THE TREACHEROUS 12

Top Threats to Cloud Computing + Industry Insights

CSA MEMBER 1

TOTAL ENTERPRISES DEFENDED: 87,268

cloud security alliance®

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

© 2017 Cloud Security Alliance – All Rights Reserved

All rights reserved. You may download, store, display on your computer, view, print, and link to The Treacherous 12 - Cloud Computing Top Threats in 2016 at https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/, subject to the following: (a) the Report may be used solely for your personal, informational, non-commercial use; (b) the Report may not be modified or altered in any way; (c) the Report may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Report as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to The Treacherous 12 - Cloud Computing Top Threats in 2016.

Contents

Acknowledgments..... 5

Executive Summary..... 6

Methodology..... 8

1. Data Breaches..... 9

2. Insufficient Identity, Credential and Access Management..... 12

3. Insecure Interfaces and APIs..... 15

4. System Vulnerabilities..... 17

5. Account Hijacking..... 19

6. Malicious Insiders..... 21

7. Advanced Persistent Threats..... 23

8. Data Loss..... 25

9. Insufficient Due Diligence..... 27

10. Abuse and Nefarious Use of Cloud Services..... 30

11. Denial of Service..... 32

12. Shared Technology Vulnerabilities..... 34

© 2017, Cloud Security Alliance. All right reserved.

2017 Edition: Industry Insights

Acknowledgments..... 37

Executive Summary..... 38

Box mismanagement of invite links -
Data Breaches..... 39

Yahoo breach -
Data Breaches..... 40

LinkedIn failure to salt passwords when hashing -
Insufficient Identity Credential Access Management..... 41

Instagram abuse of account recovery -
Insufficient Identity Credential Access Management..... 42

MongoDB Mexican voter information leak -
Insufficient Identity Credential Access management..... 43

MongoDB unprotected, attacked by ransomware -
Insufficient Identity Credential Access Management..... 44

Moonpig insecure mobile application -
Insecure Interface and APIs..... 45

Dirty Cow Linux privilege escalation vulnerability -
System Vulnerabilities..... 46

OAuth Insecure implementation -
Account Hijacking 47

Zynga ex-employees alleged data theft -
Malicious Insiders..... 48

© 2017, Cloud Security Alliance. All right reserved.

T-Mobile customer information theft -
Malicious Insiders..... 49

NetTraveler advanced persistent threats -
Advanced Persistent Threats (APTs)..... 50

Virlock ransomware -
Data Loss..... 51

Yahoo breach -
Insufficient Due Diligence..... 52

Malware using cloud services to exfiltrate data and avoid detection -
Abuse and Nefarious Use of Cloud Services..... 53

Zepto ransomware spread and hosted on cloud storage services -
Abuse and Nefarious Use of Cloud Services..... 54

CloudSquirrel malware hosting command and control (C&C) in Dropbox -
Abuse and Nefarious Use of Cloud Services..... 55

CloudFanta Malware using cloud storage for malware delivery -
Abuse and Nefarious Use of Cloud Services..... 56

Dyn DDoS attack -
Denial of Service..... 57

Australian Bureau of Statistics denial of service -
Denial of Service..... 58

Cloudflare/Cloudbleed buffer overrun vulnerability -
Shared Technology Vulnerabilities..... 59

© 2017, Cloud Security Alliance. All right reserved.

Acknowledgments

Co-Chairs
Jon-Michael C. Brook
Scott Field
Dave Shackleford

Contributors
Jon-Michael Brook
Scott Field
Dave Shackleford
Vic Hargrave
Laurie Jameson
Michael Roza

CSA Global Staff
Victor Chin
Stephen Lumpe (Design)

CSA Chapters
CSA Greater Seattle Chapter
CSA Thailand Chapter

© 2017, Cloud Security Alliance. All right reserved.

Executive Summary

At an unprecedented pace, cloud computing has simultaneously transformed business and government, and created new security challenges. The development of the cloud service model delivers business-supporting technology more efficiently than ever before. The shift from server to service-based thinking is transforming the way technology departments think about, design, and deliver computing technology and applications. Yet these advances have created new security vulnerabilities as well as amplify existing vulnerabilities, including security issues whose full impact are finally being understood. Among the most significant security risks associated with cloud computing is the tendency to bypass information technology (IT) departments and information officers. Although shifting to cloud technologies exclusively may provide cost and efficiency gains, doing so requires that business-level security policies, processes, and best practices are taken into account. In the absence of these standards, businesses are vulnerable to security breaches that can erase any gains made by the switch to cloud technology.

Seeing both the promise of cloud computing, and the risks associated with it, the Cloud Security Alliance (CSA) has created industry-wide standards for cloud security. In recent years, CSA released the "Security Guidance for Critical Areas in Cloud Computing" and the "Security as a Service Implementation Guidance". These documents have quickly become the industry-standard catalogue of best practices to secure cloud computing, comprehensively addressing this within the thirteen domains of CSA Guidance and ten categories of service associated with the Security as a Service (SecaaS) Implementation Guidance series. Many businesses, organizations, and governments have incorporated this guidance into their cloud strategies.

Similar to the earlier mentioned research artifacts, the "The Treacherous 12 - Cloud Computing Top Threats in 2016" play a crucial role in the CSA research ecosystem. The purpose of the report is to provide organizations with an up-to-date, expert-informed understanding of cloud security concerns in order to make educated risk-management decisions regarding cloud adoption strategies. The report reflects the current consensus among security experts in CSA community about the most significant security issues in the cloud.

While there are many security concerns in the cloud, this report focuses on 12 specifically related to the shared, on-demand nature of cloud computing. To identify the top concerns, CSA conducted a survey of industry experts to compile professional opinions on the greatest security issues within cloud computing. The Top Threats working group used these survey results alongside their expertise to craft the final 2016 report. In this most recent edition of the report, experts identified the following 12 critical issues to cloud security (ranked in order of severity per survey results):

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss

© 2017, Cloud Security Alliance. All right reserved.

9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Vulnerabilities

The 2016 Top Threats release mirrors the shifting ramifications of poor cloud computing decisions up through the managerial ranks, instead of being an IT issue it is now a boardroom issue. The reasons may lie with the maturation of cloud, but more importantly, higher strategic decisions by executives in cloud adoption. The 2013 edition highlighted developers and IT departments rolling out their own self-service Shadow IT projects, and the bypassing of organizational security requirements. In 2016, cloud adoption may be effectively aligned with the executive strategies to maximize shareholder value. The always-on nature of Cloud Computing impacts factors that may skew external perceptions and in turn company valuations. Wider reaching architecture/design factors of Identity, Credential and Access Management, Insecure APIs and System & Application Vulnerabilities rise in the survey, while data loss and individual account hijacking fell in comparison.

With descriptions and analysis of the Treacherous 12, this report serves as an up-to-date guide that will help

We've updated the document with recent examples and anecdotes as of 2017.
Please find further details below.

[1] The STRIDE Threat Model. https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx
[2] NIST Risk Management Framework (RMF) Overview. http://csrc.nist.gov/groups/SMA/fisma/framework.html

© 2017, Cloud Security Alliance. All right reserved.

cloud users and providers make informed decisions about risk mitigation within a cloud strategy. This threat research document should be utilized in conjunction with the best practices guides, "Security Guidance for Critical Areas in Cloud Computing V.3" and "Security as a Service Implementation Guidance". A threat analysis was also conducted with the STRIDE Threat Model[1] and the working group recommends the NIST Risk Management Framework[2] on guidance for how to manage information technology risk. Together, these documents will offer valuable guidance during the formation of comprehensive, appropriate cloud security strategies.

Methodology

In creating The Treacherous 12 - Cloud Computing Top Threats in 2016, the CSA Top Threats Working Group conducted research in two primary stages. Both stages used surveys and questionnaires as instruments of study.

In the first stage of the research, our goal was to create a short list of cloud security concerns. The group first started with a list of 20 security concerns, updating last year's eight issues and adding 12 new issues. We presented the 20 concerns via a series of consultations asking working group members to indicate the importance of each concern to their organization. This stage of the research also provided the opportunity for respondents to suggest other concerns. After considering all the survey results and additional information, the working group identified the top 13 most salient cloud security concerns.

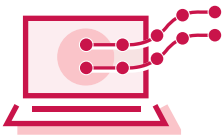
In the second stage of the research, the group's main goal was to rank the previously short-listed cloud security concerns. The group wanted the study to capture what people thought were the most relevant cloud security concerns; a 4-point Likert scale was chosen as the research instrument. A Likert scale is a popular quantitative research method in surveys and is used to represent people's attitudes on a topic. The scale is: 1 (Irrelevant), 2 (Somewhat Relevant), 3 (Relevant), and 4 (Very Relevant). Every security concern was rated 1, 2, 3 or 4 and assigned corresponding scores. For example, a security concern rated as Irrelevant was given one point, a security concern rated as Somewhat Relevant was given two points, and so on. The points for each category were averaged, and the security concerns were then ranked according to their mean. The working group then dropped the security concern which ranked last, leaving the final 12.

The working group also analyzed the security concerns using the STRIDE threat model, which was developed by Microsoft to evaluate information security threats. Specifically, the security concerns discussed in this paper are evaluated to determine whether they fall into any of the following threat categories:

- Spoofing identity (S)
- Tampering with data (T)
- Repudiation (R)
- Information Disclosure(I)
- Denial of service (D)
- Elevation of privilege (E)

© 2017, Cloud Security Alliance. All right reserved.

1. Data Breaches



In the survey, a total of 271 people had responded to the study. About half were from the U.S. (48.95%) with the next highest number of respondents from Australia (5.02%).

Of the respondents who categorized their organizations, 44.65% reported themselves as being part of the technology industry; 15% reported themselves as being part of the professional services industry; and 9.30% reported themselves as being part of the public sector. The remainder was represented by the education, finance, health, and other sectors.

Of the respondents who answered demographic questions, 87.33% identified themselves as Security Specialist, 12.22% as Software Specialist and 9.95% as Networking Specialist followed by other categories.

1.1 Description

A data breach is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so. A data breach may be the primary objective of a targeted attack or may simply be the result of human error, application vulnerabilities or poor security practices. A data breach may involve any kind of information that was not intended for public release including, but not limited to, personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property.

