Feature

Cloud Insecurities

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CBCP, CDP, CISSP, ITIL V3, is an IT security consultant at ActioNet Inc., with more than 15 years of experience in IT security. Wlosinski has been a speaker on cloud security at US government and professional conferences and meetings, and has written numerous articles on the topic for professional magazines and newspapers.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

Information security events that affect cloud systems are occurring with no end in sight, so it should be no surprise that the cloud should be treated as a nonsecure environment with numerous threats and concerns. The cloud has all of the same (and even more) vulnerabilities and weaknesses as other computing platforms, including configuration issues, patching and upgrade requirements (to fix weaknesses), source code issues, unauthorized privilege escalation, and unexpected downtime, to name a few. A statistical analysis of cloud security incidents over a five-year period identified 175 cloud security incidents and 12 threats to cloud security (**figure 1**).[1]

Figure 1—CSA Threat Categories and Incident Counts

Number	Threat	Incidents
1	Abuse and nefarious use of cloud computing	12
2	Insecure interfaces and application programming interfaces (APIs)	51
3	Malicious insiders	3
4	Shared technology issues	5
5	Data loss or leakage	43
6	Account or service hijacking	3
7	Unknown risk profile	11
8	Hardware failure	18
9	Natural disasters	4
10	Closure of cloud service	4
11	Cloud-related malware	6
12	Inadequate infrastructure design and planning	15
	TOTAL	**175**

The average unavailability of cloud services has been stated to be 7.5 hours per year, which amounts to an availability rate of 99.9 percent. The cost of an hour-long outage ranges between US $89,000 and US $225,000 per hour.[2] These costs underscore the importance of having a cloud security program within an organization that will satisfy customer expectations.

The following information on vulnerabilities, threats and weaknesses is intended to not only enlighten those who manage the cloud, but also bring an awareness of what to monitor and how to implement and maintain a secure cloud environment.

PROVIDER VULNERABILITIES

The threats to cloud platforms are ongoing and affect everyone who uses cloud services for business or personal reasons.[3] **Figure 2** contains a list of recent examples of cloud-related events that were the result of security weaknesses at the provider.

PREVENTING EVENTS

The solutions lie with the providers. Providers need to implement more proactive programs in the areas of configuration management, web application hardening, internal security (e.g., background checks) and continuous monitoring, which include a regular patching program, updating of antivirus systems and event log management. The cloud service providers (CSPs) should also have mirrored systems to provide for increased uptime, a means for a patching program and business continuity for their customers.

Actions that should be taken to prevent events like those listed in **figure 2** include:

- **Configure the network and devices**—Applicable actions include removing unnecessary services and setting control parameters to only what is necessary.
- **Patch and update the system components regularly**—This includes the operating system, commercial-off-the-shelf (COTS) products, system utilities and the software that is used for custom applications. Do not expect the software used to be perfect. It is subject to human error as well.
- **Run vulnerability scans and remediate weaknesses as quickly as reasonably possible**—Critical and high vulnerabilities are the most serious and should be corrected as soon as possible.

