threats' evolving and deceptive nature [4, 5].
- **(May 2023)** The Chinese APT group APT41 exploited the "Follina" zero-day vulnerability in Microsoft software to compromise the cloud environments of various government organizations. This attack underscored APT41's capability to leverage newly discovered vulnerabilities rapidly and effectively. By exploiting the "Follina" vulnerability, they were able to gain unauthorized access and potentially extract sensitive information from government cloud systems. This incident highlights the critical need for timely patch management and vulnerability assessment in protecting against sophisticated threats [2, 4].

CSA Security Guidance for Critical Areas of Focus in Cloud Computing 5.0

Domain 1: Cloud Computing Concepts and Architecture
Domain 3: Risk, Audit, & Compliance
Domain 5: Identity & Access Management
Domain 8: Cloud Workload Security
Domain 9: Data Security
Domain 10: Application Security
Domain 11: Incident Response & Resilience

CSA CCM Controls Version 4.0

IAM Identity and Access Management
IAM-03: Identity Inventory
IAM-08: User Access Reviews

LOG Logging and Monitoring
LOG-03: Security Monitoring and Alerting
LOG-05: Audit Logs Monitoring and Response

SEF Security Incident Mgt, E-Discovery, & Cloud Forensics
SEF-03: Incident Response Plans
SEF-04: Incident Response Testing

STA Supply Chain Management, Transparency, and Accountability
STA-08: Supply Chain Risk Management

TVM Threat and Vulnerability Management
TVM-01: Threat and Vulnerability Management Policy and Procedures
TVM-02: Malware Protection Policy and Procedure
TVM-03: Vulnerability Remediation Schedule
TVM-04: Detection Updates
TVM-05: External Library Vulnerabilities
TVM-06: Penetration Testing
TVM-07: Vulnerability Identification
TVM-08: Vulnerability Prioritization
TVM-09: Vulnerability Management Reporting
TVM-10: Vulnerability Management Metrics

References

1. APT definition. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
2. CrowdStrike: CrowdStrike 2023 Threat Hunting Report https://www.crowdstrike.com/resources/reports/threat-hunting-report/
3. IBM Security: IBM X-Force Cloud Threat Landscape 2023 Report https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/09/13/x-force-cloud-threat-landscape-2023
4. Mandiant: M-Trends 2023 Report https://services.google.com/fh/files/misc/m_trends_2023_report.pdf
5. Palo Alto Networks: 2023 Unit 42 Ransomware and Extortion Report https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report
6. How APT groups ramped up in 2023 https://www.techradar.com/pro/how-apt-groups-ramped-up-in-2023

Conclusion and Future Outlook

This report analyzes the evolving landscape of cloud security threats, focusing on the persistent nature of misconfigurations, IAM weaknesses, insecure APIs, and the lack of a comprehensive security strategy. While these threats remain the same as identified in the 2022 report, their continued presence highlights their criticality.

A number of trends will likely shape the future of cloud security threats. Organizations must stay informed and adapt to these trends to maintain a secure cloud environment. The key trends include:

- **Increased Attack Sophistication:** Attackers will continue to develop more sophisticated techniques, including AI, to exploit vulnerabilities in cloud environments. These new techniques will necessitate a proactive security posture with continuous monitoring and threat-hunting capabilities.
- **Supply Chain Risk:** The growing complexity of cloud ecosystems will increase the attack surface for supply chain vulnerabilities. Organizations will need to extend security measures to their vendors and partners.
- **Evolving Regulatory Landscape:** Regulatory bodies will likely implement stricter data privacy and security regulations, requiring organizations to adapt their cloud security practices.
- **The Rise of Ransomware-as-a-Service (RaaS):** RaaS will make it easier for unskilled actors to launch sophisticated ransomware attacks against cloud environments. Organizations will need robust data backup and recovery solutions alongside strong access controls.

Some key mitigating strategies are:

- **Integrating AI Throughout the SDLC (Software Development Life Cycle):** Leveraging AI for tasks like code reviews and automated vulnerability scanning early in development will help identify and address security issues before the code reaches production.
- **Utilizing AI-powered Offensive Security Tools:** These tools simulate attacker behavior to discover vulnerabilities in cloud configurations, IAM protocols, and APIs. This proactive approach helps organizations stay ahead of potential threats.
- **Cloud-native Security Tools:** Organizations will increasingly adopt cloud-native security tools designed specifically for cloud environments. These tools offer better visibility and control than traditional security solutions.
- **Zero Trust Security Model:** The Zero Trust model emphasizes continuous verification and least privilege access and has become the standard for cloud security.
- **Automation and Orchestration:** Automating security processes and workflows will be essential for managing the complexity of cloud security at scale.

- **Security Skills Gap:** The cybersecurity skills gap will continue to be challenging. Organizations must invest in training and development programs to build the necessary expertise. Continuous education and awareness programs for employees will be crucial in addressing this gap.

Organizations can build secure and resilient cloud environments by adopting these strategies and remaining vigilant against evolving threats. However, the cybersecurity landscape is constantly changing. Continuous adaptation and investment in cutting-edge security solutions, such as Cloud Security Posture Management (CSPM) or endpoint detection and response (EDR) tools, will be critical for staying ahead of the curve and mitigating the financial and reputational risks associated with cloud security breaches.