SERVICE MODELS

IaaS | PaaS | SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☒ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☒ Elevation of Privilege

An organization's cloud-based data may have value to different parties for different reasons. For example, organized crime often seeks financial, health and personal information to carry out a range of fraudulent activities. Competitors and foreign nationals may be keenly interested in proprietary information, intellectual property and trade secrets. Activists may want to expose information that can cause damage or embarrassment. Unauthorized insiders obtaining data within the cloud are a major concern for organizations.

The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers. A cloud environment is subject to the same threats as a traditional corporate network as well as new avenues of attack by way of shared resources, cloud provider personnel and their devices and third party partners of the cloud provider. Cloud providers are highly accessible and the vast amount of data they host makes them an attractive target.

© 2017, Cloud Security Alliance. All right reserved.

1.2 Business Impacts

Although nearly any data breach can be problematic, the sensitivity of the data usually determines the extent of the damage. In many parts of the world, laws and regulations oblige organizations to exercise certain standards of care to ensure that sensitive information is protected against unauthorized use. When a data breach occurs, companies may incur large fines and may also be subject to civil lawsuits and, in some cases, criminal charges.

A company also accrues costs related to investigating a breach and notifying customers who were impacted. Some companies engage professional consulting and legal services to assist with managing the breach response. It is also customary for a company suffering a data breach to purchase credit monitoring services for consumers whose information was stolen to alert them in case of fraudulent use. Indirect impacts such as damage to a brand's reputation and resulting loss of business are much harder to calculate. Measures such as the rate at which customers leave, and any change to the cost of user acquisition can be used to estimate this.

Cloud providers often have good security for aspects they take responsibility for but, ultimately customers are responsible for protecting their data in the cloud. The best protection against data breach is an effective security program. Two important security measures that can help companies stay secure in the cloud are multifactor authentication and encryption.

1.3 Anecdotes and Examples

In mid-2015, BitDefender, an antivirus firm, had an undisclosed number of customer usernames and passwords stolen due to a security vulnerability in its public cloud application hosted on AWS. The hacker responsible demanded a ransom of $15,000.

The 2015 Anthem breach of more than 80 million customer records began with stolen credentials on the corporate network. A third-party cloud service was used to transfer the huge data store from the company's network to the public cloud where it could be downloaded by the hackers.

British telecom provider TalkTalk reported multiple security incidents in 2014 and 2015, which resulted in the theft of four million customers' personal information. The breaches were followed by a rash of scam calls attempting to extract banking information from TalkTalk customers. TalkTalk was widely criticized for its failure to encrypt customer data.

1.4 CCM v3.0.1 Control IDs

AIS-04: Application & Interface Security – Data Security/Integrity
CCC-02: Change Control & Configuration Management – Outsourced Development
DSI-02: Data Security & Information Lifecycle Management – Data Inventory/Flows
DSI-05: Data Security & Information Lifecycle Management – Information Leakage
DSI-06: Data Security & Information Lifecycle Management – Non-Production Data
DSI-08: Data Security & Information Lifecycle Management – Secure Disposal
EKM-02: Encryption & Key Management – Key Generation

© 2017, Cloud Security Alliance. All right reserved.

EKM-03: Encryption & Key Management – Sensitive Data Protection
EKM-04: Encryption & Key Management – Storage and Access
GRM-02: Governance and Risk Management – Data Focus Risk Assessments
GRM-10: Governance and Risk Management – Risk Assessments
HRS-02: Human Resources – Background Screening
HRS-06: Human Resources – Mobile Device Management
IAM-02: Identity & Access Management – Credential Lifecycle/Provision Management
IAM-04: Identity & Access Management – Policies and Procedures
IAM-05: Identity & Access Management – Segregation of Duties
IAM-07: Identity & Access Management – Third Party Access
IAM-09: Identity & Access Management – User Access Authorization
IAM-12: Identity & Access Management – User ID Credentials
IVS-08: Infrastructure & Virtualization Security – Production/Non-Production Environments
IVS-09: Infrastructure & Virtualization Security – Segmentation
IVS-11: Infrastructure & Virtualization Security – Hypervisor Hardening
SEF-03: Security Incident Management, E-Discovery & Cloud Forensics – Incident Reporting
STA-06: Supply Chain Management, Transparency and Accountability – Third Party Assessment

1.5 Links

1. The Impact of a Data Breach Can Be Minimized Through Encryption
https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/

2. Dropbox and Box leak files in security through obscurity nightmare
http://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/

3. Anthem's Breach and the Ubiquity of Compromised Credentials
https://blog.cloudsecurityalliance.org/2015/02/09/not-alone-92-companies-share-anthems-vulnerability/

4. Stolen Passwords Used in Most Data Breaches
http://www.darkreading.com/stolen-passwords-used-in-most-data-breaches/d/d-id/1204615

5. Anti-Virus Firm BitDefender Admits Breach, Hacker Claims Stolen Passwords are Unencrypted
http://www.forbes.com/sites/thomasbrewster/2015/07/31/bitdefender-hacked/

6. TalkTalk Criticised for Poor Security and Handling of Hack Attack
http://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack

© 2017, Cloud Security Alliance. All right reserved.

2. Insufficient Identity, Credential and Access Management

2.1 Description

Data breaches and enabling of attacks can occur because of a lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates.

Credentials and cryptographic keys must not be embedded in source code or distributed in public facing repositories such as GitHub, because there is a significant chance of discovery and misuse. Keys need to be appropriately secured and a well-secured public key infrastructure (PKI) is needed to ensure key-management activities are carried out.

Identity systems must scale to handle lifecycle management for millions of users as well as the CSPs. Identity management systems must support immediate de-provisioning of access to resources when personnel changes, such as job termination or role change, occur.

Identity systems are becoming increasingly interconnected, and federating identity with a cloud provider (e.g. SAML assertions) is becoming more prevalent to ease the burden of user maintenance. Organizations planning to federate identity with a cloud provider need to understand the security around the cloud provider's identity solution, including processes, infrastructure, segmentation between customers (in the case of a shared identity solution), and implemented by the cloud provider.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

THREAT ANALYSIS

STRIDE:

- ☑ Spoofing Identity
- ☑ Tampering with data
- ☑ Repudiation
- ☑ Information Disclosure
- ☑ Denial of Service
- ☑ Elevation of Privilege

Multifactor authentication systems – smartcard, OTP, and phone authentication, for example – are required for users and operators of a cloud service. This form of authentication helps address password theft, where stolen passwords enable access to resources without user consent. Password theft can manifest in common network lateral movement attacks, such as "pass the hash."

In cases where legacy systems require use of passwords alone, the authentication system must support policy enforcement such as verification of strong password use as well as organization-defined rotation period policies.

Cryptographic keys, including TLS certificates, keys used to protect access to data and keys used to encrypt data at rest must be rotated periodically. Doing so helps address attacks where keys are accessed without authorization. When cryptographic keys are stolen, a lack of key rotation policy may dramatically increase effective elapsed breach time and scope.

Any centralized storage mechanism containing data secrets (e.g. passwords, private keys, confidential customer

© 2017, Cloud Security Alliance. All right reserved.

contact database) is an extremely high-value target for attackers. Choosing to centralize passwords and keys is a compromise that an organization must weigh the trade-off of convenience of centralized key management against the threat presented by centralizing keys. As with any high-value asset, monitoring and protection of identity and key management systems should be a high priority.

2.2 Business Impacts

Malicious actors masquerading as legitimate users, operators or developers can read/exfiltrate, modify and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source. As a result, insufficient identity, credential or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

2.3 Anecdotes and Examples

Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency – "Cloud service provider credentials included in a GitHub project were discovered and misused within 36 hours of the project going live."

Praetorian Launches Cloud-based Password Cracking Service – "Praetorian, an Austin, Texas-based provider of information security solutions, has launched a new cloud-based platform that leverages the computing power of Amazon AWS in order to crack password hashes in a simple fashion."

2.4 CCM v3.0.1 Control IDs

IAM-01: Identity & Access Management – Audit Tools Access
IAM-02: Identity & Access Management – Credential Lifecycle / Provision Management
IAM-03: Identity & Access Management – Diagnostic / Configuration Ports Access
IAM-04: Identity & Access Management – Policies and Procedures
IAM-05: Identity & Access Management – Segregation of Duties
IAM-06: Identity & Access Management – Source Code Access Restriction
IAM-07: Identity & Access Management – Third Party Access
IAM-08: Identity & Access Management – Trusted Sources
IAM-09: Identity & Access Management – User Access Authorization
IAM-10: Identity & Access Management – User Access Reviews
IAM-11: Identity & Access Management – User Access Revocation
IAM-12: Identity & Access Management – User ID Credentials
IAM-13: Identity & Access Management – Utility Programs Access
HRS-01: Human Resources – Asset Returns
HRS-03: Human Resources – Employment Agreements
HRS-04: Human Resources – Employment Termination
HRS-08: Human Resources – Technology Acceptable Use
HRS-09: Human Resources – Training / Awareness
HRS-10: Human Resources – User Responsibility

© 2017, Cloud Security Alliance. All right reserved.

2.5 Links

1. Attackers Scrape GitHub for Cloud Service Credentials, Hijack Account to Mine Virtual Currency
   http://www.forbes.com/sites/runasandvik/2014/01/14/attackers-scrape-github-for-cloud-service-credentials-hijack-account-to-mine-virtual-currency/
2. Dell Releases Fix for Root Certificate Fail
   http://www.bankinfosecurity.com/dell-releases-fix-for-root-certificate-fail-a-8701/op-1

© 2017, Cloud Security Alliance. All right reserved.

3. Insecure Interfaces and APIs

3.1 Description

Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services. Provisioning, management, orchestration and monitoring are all performed with these interfaces. The security and availability of general cloud services is dependent on the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Furthermore, organizations and third parties may build on these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, because organizations may be required to relinquish their credentials to third parties in order to enable their agency.

APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack, and adequate controls protecting them from the Internet are the first line of defense and detection.

SERVICE MODELS

IaaS | PaaS | SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 6: Interoperability and Portability
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement and Access Management

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☑ Tampering with data
- ☑ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☑ Elevation of Privilege

3.2 Business Impacts

While most providers strive to ensure that security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the use, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

Threat modeling applications and systems, including data flows and architecture/design, become important regular parts of the development lifecycle. In addition to security-specific code reviews, rigorous penetration testing becomes a requirement.

3.3 Anecdotes and Examples

The IRS Breach and the Importance of Adaptive API Security – "In mid-2015, the US Internal Revenue Service (IRS) exposed over 300,000 records via a vulnerable API ("Get Transcript")."