Figure 2—Vendor Vulnerability Summary			
Report Date	**Provider/Vendor**	**Problem Type**	**Event**
9 October 2012	CloudStack	Configuration issue	The system had a configuration issue that meant any use could execute arbitrary CloudStack API calls, such as deleting all virtual machines (VMs) in the system.
22 October 2012	Amazon AWS	System not available	Several web sites that use Amazon's AWS cloud computing service for hosting, including Reddit, Coursera, Flipboard, FastCompany, Foursquare, Netflix, Pinterest and Airbnb, were taken down as it experienced degraded performance for a small number of Elastic Block Store (EBS) volumes in a single availability zone in the Northern Virginia (USA) zone.
30 October 2012	Not specified	Inadequate CSP protection	Some CSPs failed to detect and block malicious traffic originating from their networks, which provided cybercriminals with an opportunity to launch attacks in a botnet-like fashion, according to a report from security consultancy firm, Stratsec.
6 November 2012	Amazon EC2	Inadequate key protection	Scientists devised a VM that can extract private cryptographic keys stored on a separate VM when it resides on the same piece of hardware.
16 November 2012	VMware	Directory traversal vulnerability	VMware patched a critical vulnerability in its VMware View desktop virtualization product that could have led to a directory traversal attack and an attacker reading or downloading files without the need for authentication.
28 November 2012	Cloud browsers	Mobile device weaknesses	Researchers found that mobile device browser services can be abused to crack passwords, wage denial-of-service (DoS) attacks or perform other unauthorized computations with the free computing power.
28 March 2013	Amazon	Data exposure	A researcher at Rapid 7 found sensitive files exposed to the Internet in Amazon's Simple Storage System (S3) cloud service due to users improperly configuring the service.
25 August 2013	Amazon	Data integrity	A packet loss issue at an Amazon cloud services data center caused outages for several high-profile web services including Instagram, Netflix and Vine. The problem was caused by a partial failure of a networking device.
15 November 2013	VMware	Account privilege escalation	VMware released updates for its VMware Workstation and VMware Player software, thereby fixing a vulnerability in how shared libraries are handled. The vulnerability could have allowed an attacker to escalate their privileges to root.
4 December 2013	VMware	Privilege escalation	VMware published updates for certain versions of its Workstation, Fusion, ESXi and ESX products, closing a vulnerability that could have allowed privilege escalation in older versions of Windows.
31 January 2014	Oracle's Java	Unauthorized access and more	Researchers at Security Explorations analyzed Oracle's Java Cloud Service and found 28 security issues—16 of which could be leveraged to bypass the Java security sandbox of a targeted WebLogic server environment. The vulnerabilities could also be leveraged to gain access to deployments of other users in the same regional data center.
23 April 2014	Amazon	Missing patches	In the course of a customer-prompted investigation, researchers at Bkav found that several servers for Amazon's cloud Infrastructure as a Service (IaaS) and HP's public cloud service contain several vulnerabilities as a result of Microsoft Windows Server installations not being updated for several months.
15 May 2014	Adobe	System availability	Adobe restored service to users of its Creative Cloud service after a 24-hour outage that left users unable to use some aspects of the service and unable to use the service if not already logged in.
25 June 2014	Oracle DB Java VM	Privilege escalation	Security Explorations' researchers reported finding 22 vulnerabilities affecting the Java VM implementation used in Oracle Database that could be leveraged by an attacker to escalate privileges and execute arbitrary Java code on vulnerable Oracle Database servers.

Figure 2—Vendor Vulnerability Summary *(cont.)*

Report Date	Provider/Vendor	Problem Type	Event
26 June 2014	VMware	Product vulnerabilities	VMware released an update for its vCenter Operations Management Suite (vCOps) that closed several vulnerabilities affecting the Apache Struts Java application framework.
23 July 2014	VMWare vCenter servers	Product vulnerabilities	Data collected and analyzed by CloudPhysics found that 57 percent of deployed VMware vCenter servers and 58 percent of ESXi hypervisor hosts remained vulnerable to the Heartbleed virus in OpenSSL, affecting 40 percent of organizations in the CloudPhysics dataset.
2 October 2014	VMware	Product vulnerabilities	VMware releases a software patch to fix Shellshock bug.

Based on: US Department of Homeland Security (DHS), Daily Open Source Infrastructure Reports, USA, 2013-2014, *www.dhs.gov/dhs-daily-open-source-infrastructure-report*

- **Design and implement good architectural best practices**—This includes having at least one firewall. If an organization is on the receiving end of a DoS attack, consider sharing (or splitting) the attack among multiple and/or layered firewalls. Having an intrusion detection system (IDS) and an intrusion prevention system (IPS) that is monitored daily is essential to protecting systems and data. If an organization lacks internal capability, investigate Security as a Service (SecaaS). Having a third party that is dedicated to protecting an organization's assets will compensate for lack of staff or the appropriate skill sets. Organizations should also consider having a network architect to design a secure environment.
- **Prepare for unexpected hardware failures**—This can be done with spare devices/components, a tested contingency plan and, possibly, a mirrored site.