© 2017, Cloud Security Alliance. All right reserved.

Why Exposed API Keys and Sensitive Data are Growing Cause for Concern – API security involves more than just securing the API itself: it involves protecting API keys, cloud credentials and other sensitive data from public exposure—security measures that are sometimes overlooked by developers.

3.4 CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security – Application Security
AIS-04: Application & Interface Security – Data Security/Integrity
IAM-08: Identity & Access Management – Trusted Sources
IAM-09: Identity & Access Management – User Access Authorization

3.5 Links

1. Insecure API Implementations Threaten Cloud
http://www.darkreading.com/cloud/insecure-api-implementations-threaten-cloud/d/d-id/1137550

2. Web Services Single Sign-On Contains Big Flaw
http://www.darkreading.com/risk-management/web-services-single-sign-ons-contain-big-flaws/d/d-id/1103454?

3. IRS Breach and Importance of Adaptive API Security
http://apigee.com/about/blog/technology/irs-breach-and-importance-adaptive-api-security

4. OWASP API Security Project
https://owasp.org/index.php?title=OWASP_API_Security_Project&setlang=en

5. Your API Authentication is Insecure, and we'll tell you why
http://sakurity.com/blog/2015/03/04/hybrid_api_auth.html

6. Why Exposed API Keys and Sensitive Data are Growing Cause for Concern
http://www.programmableweb.com/news/why-exposed-api-keys-and-sensitive-data-are-growing-cause-concern/analysis/2015/01/05

© 2017, Cloud Security Alliance. All right reserved.

4. System Vulnerabilities

4.1 Description

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.

This type of threat is nothing new; bugs have been a problem ever since the invention of computers; they became exploitable remotely when networks were created. With the advent of multitenancy in cloud computing, systems from various organizations are placed in close proximity to each other, and given access to shared memory and resources, creating a new attack surface.

While the damage resulting from attacks on system vulnerabilities can be considerable, such attacks can be mitigated with basic IT processes. Regular vulnerability scanning, following up on reported system threats and installation of security patches or upgrades go a long way toward closing the security gaps left open by system vulnerabilities. Secure design and architecture can lessen the chances of an attacker taking full control of every part of an information system by limiting who has access to specific systems.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 2: Governance and Enterprise Risk Management
Doman 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 8: Data Center Operations
Domain 10: Application Security
Domain 13: Virtualization

THREAT ANALYSIS

STRIDE:

- ☑ Spoofing Identity
- ☑ Tampering with data
- ☑ Repudiation
- ☑ Information Disclosure
- ☑ Denial of Service
- ☑ Elevation of Privilege

4.2 Business Impacts

The impact from unpatched system vulnerabilities on information system security is profound and costly. However, the costs for protection are relatively small compared to other IT expenditures, which can include cleaning up after successful system attacks. Operating system vendors acting on information from the threat research community offer free patches, usually within days of announcements of common vulnerabilities and exposures (CVEs).

Likewise, the cost of putting IT processes in place to discover and repair vulnerabilities is small in comparison to the potential damage they can cause.

Organizations that are highly regulated (e.g. government and financial institutions) need to be capable of handling patching quickly and, when possible, in an automatic recurring fashion. Security management must put in place a threat intelligence function, to fill the gap between the time a vulnerability is announced (known as '0-day'), and the time a patch is provided by the vendor.

© 2017, Cloud Security Alliance. All right reserved.

Change control processes that address emergency patching of critical resources, and various vulnerability scenarios must be created to ensure vulnerability remediation activities are properly documented and reviewed by technical teams prior to being mitigated, validated, and closed. Any other method of handling the threat, such as elimination, transference, or acceptance, must also be documented and tracked.

4.3 Anecdotes and Examples

Magnified Losses, Amplified Need for Cyber-Attack Preparedness – "Heartbleed and Shellshock proved that even open source applications, which were believed more secure than their commercial counterparts … , were vulnerable to threats. They particularly affected systems running Linux, which is concerning given that 67.7% of websites use UNIX, on which the former (Linux) is based."

Verizon 2015 Data Breach Investigations Report – "The Shellshock bug in Bash was 2014's second tumultuous OSS vulnerability event, quickly eclipsing Heartbleed due to many more successful attacks."

2014 Cyberthreat Defense Report – "75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching."

4.4 CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security – Application Security
AIS-02: Application & Interface Security – Customer Access Requirement
AIS-03: Application & Interface Security – Data Integrity
AIS-04: Application & Interface Security – Data Security/Integrity
BCR-04: Business Continuity Management & Operational Resilience - Documentation
CCC-03: Change Control & Configuration Management - Quality Testing
IVS-05: Infrastructure & Virtualization Security Management – Vulnerability Management
IVS-07: Infrastructure & Virtualization Security Management – OS Hardening and Base Controls
TVM-02: Threat and Vulnerability Management – Patch Management

4.5 Links

1. 2014 Cyberthreat Defense Report
   http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cyberedge-2014-cdr.pdf

2. Magnified Losses, Amplified Need for Cyber-Attack Preparedness
   http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf

3. Verizon 2015 Data Breach Investigations Report
   http://www.verizonenterprise.com/DBIR/2015/

© 2017, Cloud Security Alliance. All right reserved.

5. Account Hijacking

5.1 Description

Account or service hijacking is not new. Attack methods such as phishing, fraud and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information and redirect your clients to illegitimate sites. Your account or service instances may become a new base for attackers. From here, they may leverage the power of your reputation to launch subsequent attacks.

Organizations should be aware of these types of attacks as well as common defense-in-depth protection strategies to contain the damage – and possible litigation – resulting from a breach. Organizations should look to prohibit the sharing of account credentials among users and services and leverage strong two-factor authentication techniques where possible. All accounts and account activities should be monitored and traceable to a human owner, even service accounts.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 9: Incident Response
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

THREAT ANALYSIS

STRIDE:

- ☑ Spoofing Identity
- ☑ Tampering with data
- ☑ Repudiation
- ☑ Information Disclosure
- ☑ Denial of Service
- ☑ Elevation of Privilege

5.2 Business Impacts

Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services.

Attackers can leverage account access to steal data, impact cloud services and systems, damage the reputation of tenants and more.

5.3 Anecdotes and Examples

In April 2010, Amazon experienced a cross-site scripting (XSS) bug that allowed attackers to hijack credentials from the site. In 2009, numerous Amazon systems were hijacked to run Zeus botnet nodes.

In June 2014, Code Spaces' Amazon AWS account was compromised when it failed to protect the administrative console with multifactor authentication. All the company's assets were destroyed, putting it out of business.

© 2017, Cloud Security Alliance. All right reserved.

5.4 CCM v3.0.1 Control IDs

IAM-02: Identity & Access Management – Credential Lifecycle/Provision Management
IAM-08: Identity & Access Management – Trusted Sources
IAM-09: Identity & Access Management – User Access Authorization
IAM-10: Identity & Access Management – User Access Reviews
IAM-11: Identity & Access Management – User Access Revocation
IAM-12: Identity & Access Management – User ID Credentials
IVS-01: Infrastructure & Virtualization Security – Audit Logging/Intrusion Detection
SEF-02: Security Incident Management, E-Discovery & Cloud Forensics – Incident Management

5.5 Links

1. Amazon purges account hijacking threat from site
   http://www.theregister.co.uk/2010/04/20/amazon_website_treat/

2. Zeus bot found using Amazon's EC2 as C&C Server
   http://www.theregister.co.uk/2009/12/09/amazon_ec2_bot_control_channel/

3. Code Spaces RIP: Code hosting provider ceases trading after "well-orchestrated" DDoS attack
   http://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/

© 2017, Cloud Security Alliance. All right reserved.

6. Malicious Insiders

6.1 Description

The risk caused by malicious insiders has been debated in the security industry. While the level of threat is left to debate, the fact that insider threat is a real adversary is not. CERN defines an insider threat as follows:

"A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 2: Governance and Enterprise Risk Management
Domain 5: Information Management and Data Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management

THREAT ANALYSIS

STRIDE:

- ☑ Spoofing Identity
- ☑ Tampering with data
- ☒ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☒ Elevation of Privilege

6.2 Business Impacts

A malicious insider, such as a system administrator, can access potentially sensitive information.

From IaaS to PaaS and SaaS, a malicious insider can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on the cloud service provider (CSP) for security are at greater risk here.

Implementations that use encryption provided by the CSP are still vulnerable to malicious insider attack, even though the service provider's key management duties are separated from data storage administration in mature organizations. The key finding here surrounds the CSP's auditable processes and any observations of ad hoc or less-than-measured procedures. The controls available to limit risk from malicious insiders include controlling the encryption process and keys yourself, ensuring that the CSP has proper policies; segregating duties; minimizing access by role; and effective logging, monitoring and auditing of administrators' activities.

It should be noted that the "Insider Threat" does not always involve malicious actors. Insiders might not necessarily be malicious but are "just trying to get their job done". For example, they might accidentally upload a customer database to a public repository or copy sensitive data between jurisdictions or countries.

6.3 Anecdotes and Examples

Insider Threats to Cloud Computing – "Overall, the 'inside job' is responsible for most cloud computing security woes. Enterprises have to become proactive in finding solutions to their security threats to protect their sensitive information."

© 2017, Cloud Security Alliance. All right reserved.

Cloud's Privileged Identity Gap Intensifies Insider Threats – "Organizations need to rein in shared accounts and do a better job tracking user activity across cloud architectures."

6.4 CCM v3.0.1 Control IDs

DCS-04: Datacenter Security – Off-Site Authorization
DCS-08: Datacenter Security – Unauthorized Persons Entry
DCS-09: Datacenter Security – User Access
DSI-04: Data Security & Information Lifecycle Management – Handling/Labeling/Security Policy
DSI-06: Data Security & Information Lifecycle Management – Ownership/Stewardship
EKM-02: Encryption & Key Management – Key Generation
EKM-03: Encryption & Key Management – Sensitive Data Protection
GRM-07: Governance and Risk Management – Policy Enforcement
GRM-10: Governance and Risk Management – Risk Assessments
HRS-02: Human Resources – Background Screening
HRS-07: Human Resources – Roles/Responsibilities
IAM-05: Identity & Access Management – Segregation of Duties
IAM-01: Identity & Access Management – Audit Tools Access
IAM-08: Identity & Access Management – Trusted Sources
IAM-09: Identity & Access Management – User Access Authorization
IAM-10: Identity & Access Management – User Access Reviews
IVS-09: Infrastructure & Virtualization Security – Segmentation
STA-09: Supply Chain Management, Transparency and Accountability – Third Party Audits

6.5 Links

1. Insider threats to cloud computing
   http://www.cloudtweaks.com/2012/10/insider-threats-to-cloud-computing/

2. Cloud's privileged identity gap intensifies insider threats
   http://www.darkreading.com/vulnerabilities---threats/clouds-privileged-identity-gap-intensifies-insider-threats/d/d-id/1138974

3. Insider Threats to Cloud Computing: Directions for New Research Challenges
   http://resources.sei.cmu.edu/asset_files/WhitePaper/2012_019_001_52385.pdf

4. The Insider Threat in Cloud Computing
   https://www.infosec.aueb.gr/Publications/CRITISCloud%20Insider.pdf

© 2017, Cloud Security Alliance. All right reserved.

7. Advanced Persistent Threats

7.1 Description

Advanced Persistent Threats (APTs) are a parasitical form of cyberattack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Spearphishing, direct hacking systems, delivering attack code through USB devices, penetration through partner networks and use of unsecured or third-party networks are common points of entry for APTs. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives.

It pays for IT departments to be informed about the latest advanced cybersecurity attacks that target companies and government organizations. Although APTs can be difficult to detect and eliminate, some can be stopped with proactive security measures. For example, it is critical that users be educated to recognize and handle social engineering techniques such as spearphishing that are commonly used to introduce APTs.

Awareness programs that are regularly reinforced are one of the best defenses against these types of attacks, because many of these vulnerabilities require user intervention or action. Staff should be ingrained with thinking twice before opening an attachment or clicking a link.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 2: Governance and Enterprise Risk Management
Doman 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 8: Data Center Operations
Domain 10: Application Security
Domain 13: Virtualization

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☒ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☑ Elevation of Privilege

7.2 Business Impacts

Combating complex APTs may require more advanced security controls, process management, incident response plans and IT staff training, all of which can lead to increased security budgets. This cost should be weighed against the economic damage inflicted by successful APT attacks.

7.3 Anecdotes and Examples

Carbanak: How Would You Have Stopped a $1 Billion APT Attack? – "… Carbanak, an APT attack against financial institutions around the world, may well be considered the largest cyberheist to date. … Unlike the usual cybercriminal method of stealing consumer credentials or compromising individual online banking sessions with malware, the

© 2017, Cloud Security Alliance. All right reserved.

brazen Carbanak gang targeted banks' internal systems and operations, resulting in a multichannel robbery that averaged $8 million per bank."

Current Trends in the APT World – "The alleged Chinese Cyber-Espionage with its APTs caused the theft of " 'hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006.' "

Current Trends in the APT World – "The Department of Homeland Security reports that APTs 'directed toward businesses have created a surging worldwide demand for solutions to combat these dangerous emerging threats.' "

7.4 CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security – Application Security
AIS-02: Application & Interface Security – Customer Access Requirement
AIS-03: Application & Interface Security – Data Integrity
AIS-04: Application & Interface Security – Data Security/Integrity
BCR-04: Business Continuity Management & Operational Resilience – Documentation
IVS-01: Infrastructure & Virtualization Security – Audit Logging/Intrusion Detection
IVS-02: Infrastructure & Virtualization Security – Change Detection
IVS-05: Infrastructure & Virtualization Security Management – Vulnerability Management
IVS-07: Infrastructure & Virtualization Security Management – OS Hardening and Base Controls
IVS-13: Infrastructure & Virtualization Security Management – Network Architecture
TVM-01: Threat and Vulnerability Management – Anti-Virus/Malicious Software
TVM-02: Threat and Vulnerability Management – Vulnerability/Patch Management

7.5 Links

1. Advanced Persistent Awareness.
http://www.trendmicro.co.uk/media/misc/apt-survey-report-en.pdf

2. Current Trends in the APT World.
http://resources.infosecinstitute.com/current-trends-apt-world/

3. Carbanak: How Would You Have Stopped a $1 Billion APT Attack?
https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/

4. Managing Information Security.
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

5. Understand and combat advanced persistent threats and targeted attacks.
http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/#what-happens-during-an-attack

© 2017, Cloud Security Alliance. All right reserved.

8. Data Loss

8.1 Description

For both consumers and businesses, the prospect of permanently losing one's data is terrifying.

Data stored in the cloud can be lost for reasons other than malicious attacks. An accidental deletion by the cloud service provider, or worse, a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, following best practices in business continuity and disaster recovery – as well as daily data backup and possibly off-site storage. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud but loses the encryption key, the data will be lost as well.

Cloud consumers should review the contracted data loss provisions, ask about the redundancy of a provider's solution, and understand which entity is responsible for data loss and under what conditions. Some providers offer solutions for geographic redundancy, data backup within the cloud, and premise-to-cloud backups. The risk of relying on the provider to store, backup and protect the data must be considered against handling that function in-house, and the choice to do both may be made if data is highly critical.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 5: Information Management and Data Security
Domain 10: Application Security
Domain 12: Identity, Entitlement and Access Management
Domain 13: Virtualization

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☑ Repudiation
- ☒ Information Disclosure
- ☑ Denial of Service
- ☒ Elevation of Privilege

8.2 Business Impacts

Information may not be seen as a critical asset, but it is the lifeblood of virtually all modern organizations. It is the single most valuable asset most companies possess. Even small companies that sell physical products and related services rely on access to data for daily operations: inventory, supplier and customer lists, orders, scheduling, billing, payroll, financials and more. Data loss can be catastrophic; more than one company has been forced out of business because management failed to take steps to ensure that it could recover critical information stored in the cloud.

Under the new EU data protection rules, data destruction and corruption of personal data are considered forms of data breaches and require appropriate notifications.

Additionally, many compliance policies require organizations to retain audit records or other documentation. If an organization stores this data in the cloud, loss of that data can jeopardize its compliance status.

8.3 Anecdotes and Examples

In April 2011, Amazon EC2 suffered a crash that led to significant data loss for many customers.

© 2017, Cloud Security Alliance. All right reserved.

In November 2014, attackers broke into Sony and leaked confidential information such as PII and email exchanges among Sony employees. In the first quarter 2015, Sony set aside USD $15 million to address ongoing damages from the hack.

In June 2014, Code Spaces, an online hosting and code publishing provider, was hacked, leading to the compromise and complete destruction of most customer data. The company was ultimately unable to recover from this attack and went out of business.

8.4 CCM v3.0.1 Control IDs

BCR-04: Business Continuity Management & Operational Resilience – Retention Policy
BCR-05: Business Continuity Management & Operational Resilience – Environmental Risks
BCR-06: Business Continuity Management & Operational Resilience – Equipment Location
GRM-02: Governance and Risk Management – Data Focus Risk Assessments

8.5 Links

1. Cloud Computing Users Are Losing Data, Symantec Finds
http://www.investors.com/cloud-computing-data-loss-high-in-symantec-study/

2. Kill the Password: Why a String of Characters Can't Protect Us Anymore
http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/

3. Code Spaces RIP: Code hosting provider ceases trading after "well-orchestrated" DDoS attack
http://www.cloudcomputing-news.net/news/2014/jun/19/code-spaces-rip-code-hosting-provider-ceases-trading-after-well-orchestrated-ddos-attack/

4. Everything You Ever Wanted to Know About the Amazon EC2 Crash
http://siliconangle.com/blog/2011/04/29/everything-you-ever-wanted-to-know-about-the-amazon-ec2-crash/

5. Inside the Hack of the Century
http://fortune.com/sony-hack-part-1/

© 2017, Cloud Security Alliance. All right reserved.

9. Insufficient Due Diligence

9.1 Description

When executives create business strategies, cloud technologies and CSPs must be considered. Developing a good roadmap and checklist for due diligence when evaluating technologies and CSPs is essential for the greatest chance of success. An organization that rushes to adopt cloud technologies and choose CSPs without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success. This applies whether the company is considering moving to the cloud or merging with or acquiring a company that has moved to the cloud or is considering doing so.

9.2 Business Impacts

Commercial: Anticipated or newly designed customer services that rely on the CSP to develop new systems and processes may not be a priority for or an expertise of the CSP.

Technical: Unknown operational and architectural issues can arise when designers and architects unfamiliar with cloud technologies are designing applications being pushed to the cloud.

Legal: Data in use, motion or at rest in foreign locations during normal operations or even during recovery may subject the company to regulatory redress.

Compliance: Moving applications that depend on "internal" network-level data privacy and security controls to the cloud is dangerous when those controls disappear.

The bottom line for enterprises and organizations moving to a cloud technology model is that they must perform extensive due diligence to understand the risks they assume by adopting this technology model and engaging the suppliers who provide it.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal Issues: Contracts and Electronic Discovery
Domain 4: Compliance and Audit Management
Domain 5: Information Management and Data Security
Domain 6: Interoperability and Portability
Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
Domain 8: Data Center Operations
Domain 9: Incident Response
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Virtualization
Domain 14: Security as a Service

9.3 Anecdotes and Examples

Capable Resources/Controls/Policies – In 2012, the Amazon Web Service (AWS) public cloud—which Netflix relies on to stream content to customers – , experienced an outage in its U.S.-East region (spanning multiple zones in AWS), due to the accidental deletion of information that controls load balancing.

© 2017, Cloud Security Alliance. All right reserved.

Contract and Financial Viability – In 2013, Nirvanix, a cloud storage specialist that hosted data for IBM, Dell and its own customers, filed for Chapter 11 bankruptcy and shuttered its operations. Customers were given less than two weeks to move their data to another service, which highlighted the following issues:

- Data loss: What would happen to Nirvanix customer data, if they could not reclaim it within two weeks?
- Operational disruptions: Film and TV production studio Relativity Media was using Nirvanix' cloud as a hub through which employees in its global locations could collaborate and share massive digital files to accelerate production.
- Security breaches: A cash-strapped service provider may scrimp on security technology and personnel, and a frenetic wind-down may mean that normal security procedures fall through the cracks.
- Non-Compliance: Healthcare and financial services must retain data to meet government compliance regulations. If the data is lost, these services become non-compliant.

THREAT ANALYSIS

STRIDE:

- ☑ Spoofing Identity
- ☑ Tampering with data
- ☑ Repudiation
- ☑ Information Disclosure
- ☑ Denial of Service
- ☑ Elevation of Privilege

M&A – In 2011, Facebook settled FTC charges that it deceived consumers by failing to keep its privacy promises. Under the terms of the FTC's order, Facebook must get consumer's' affirmative consent before making changes that override their privacy settings, among other requirements.

Jason Weinstein, former deputy assistant attorney general, U.S. Department of Justice, summarized the issue of cybersecurity due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data-security problems." In other words, "cyber risk should be considered right along with financial and legal due diligence considerations."

9.4 CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security – Application Security
AIS-04: Application & Interface Security – Data Security / Integrity
AAC-01: Audit Assurance & Compliance – Audit Planning
AAC-02: Audit Assurance & Compliance – Independent Audits
AAC-03: Audit Assurance & Compliance – Info. System Regulatory Mapping
BCR-01: Business Continuity Management & Operational Resilience – Business Continuity Planning
BCR-02: Business Continuity Management & Operational Resilience – Business Continuity Testing
BCR-03: Business Continuity Management & Operational Resilience – Datacenter Utilities / Environ. Conditions
BCR-04: Business Continuity Management & Operational Resilience – Documentation
BCR-05: Business Continuity Management & Operational Resilience – Environmental Risks
BCR-06: Business Continuity Management & Operational Resilience – Equipment Location
BCR-07: Business Continuity Management & Operational Resilience – Equipment Maintenance
BCR-08: Business Continuity Management & Operational Resilience – Equipment Power Failures
BSR-09: Business Continuity Management & Operational Resilience – Impact Analysis
BCR-10: Business Continuity Management & Operational Resilience – Policy
BCR-11: Business Continuity Management & Operational Resilience – Retention Policy

© 2017, Cloud Security Alliance. All right reserved.

GRM-01: Governance & Risk Management – Baseline Requirements
GRM-02: Governance & Risk Management – Data Focus Risk Assessments
GRM-03: Governance & Risk Management – Management Oversight
GRM-04: Governance & Risk Management – Management Program
GRM-05: Governance & Risk Management – Management Support/Involvement
GRM-06: Governance & Risk Management – Policy
GRM-07: Governance & Risk Management – Policy Enforcement
GRM-08: Governance & Risk Management – Policy Impact on Risk Assessments
GRM-09: Governance & Risk Management – Policy Reviews
GRM-10: Governance & Risk Management – Risk Management Assessments
GRM-11: Governance & Risk Management – Risk Management Framework
IVS-06: Infrastructure & Virtualization Security – Network Security
IVS-09: Infrastructure & Virtualization Security – Segmentation

9.5 Links

1. Technology: A lack of due diligence still a top threat in the cloud
http://www.insidecounsel.com/2013/12/06/technology-a-lack-of-due-diligence-still-a-top-thr

2. Due Diligence: 50 Questions for Cloud Computing Providers
http://www.techbridge.org/documents/TechBridge%20-%20Due%20Diligence%20-%2050%20Questions%20for%20Cloud%20Providers.pdf

3. With All Due Diligence
http://www.tierpoint.com/index.php/download_file/364

4. Cloud Service Vendor Evaluation and Due Diligence
http://blog.itil.org/2015/01/itil/cloud-service-vendor-evaluation-and-due-diligence/

5. ISO Standards Catalogue
http://www.iso.org/iso/catalogue_detail?csnumber=56269

6. How long will big-name customers like Netflix put with Amazon cloud outages?
http://www.networkworld.com/article/2162488/cloud-computing/how-long-will-big-name-customers-like-netflix-put-up-with-amazon-cloud-outages-.html

7. Summary of the December 24, 2012 Amazon ELB Event in the U.S.-East Region
http://aws.amazon.com/message/680587/?tag=viglink125435-20

8. Avoiding the Fallout From a Bankruptcy in the Cloud
http://www.cruxialcio.com/nirvanix-bankruptcy-2037

9. FTC Notifies Facebook, WhatsApp of Privacy Obligations in Light of Proposed Acquisition
https://www.ftc.gov/news-events/press-releases/2014/04/ftc-notifies-facebook-whatsapp-privacy-obligations-light-proposed

© 2017, Cloud Security Alliance. All right reserved.

10. Abuse and Nefarious Use of Cloud Services

10.1 Description

Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

Malicious actors may leverage cloud computing resources to target users, organizations or other cloud providers. Examples of misuse of cloud service-based resources include launching DDoS attacks, email spam and phishing campaigns; "mining" for digital currency; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting of malicious or pirated content.

Mitigations for misuse of cloud services includes CSP detection of payment instrument fraud and of misuse of cloud offerings, including examples of inbound and outbound network DoS attacks. A cloud provider must have an incident response framework to address misuse of resources, as well as a means for customers to report abuse originating from a cloud provider. A cloud provider should include relevant controls that allow a customer to monitor the health of their cloud workload.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 3: Legal Issues: Contracts and Electronic Discovery
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 9: Incident Response

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☒ Repudiation
- ☒ Information Disclosure
- ☑ Denial of Service
- ☒ Elevation of Privilege

10.2 Business Impacts

Malicious use of cloud service resources can reduce available capacity for legitimate customers hosted by cloud service providers. Responding to malicious use can also reduce the availability of response resources for addressing other customer support issues.

Fraudulent payment instrument use can result in passing increased costs along to innocent parties such as financial institutions or cloud providers and ultimately to customers and others.

DDoS attacks originating from or directed at a cloud provider can lead to lack of availability, business disruption and loss of revenue for other sites that are hosted on the same cloud platform.

Even though the organization itself may not be performing any of these actions, because of the shared nature of some cloud services, this type of threat presents data and service availability concerns to an organization.

10.3 Anecdotes and Examples

The DDoS That Almost Broke the Internet – "The attackers were able to generate more than 300 Gbps of traffic likely

© 2017, Cloud Security Alliance. All right reserved.

with a network of their own that only had access to 1/100th of that amount of traffic themselves."

Hackers Sneak Back Into AWS for DDoS Launch Hub – "Amazon's Elastic Cloud Computing division was suffering from a highly sophisticated attack by a group of unknown hackers, who had found a way to reverse engineer proof-of-concept code and create an easily-accessible backdoor for themselves into Amazon's massive bank of available processing power."

10.4 CCM v3.0.1 Control IDs

HRS-01: Human Resources - Asset Returns
HRS-02: Human Resources - Background Screening
HRS-03: Human Resources - Employment Agreements
HRS-04: Human Resources - Employment Termination
HRS-07: Human Resources - Roles / Responsibilities
HRS-08: Human Resources - Technology Acceptable Use
HRS-10: Human Resources - User Responsibility
SEF-01: Security Incident Management, E-Discovery & Cloud Forensics - Contact / Authority Maintenance
SEF-02: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management
SEF-03: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting
SEF-04: Security Incident Management, E-Discovery & Cloud Forensics - Legal Preparation

10.5 Links

1. The DDoS That Almost Broke the Internet
https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

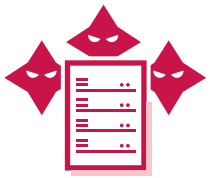
2. Password Cracking in the Cloud
http://www.networkworld.com/article/2194881/cloud-computing/password-cracking-in-the-cloud.html

3. Hackers Sneak Back into AWS for DDoS Launch Hub
https://vpncreative.net/2014/07/29/hackers-sneak-back-aws-ddos-launch-hub/

4. Praetorian Launches Cloud-based Password Cracking Service
http://www.securityweek.com/praetorian-launches-cloud-based-password-cracking-service

© 2017, Cloud Security Alliance. All right reserved.

11. Denial of Service



11.1 Description

Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker—or attackers, as is the case in distributed denial-of-service (DDoS) attacks—causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding.

While DDoS attacks tend to generate fear and media attention—especially when the perpetrators are acting out of a sense of political "hacktivism"—they are by no means the only form of DoS attack. Asymmetric application-level DoS attacks take advantage of vulnerabilities in web servers, databases or other cloud resources, allowing a malicious individual to take out an application with a single extremely small attack payload—in some cases less than 100 bytes long. Other attacks may target equally confined resources: an economic DoS jeopardizes a company's cash flow, using cloud's dynamic nature to overwhelm a startup's ability to pay. Likewise, the human capital of an organization may be tied up quickly in legal work for a bureaucratic DoS and leave a company equally unable to provide a service.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 8: Data Center Operations
Domain 9: Incident Response
Domain 10: Application Security
Domain 13: Virtualization
Domain 14: Security as a Service

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☒ Repudiation
- ☒ Information Disclosure
- ☑ Denial of Service
- ☒ Elevation of Privilege

11.2 Business Impacts

Experiencing a denial-of-service attack is like being caught in rush-hour traffic gridlock: there is no way to get to your destination, and there is nothing you can do about it except sit and wait. As a consumer, service outages not only frustrate you, but also force you to consider whether moving your critical data to the cloud to reduce infrastructure costs was really worthwhile. Worse, because cloud providers often bill clients based on compute cycles and disk space, an attacker may not be able to completely knock your service off the Internet, but may cause it to consume so much processing time that you will be forced to take it down yourself.

In some cases, DDoS attacks have served as a smokescreen for attacks taking place elsewhere in the environment while defenders are occupied with the DDoS. From a risk standpoint, DoS attacks may be more likely in the cloud because other tenants are coming under fire. Cloud providers, however, may be better equipped to mitigate DoS attacks in general.

DDoS attacks must first be visible, so detection is needed. Noticing the website is slow is not an adequate form of detection for an enterprise. Once detected, the key to mitigating a DDoS attack is being prepared for one before it occurs; system administrators must be able to immediately access resources that can be used as mitigation.

© 2017, Cloud Security Alliance. All right reserved.

11.3 Anecdotes and Examples

As Cloud Use Grows, So Will Rate of DDoS Attacks – "Cloud providers face increasing number of DDoS attacks, [similar to those that] private data centers already deal with today"

Feedly Knocked Offline by DDoS Attack Following Evernote and Deezer Attacks – "In what looks like a series of co-ordinated cyber-attacks by a criminal gang, three major cloud-based services have all been knocked offline in recent days. News aggregator Feedly, note-taking app Evernote and music streaming service Deezer have all come under attack from criminals in the last few days leading to all three suffering service outages.

11.4 CCM v3.0.1 Control IDs

AIS-01: Application & Interface Security - Application Security
BCR-08: Business Continuity Management & Operational Resilience - Equipment Power Failures
GRM-01: Governance and Risk Management - Baseline Requirements
IVS-04: Infrastructure Virtualization Security - Information System Documentation

11.5 Links

1. As Cloud Use Grows, So Will Rate of DDoS Attacks
   http://www.infoworld.com/article/2613310/cloud-security/as-cloud-use-grows--so-will-rate-of-ddos-attacks.html

2. Computerworld: DDoS is Cloud's security Achilles heel (September 15, 2011)
   http://www.computerworld.com.au/article/401127/ddos_cloud_security_achil les_heel

3. OWASP: Application Denial of Service
   https://www.owasp.org/index.php/Application_Denial_of_Service

4. Radware DDoSpedia
   http://security.radware.com/knowledge-center/DDoSPedia/

5. DDoS Attacks, The Necessity of Multi-Layered Defense
   https://blog.arbornetworks.com/ddos-attacks-the-necessity-of-multi-layered-defense/

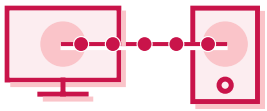
6. Wave Of DDoS Attacks Down Cloud-Based Services
   http://www.darkreading.com/attacks-breaches/wave-of-ddos-attacks-down-cloud-based-services/d/d-id/1269614

7. How New Types of DDoS Affect the Cloud
   http://www.datacenterknowledge.com/archives/2014/10/22/as-apps-move-to-the-cloud-ddos-attacks-take-new-shape/

8. Feedly Knocked Offline by DDoS Attack Following Evernote and Deezer Attacks
   http://www.ibtimes.co.uk/feedly-knocked-offline-by-ddos-attack-following-evernote-deezer-attacks-1452237

© 2017, Cloud Security Alliance. All right reserved.

12. Shared Technology Vulnerabilities



12.1 Description

Cloud service providers deliver their services scalably by sharing infrastructure, platforms or applications. Cloud technology divides the "as a Service" offering without substantially changing the off-the-shelf hardware/software—sometimes at the expense of security. Underlying components (e.g., CPU caches, GPUs, etc.) that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multitenant architecture (IaaS), re-deployable platforms (PaaS) or multicustomer applications (SaaS). This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models. A defense in-depth strategy is recommended and should include compute, storage, network, application and user security enforcement and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

Mitigations to prevent a breach in shared resources should be implemented, such as multi-factor authentication on all hosts, Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection Systems (NIDS on internal networks, applying concepts of networking least privilege and segmentation, and keeping shared resources patched.

SERVICE MODELS

IaaS	PaaS	SaaS

CSA SECURITY GUIDANCE REFERENCE

Domain 1: Cloud Computing Architectural Framework
Domain 5: Information Management and Data Security
Domain 11: Encryption and Key Management
Domain 12: Identity, Entitlement, and Access Management
Domain 13: Virtualization

THREAT ANALYSIS

STRIDE:

- ☒ Spoofing Identity
- ☒ Tampering with data
- ☒ Repudiation
- ☑ Information Disclosure
- ☒ Denial of Service
- ☑ Elevation of Privilege

12.2 Business Impacts

A compromise of an integral piece of shared technology such as the hypervisor, a shared platform component, or an application in a SaaS environment exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. This vulnerability is dangerous because it potentially can affect an entire cloud at once.

12.3 Anecdotes and Examples

Cross-VM Side Channels and Their Use to Extract Private Keys – "…construction of an access-driven side-channel attack by which a malicious virtual machine (VM) extracts fine-grained information from a victim VM running on the same physical computer."

Understanding the VENOM Vulnerability – "The unchecked buffer vulnerability (CVE-2015-3456) occurs in the code for QEMU's virtual floppy disk controller. A successful buffer overflow attack exploiting this vulnerability can enable an attacker to execute his or her code in the hypervisor's security context and escape from the guest operating system to gain control over the entire host."

© 2017, Cloud Security Alliance. All right reserved.

12.4 CCM v3.0.1 Control IDs

DSI-04: Data Security & Information Lifecycle Management - Handling/Labeling/Security Policy
EKM-03: Encryption & Key Management - Sensitive Data Protection
GRM-01: Governance and Risk Management - Baseline Requirements
IAM-02: Identity & Access Management - Credential Lifecycle/Provision Management
IAM-05: Identity & Access Management - Segregation of Duties
IAM-12: Identity & Access Management - User ID Credentials
IVS-01: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection
IVS-09: Infrastructure & Virtualization Security - Segmentation
TVM-02: Threat and Vulnerability Management - Vulnerability/Patch Management

12.5 Links

Shared technology examples for virtualization isolation/bare metal execution:

1. EC2 Maintenance Update
   https://aws.amazon.com/blogs/aws/ec2-maintenance-update/

2. The VENOM "virtual machine escape" bug – what you need to know
   https://nakedsecurity.sophos.com/2015/05/14/the-venom-virtual-machine-escape-bug-what-you-need-to-know/

3. Escaping VMWare Workstation through COM1
   https://docs.google.com/document/d/1sIYgqrytPK-CFWfqDntraA_Fwi2Ov-YBgMtl5hdrYd4/preview

4. Seriously, get off my cloud! Cross-VM RSA Key Recovery in a Public Cloud
   https://eprint.iacr.org/2015/898.pdf

© 2017, Cloud Security Alliance. All right reserved.

2017 Edition: Industry Insights

The Treacherous 12 - Top Threats to Cloud Computing

© 2017, Cloud Security Alliance. All right reserved.

Acknowledgments

Co-Chairs
Jon-Michael C. Brook
Scott Field
Dave Shackleford

Contributors to the anecdotes and examples document are:
Fitzgerald Barth
Victor Chin
Moshe Ferber
Sean Hittel
Laurie Jameson
Nathaniel Mason
Hardeep Mehrotara
Ashish Mehta
Mihir Mohanty
Krishna Narayanaswamy
Michael Roza

CSA Global Staff
Victor Chin
Frank Guanco
John Yeoh

Special Thanks
Dan Hiestand

© 2017, Cloud Security Alliance. All right reserved.

Executive Summary

This appendix serves as an update of anecdotes for the research published by the Cloud Security Alliance (CSA) Top Threats Working Group in 2016 entitled The Treacherous 12: Cloud Computing Top Threats in 2016. This 2017 Edition: Industry Insights document contains 21 industry insights of recent incidents or developments that relate to the 12 categories of security issues mentioned in the 2016 document.

The industry insights mentioned in this document include:

- Box mismanagement of invite links - Data Breaches
- Yahoo breach - Data Breaches
- LinkedIn failure to salt passwords when hashing - Insufficient Identity Credential Access Management
- Instagram abuse of account recovery - Insufficient Identity Credential Access Management
- OAuth Insecure implementation - Account Hijacking
- Zynga ex-employees alleged data theft - Malicious Insiders
- Yahoo breach - Insufficient Due Diligence
- MongoDB Mexican voter information leak - Insufficient Identity Credential Access management
- Dyn DDoS attack - Denial of Service
- Dirty Cow Linux privilege escalation vulnerability - System Vulnerabilities
- T-Mobile customer information theft - Malicious Insiders
- MongoDB unprotected, attacked by ransomware - Insufficient Identity Credential Access Management
- Malware using cloud services to exfiltrate data and avoid detection - Abuse and Nefarious Use of Cloud Services
- Australian Bureau of Statistics denial of service - Denial of Service
- Virlock ransomware - Data Loss
- Zepto ransomware spread and hosted on cloud storage services - Abuse and Nefarious Use of Cloud Services
- CloudSquirrel malware hosting command and control (C&C) in Dropbox - Abuse and Nefarious Use of Cloud Services
- CloudFanta Malware using cloud storage for malware delivery - Abuse and Nefarious Use of Cloud Services
- Moonpig insecure mobile application - Insecure Interface and APIs
- Cloudflare/Cloudbleed buffer overrun vulnerability - Shared Technology Vulnerabilities
- NetTraveler advanced persistent threats - Advanced Persistent Threats (APTs)

The Top Threats Working Group hopes that providing an update of industry insights relating to the 12 security issues cited in the 2016 report will provide readers with relevant context that is updated and in line with what is currently happening in the security industry.

— CSA Top Threats Working Group

© 2017, Cloud Security Alliance. All right reserved.

Box mismanagement of invite links -

Data Breaches

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 9
Anecdote/Example	A security researcher using online search engines found collaboration links to private data belonging to a number of accounts, both corporate and individual in nature. A collaboration link allows shared file and folder access to users, with permission to download, upload, view, edit and rename files. By default, the collaboration links were generated with editor permissions. Box.com attributed the issue to users over-sharing and publishing the invite links, but also took steps to ensure that public collaboration invite links would not be indexed by search engines going forward.
Link	https://threatpost.com/box-com-plugs-account-data-leakage-flaw/122810/
Date	3rd January 2017

© 2017, Cloud Security Alliance. All right reserved.

Yahoo breach -

Data Breaches

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 9]

Anecdote/Example

Yahoo confirmed in September 2016 that more than 1 billion user accounts were compromised in August 2013. Subsequently, 500 million user accounts were breached in 2014. When combined, these security failures constitute the single-largest breach in history. The company believes the data hacks are connected and that the breaches are "state-sponsored." Yahoo's chief information security officer, Bob Lord, confirmed that hackers used "forged cookies," or bits of code that linger in a user's browser cache so that a website does not require a login with every visit. These cookies allowed intruders access to user accounts without a password.

Yahoo began to suspect the breach when law enforcement officials approached the company and advised them that they had observed Yahoo user account names and passwords for sale on the darknet market site "TheRealDeal." The seller, known as "Peace_of_Mind," stated in confidential interviews with VICE and WIRED magazines that he had possessed the data for some time and had been selling it privately since late 2015. Yahoo confirmed that stolen user account information would have included names, e-mail addresses, telephone numbers, dates of birth, hashed passwords and, in some cases, encrypted or unencrypted security questions and answers.

Yahoo's delay in discovering and reporting these breaches, as well as implementing improved security features, has become a point of criticism for the company.

Link http://www.cnbc.com/2016/09/22/yahoo-data-breach-is-among-the-biggest-in-history.html

Date 22nd September 2016

© 2017, Cloud Security Alliance. All right reserved.

LinkedIn failure to salt passwords when hashing -

Insufficient Identity, Credential and Access Management

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 12]

Anecdote/Example

In 2012, LinkedIn reportedly lost 167 million account credentials in a data breach. A hacker stole encrypted passwords from the site, cracked and posted them to a Russian crime forum the following day. The hacker, known as "Peace_of_Mind," was observed selling e-mail and password combinations on a dark web marketplace.

Internet security experts said the passwords were easy to unscramble because of LinkedIn's failure to use a salt when hashing them. This is considered an insecure practice because it allows attackers to quickly reverse the scrambling process using existing standard rainbow tables and pre-made lists of matching scrambled and unscrambled passwords.

The LinkedIn compromise is connected to a number of confirmed incidents where data exfiltration has taken place at other organizations, including Citrix Systems.

On June 18, 2016, Citrix posted an alert warning of an incident that forced the company to reset all of their customer's passwords. John Bennett, product line director for Citrix, explained the problem in a Threatpost article.

"Citrix can confirm the recent incident was a password reuse attack, where attackers used usernames and passwords leaked from other websites to access the accounts of GoToMyPC users," Bennett said.

Security researchers confirmed that attackers who had the LinkedIn list would know the person's name, their work history, and their password, giving them a list of possible targets and some base passwords to start with.

Link http://arstechnica.com/security/2016/05/then-there-were-117-million-linkedin-password-breach-much-bigger-than-thought/

Date 18th May 2016

© 2017, Cloud Security Alliance. All right reserved.

Instagram abuse of account recovery -

Insufficient Identity, Credential and Access Management

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 12
Anecdote/Example	A security researcher determined that Instagram's password reset process could easily allow an attacker to access a password reset page without entering any credentials. A successful attack could be executed as long as the hacker had an account ID name, information the researcher surmised could be easily guessed. From the password reset page, the attacker could update the e-mail address or phone number of the temporarily locked account and then perform a password reset via e-mail to gain full access. Approximately, 4 percent, or 20 million accounts, were vulnerable to such an attack. However, there have been no known reports of Instagram accounts being compromised in this manner.
Link	http://www.infosecurity-magazine.com/news/20m-instagram-accounts-vulnerable/
Date	23rd May 2016

© 2017, Cloud Security Alliance. All right reserved.

MongoDB Mexican voter information leak -

Insufficient Identity, Credential and Access Management

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 12
Anecdote/Example	In April 2016, Chris Vickery, a security researcher from MacKeeper, browsed the Shodan search engine for MongoDB open ports (port:27017). During his search, he stumbled upon an open MongoDB instance hosted on Amazon AWS without any authentication or access control protecting the service. He also discovered what seemed to be a significant amount of personally identifiable information belonging to Mexican citizens, later determined to be voting records of 93 million Mexican voters owned by the National Electoral Institute of Mexico.
Link	http://www.informationweek.com/cloud/infrastructure-as-a-service/93-million-mexican-voter-database-exposed-on-amazon-cloud/d/d-id/1325259 http://www.csoonline.com/article/3060204/security/mongodb-configuration-error-exposed-93-million-mexican-voter-records.html https://www.theregister.co.uk/2016/04/25/mexico_voter_data_breach/
Date	26th April 2016

© 2017, Cloud Security Alliance. All right reserved.

MongoDB unprotected, attacked by ransomware -

Insufficient Identity Credential Access Management

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 12]

Anecdote/Example

Typically, ransomware has been used by hackers to encrypt part or all of a user's data. The demand for ransom payments is usually requested in the form of untraceable bitcoin cryptocurrency. Recent ransomware attacks have also targeted online MongoDB instances, taking advantage of weak configurations in the installation of MongoDB in Internet-accessible databases.

Here's how it works: A database that is directly Internet accessible is listening to query requests on certain ports. When a query request is received, it should be authenticated before being executed. But in this case, since the database is accessible from the Internet, it may be fingerprinted by the listening ports easily. Because there is no password for the administrator, any changes may be made as an admin without a password, up to and including removal of all data in the database and leaving a ransom note. The owner of the database has to pay the ransom to get the data back.

Unlike other ransomware attacks, this one needs no advanced malware or exploitation to be successful. The database are vulnerable because a simple best practice was bypassed. To prevent attacks, databases should not be exposed to the Internet; rather, they should be accessed through a local host only during setup. Additionally, other safeguards include properly configuring databases with passwords and other access controls and utilizing authentication mechanisms prior to Internet connectivity.

Link http://www.networkworld.com/article/3154536/security/hacker-wiping-unprotected-mongodb-installs-and-holding-data-for-ransom.html#tk.twt_nww

Date 4th January 2016

© 2017, Cloud Security Alliance. All right reserved.

Moonpig insecure mobile application -

Insecure Interfaces and APIs

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 15
Anecdote/Example	In 2015, Moonpig—a European online greeting card vendor that created a mobile application for sending e-cards—was the victim of a data breach that occurred because of an insecure API. Moonpig's mobile application used static authentication, providing only one set of certificates for all users. Additionally, customer IDs were numbered sequentially, not utilizing the best practice of random seeding/padding. Attackers gathered Moonpig's customer information by simply trying all customer IDs in order. While compromised data for Moonpig's 3.6 million customers in the U.K., U.S., and Australia did not include complete credit card numbers, the last four digits of credit card numbers, card expiration dates and customer names were stolen.
Link	http://computerworld.com/article/2865794/moonpig-jeopardizes-data-of-millions-of-customers-through-insecure-api.html
Date	6th January 2015

© 2017, Cloud Security Alliance. All right reserved.

Dirty Cow Linux privilege escalation vulnerability -

System Vulnerabilities

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 17]

Anecdote/Example

The Dirty Cow Linux vulnerability was in existence for at least eight years prior to patch availability in November 2016.

This vulnerability gives guest users the ability to gain root/admin-level access to a Linux machine by virtue of triggering a race condition in the kernel. A defense-in-depth approach will mitigate access to a guest user.

If exploited, this vulnerability has implications at the server level (especially on servers which do not have automatic patching enabled by default or have non-reliable Internet access), as well as at the client level via Android machines. Additionally, the vulnerability is only patched above Android version 7.0.

This vulnerability can potentially impact cloud computing at three levels: (1) cloud service providers must protect underlying infrastructure; (2) systems utilizing Infrastructure as a Service (IaaS) strategies must be protected and; (3) devices that administrators use also require protection. Given that only 2 percent of all Android machines used globally are updated to the latest version 7.0, there is ample opportunity to exploit this huge, installed base of more than 1 billion machines.

Link

https://www.linux.com/blog/how-bad-dirty-cow

https://threatpost.com/dirty-cow-vulnerability-patched-in-android-security-bulletin/122266/

https://threatpost.com/google-releases-supplemental-patch-for-dirty-cow-vulnerability/121843/

https://source.android.com/security/bulletin/2016-12-01.html

https://developer.android.com/about/dashboards/index.html

https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

https://www.statista.com/statistics/385001/smartphone-worldwide-installed-base-operating-systems/

Date 24th October 2016

© 2017, Cloud Security Alliance. All right reserved.

OAuth Insecure implementation -

Account Hijacking

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 19
Anecdote/Example	Researchers found that more than 40 percent of third-party mobile apps, when tested, are vulnerable to man-in-the-middle attack. This is due to insecure implementation of OAuth 2.0, which allows attackers to exploit user accounts. The root cause is misplaced trust in the authenticating information received from the mobile application.
Link	https://threatpost.com/oauth-2-0-hack-exposes-1-billion-mobile-apps-to-account-hijacking/121889/
Date	10th November 2016

© 2017, Cloud Security Alliance. All right reserved.

Zynga ex-employees alleged data theft -

Malicious Insiders

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 21
Anecdote/Example	Employees with access to highly confidential files at game company Zynga copied a large quantity of proprietary data from the company's Google Drive account to a local USB drive before leaving the company to join a rival game maker.
Link	http://arstechnica.com/tech-policy/2016/11/zynga-sues-2-former-employees-over-alleged-massive-data-heist/
Date	29th November 2016

© 2017, Cloud Security Alliance. All right reserved.

T-Mobile customer information theft -

Malicious Insiders

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 21
Anecdote/Example	A malicious insider is very hard to cope with, as one Czech Republic T-Mobile company discovered. According to multiple news outlets reporting on the story in June 2016, an employee who was "part of a small team that worked with customer data" was caught trying to sell 1.5 million customer records on the black market.
Link	http://thehackernews.com/2016/06/t-mobile-hacked.html
Date	20th June 2016

© 2017, Cloud Security Alliance. All right reserved.

NetTraveler advanced persistent threats -

Advanced Persistent Threats (APTs)

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 23]

Anecdote/Example

NetTraveler, an APT used in cyber-attack campaigns since 2016, is delivered by actors to targets in Russia, Mongolia, Belarus and other European countries via spear phishing. NetTraveler is a Trojan that uses Uniform Resource Locator (URL) links to Roshal Archive (RAR)-compressed executables and Microsoft (MS) Office attachments, built with the MNKit, that exploits the CVE-2012-0158 vulnerability.

In January 2016, the Palo Alto Networks blog reported: "On December 12, 2015, a spear-phishing e-mail was sent to a diplomat of the Embassy of Uzbekistan. The body and subject of the e-mail suggests that the e-mail was spoofed to look like it was sent by the Russian Foreign Ministry and the attachment may contain an official annual report on CHS (Council of Heads of Member States), who form the SCO (Shanghai Cooperation Organization)."

The attachment was found to have been created with the MNKit Toolkit.

When the document delivered by the e-mail is opened, an executable is deposited on the user's system that could exploit a weakness in the Microsoft Media Server (MMS) Windows Common Controls ActiveX control (MSCOMCTL.OCX), which in turn could allow a remote attacker to execute arbitrary code on the system with the privileges of the victim.

The Common Vulnerabilities and Exposures (CVE) associated with NetTraveler, CVE-2012-0158, has been addressed in current versions of MS Office. This APT, however, is still active and used in targeting organizations that include weapons manufacturers, human rights activists, and pro-democracy groups.

Link

https://www.proofpoint.com/sites/default/files/proofpoint_q4_threat_report-a4.pdf - Page 18 – NetTraveler APT Targets Russian, European Interests

https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests

http://researchcenter.paloaltonetworks.com/2016/01/nettraveler-spear-phishing-email-targets-diplomat-of-uzbekistan/

Date

7th July 2016

© 2017, Cloud Security Alliance. All right reserved.

Virlock ransomware -

Data Loss

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 25
Anecdote/Example	Virlock is a special case of ransomware that encrypts files and also infects them, thereby making it a polymorphic file infector ransomware. As a result, any user who subsequently opens the infected file also becomes infected, infecting/encrypting all the files on the new system. Virlock ransomware exhibits a new propagation vector with a combination of ransomware and file infection characteristics that would be detrimental for an enterprise organization. This infection amplification requires adequate security scanning on all resources, including cloud shares.
Link	https://resources.netskope.com/h/i/290799411-cloud-malware-fan-out-with-virlock-ransomware
Date	27th September 2016

© 2017, Cloud Security Alliance. All right reserved.

Yahoo breach -

Insufficient Due Diligence

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 27]

Anecdote/Example

In July 2016, Verizon agreed to buy Yahoo's core Internet business for $4.8 billion, although the final sale is pending. Since that time, two major breaches of Yahoo's security have been reported. The first breach—occurring in August 2013—was reported in December 2016. This attack affected approximately 1 billion user accounts. The most recent breach—occurring in late 2014 and reported in September 2016—affected approximately 500 million accounts.

Concerns regarding disclosure, security policies, security procedures and apparent lackluster investments in system-wide security infrastructure have been raised. Why did reporting take so long? Why was old encryption technology used? Why were security questions and answers stored without encryption?

The most significant comment came from Verizon General Counsel Craig Silliman: "I think we have a reasonable basis to believe right now that the impact is material, and we're looking to Yahoo to demonstrate to us the full impact. If they believe that it's not, then they'll need to show us that."

As a result of the attacks, the two companies announced a revised agreement on February 21, 2017 to cut the original price of their deal by $350 million. Under the new conditions, Yahoo will also be responsible for liabilities arising from shareholder lawsuits and U.S. Securities and Exchange Commission (SEC) investigations. Additionally, after the sale is finalized, Yahoo will continue to be responsible for 50 percent of any cash liabilities that may be incurred related to non-SEC investigations, as well as third-party litigation connected to the breaches. The transaction is still expected to close sometime in the second quarter of 2017.

Link

https://en.wikipedia.org/wiki/Yahoo!_data_breaches

https://www.leahy.senate.gov/imo/media/doc/9-27-16%20Yahoo%20Breach%20Letter.pdf

http://fortune.com/2016/12/19/yahoo-hack-cyber-security/

http://www.nbcnews.com/tech/tech-news/your-yahoo-account-was-probably-hacked-company-set-confirm-massive-n652586

http://www.reuters.com/article/us-verizon-yahoo-cyber-idUSKCN12D2PW

http://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement

Date 1st July 2016

© 2017, Cloud Security Alliance. All right reserved.

Malware using cloud services to exfiltrate data and avoid detection -

Abuse and Nefarious Use of Cloud Services

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 30]

Anecdote/Example

Cloud services provide excellent infrastructure or platforms to build applications. They are robust, accessible and have many cost advantages when properly designed. However, these same advantages also attract hackers because cloud infrastructure is a tempting location for hosting Command and Control (C&C) infrastructure for botnets. Organizations rarely block traffic to large cloud providers, meaning cloud services are nearly always accessible. Because legitimate traffic is also used in conjunction with malicious traffic, nefarious traffic is harder to detect.

In December 2015, a FireEye report revealed a spear phishing campaign—directed at a Hong Kong media organization—that used a variant of the LOWBALL malware to target the local network. The malware used Hyper Text Transfer Protocol Secure (HTTPS) to access Dropbox application programming interface (API) and download configuration files located on a Dropbox shared folder. The use of such a common API over legitimate ports to a commercial service is utilized by attackers in order to "blend into the crowd," thus avoiding certain types of detection tools over the network.

Link http://www.securityweek.com/malware-used-china-apt-group-abuses-dropbox

Date 1st December 2015

© 2017, Cloud Security Alliance. All right reserved.

Zepto ransomware spread and hosted on cloud storage services -

Abuse and Nefarious Use of Cloud Services

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 30
Anecdote/Example	In July 2016, security researchers discovered a new strain of the Zepto ransomware shared among cloud users. This strain of Zepto arrives at its destination via spam e-mails that use enticing messages and file names to encourage the recipient to open the e-mail and download the infected file. These files use an extension of .wsf, which causes Windows to assign an icon that appears similar to a spreadsheet icon. This icon (coupled with a filename of spreadsheet_286.wsf) may cause all but the most attentive recipients to view the attachment as legitimate. The files/messages are then shared among colleagues using cloud SaaS applications such as Microsoft OneDrive, Google Drive, Box, Dropbox, etc.
Link	https://resources.netskope.com/h/i/273457617-zepto-variant-of-locky-ransomware-delivered-via-popular-cloud-storage-apps
Date	19th July 2016

© 2017, Cloud Security Alliance. All right reserved.

CloudSquirrel malware hosting command and control (C&C) in Dropbox -

Abuse and Nefarious Use of Cloud Services

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 30]

Anecdote/Example Likely originating in Brazil (based on names and parameters), CloudSquirrel is written in Java and is distributed using ServInt's Jelastic Platform-as-a-Service (PaaS). Jelastic redirects to the CloudApp collaboration platform which, in turn, uses Amazon AWS for its backend cloud services. This cloud malware actively uses Dropbox for its Command and Control (C&C) communications.

The CloudSquirrel attack arrives via an e-mail phishing attack. This attack e-mail attempts to trick its victim into opening it with a "tax invoice" or other seemingly official-sounding links. Once open, CloudSquirrel infects users by downloading additional malicious encrypted payloads via a JAR file. Payloads can include information and password stealers. Once the cloud malware establishes a connection with its C&C hosted in Dropbox, its commands masquerade as plain text files with fake extensions, such as .mp4, .wmv, .png, .dat, and .wma.

Link https://resources.netskope.com/h/i/272453388-cloudsquirrel-malware-squirrels-away-sensitive-user-data-using-popular-cloud-apps

Date 15th July 2016

© 2017, Cloud Security Alliance. All right reserved.

CloudFanta Malware using cloud storage for malware delivery -

Abuse and Nefarious Use of Cloud Services

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 30
Anecdote/Example	CloudFanta arrives as an attachment or link in a spear phishing e-mail that lures the victim to execute the file or click the link. The CloudFanta malware uses the SugarSync cloud storage app for delivering a JAR file that functions as a downloader. The downloader JAR file again uses SugarSync for downloading Dynamic Linked Library (DLL) files with a ".png" extension. These DLL files, which are later renamed to the extension ".twerk," are responsible for stealing the victim's e-mail credentials, sending malicious e-mails on behalf of the victim, and also for monitoring victims' online banking activities.
Link	https://resources.netskope.com/h/i/295875750-cloudfanta-pops-with-the-cloud-using-sugarsync
Date	18th October 2016

© 2017, Cloud Security Alliance. All right reserved.

Dyn DDoS attack -

Denial of Service

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 32]

Anecdote/Example

This attack involved compromised Internet of things (IoT) devices that either had no basic password protection or were enabled with default passwords. The attackers targeted the Domain Name System (DNS) provider, Dyn, after attacking well-known security journalist Brian Krebs.

This attack affected the ability of customers to access many major cloud-based companies, including Twitter, Spotify and some cloud service providers offering various cloud-based services such as authentication and encryption. Many of these companies exclusively used Dyn for their Domain Name Service and were thus unable to sidestep the attack.

Mitigations for this attack included either using a secondary DNS provider in-house, or another third-party DNS provider as a backup.

The attack was finally stopped by blocking all infected IoT devices from the Internet. As long as IoT device manufacturers continue to use default passwords and legacy network protocols (telnet), such attacks will continue to occur in the future.

Link

http://www.darkreading.com/attacks-breaches/ddos-attack-on-dns-provider-disrupts-okta-twitter-pinterest-reddit-cnn-others/d/d-id/1327252

https://www.nanog.org/sites/default/files/20161016_Madory_Backconnect_S_Suspicious_Bgp_v2.pdf

https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

https://blog.cloudmark.com/2016/10/21/circumventing-the-dyn-ddos-attack-and-preventing-others-like-it/

http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet

Date 21st October 2016

© 2017, Cloud Security Alliance. All right reserved.

Australian Bureau of Statistics denial of service -

Denial of Service

Original Reference [The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 32]

Anecdote/Example

On August 9, 2016, the Australian Bureau of Statistics (ABS) attempted to implement the first national census conducted fully online. Despite planning for issues related to anticipated load and conducting systems tests prior to launch, the census website crashed and went offline on census night. As a result, no one was able to complete their (legally required) census form.

The ABS released a media statement on August 10, stating: "The 2016 online census form was subject to four Denial of Service attacks yesterday of varying nature and severity. The first three caused minor disruptions...After the fourth attack, just after 7:30 p.m., the ABS took the precaution of closing down the system to ensure the integrity of the data."

In a subsequent senate hearing, representatives reported that the majority of DDoS traffic that brought the website down was routed through Singapore. IBM executives admitted that outage may not have occurred if they had turned their router "off and on again."

Link

http://www.cso.com.au/article/604910/attack-australian-census-site-didn-t-register-global-ddos-sensors/

http://www.cso.com.au/article/604910/attack-australian-census-site-didn-t-register-global-ddos-sensors/

http://www.abs.gov.au/ausstats/abs@.nsf/mediareleasesbyReleaseDate/617D51FA32D27BF9CA25800A0077B7BD?

http://www.abc.net.au/news/2016-10-25/abs-officials-face-parliamentary-grilling-over-census/7960480

Date

11th August 2016

© 2017, Cloud Security Alliance. All right reserved.

Cloudflare/Cloudbleed buffer overrun vulnerability -

Shared Technology Vulnerabilities

Original Reference	The Treacherous 12: Cloud Computing Top Threats in 2016 – Pg. 34
Anecdote/Example	Cloudflare is a popular online web security-as-a-service offering. It provides content distribution, protection against denial of service and other web-based attacks. In February 2017, Tavis Ormandy from Google's Project Zero security team discovered that three of Cloudflare's features contained a buffer overrun vulnerability that led to memory leakage. The vulnerability was triggered by unbalanced Hypertext Markup Language (HTML) tags on pages. Passwords, API keys and confidential chats from various Cloudflare customers are amongst the data leaked and possibly cached by search engines. The vulnerability has since been named "Cloudbleed," and reportedly affected 3,438 domains and 150 Cloudflare customers.
Link	https://www.theregister.co.uk/2017/02/24/cloudbleed_buffer_overflow_bug_spaffs_personal_data/ https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/
Date	23rd February 2017

© 2017, Cloud Security Alliance. All right reserved.