CRIMINAL ACTIVITY

Since October 2012, many criminal and malicious activities have occurred in the cloud environment, for example:

- VMware source code exposure[4]
- Advanced persistent threats (APTs) utilizing cloud-based platforms[5]
- Cybercriminals using cloud services to distribute their malware[6]
- Cybercriminals using Google Cloud Messaging as a command and control for their Android malware[7]
- Spammers using SoundCloud to spread links to spam[8]
- Cloud hosting service provider DigitalOcean targeted by a distributed denial-of-service (DDoS) attack[9]
- A cloud-based Microsoft Structured Query Language (MSSQL) database used by a botnet to steal online banking credentials[10]
- A hypervisor management console used by attackers who exploited an insecure password[11]
- Cybercriminals abusing cloud services to create and host malicious web sites[12]
- The Trojan Zeus used to attack Platform as a Service (PaaS) and Software as a Service (SaaS) infrastructures[13]
- Vulnerabilities in major web browsers used to compromise cloud-based point of service (PoS) software used by grocery stores, retailers and small businesses[14]
- CodeSpaces ceased operations because an attacker accessed their Amazon Elastic Compute Cloud (EC2) and deleted the customer database and most backups[15]
- Botnets and malware hosted on cloud servers[16]
- Attackers using Amazon Cloud Services to launch DDoS attacks[17]
- Cybercriminals using Amazon cloud to host Linux DDoS Trojans[18]

To combat these types of events, the following actions could have been taken by CSPs:

- Implement a company security program that includes patching, configuration management, firewall, antivirus software, intrusion detection and prevention systems, testing backup recovery capability, performing web site scans, and using data encryption whenever possible (especially for critical systems and sensitive data).
- Conduct awareness training. Users need to be trained on spam and other criminal tricks that can circumvent technical defenses.
- Implement a secure network design that is able to withstand DDoS attacks.
- Implement password strength testing and controls that limit access attempts.

- To prevent (or limit) cloud provider misuse, implement a program of continuous monitoring of outbound traffic for contract violations (i.e., enforcement of security practices), implement SecaaS, and harden web sites/applications against SQL attacks.

OTHER WEAKNESSES

Weaknesses in the cyberworld that affect cloud system users include users not having the tools or means to prevent remote access. One example is that operating systems (OSs) do not identify what is running in the tasking/monitoring table(s). Since the utilities are cryptic, users will not even try to end a system process on their computer because they fear that deleting one could possibly harm their system(s). More actionable information needs to be available to users in the operating system utilities to protect their computing devices because purchased, existing tools (e.g., firewalls, antivirus software, intrusion detection systems) are not good enough. User action is the last resort and the OS information provided is currently insufficient to protect these devices. Malware is constantly being installed on home computers and portable devices via the Internet, and the cloud and CSPs are being used as distribution agents for criminals. Providers need to implement security measures similar to those that governments and financial institutions use to protect their systems and their data.

Vendor products, such as security suites, that continually report that a system has weaknesses and that settings have changed and malware are other areas of concern. Vendors need to come together to unite their efforts for the optimal solution. Competition between antivirus vendors can do only so much to aid the user. This is because vendors are not constantly at their best. Reasons include being distracted by company takeovers, loss of key staff and poor product comparative ratings. These product weaknesses affect everyone and need to be dealt with in a cooperative manner.

> “Think like criminals in order to better know their methods.”

WHAT ELSE CAN BE DONE?

To prevent misuse of the cloud, organizations should think like criminals in order to better know their methods, asking themselves, for example: How does the organization combat an attack system that searches all computers connected to the Internet for weaknesses? The answer may lie in understanding a cybercriminal's approach to conducting an attack. The following steps taken by an attacker leading up to an attack can be analyzed and countermeasures implemented:

1. Gather data of device weaknesses.
2. Create or obtain a program or series of programs to exploit those weaknesses.
3. Plant malware to allow access and retrieve data of value from those devices.
4. Categorize the devices by expected value (e.g., bank, accounting system, private personnel information, normal users).
5. Assign specialists to search and retrieve data of value (e.g., account numbers, customer names, passwords, privacy information).
6. Store and compile the data for misuse (e.g., funds transfer, blackmail, identity theft, resale).

Another question to ask is: If one knows what countries are not cooperating with capturing and preventing malicious cyberactivity, what can be done to prevent those countries from receiving data? Furthermore, should there be a strengthening of international laws (especially by country) to restrict the data they receive? Do new monitoring devices and/or software that enforce the law(s) need to be created and implemented? Where could these protective tools be placed, and could they be used to track the source(s)?

With all of the vulnerabilities, threats and malicious activity that are going on, it is important to be as vigilant with a private cloud (i.e., your in-house computing environment) as with public clouds.

CONCLUSION

In addition to what businesses can do to protect themselves, authorities need to work with businesses to implement protections and enforcement on a global scale. Many clouds are not only global in nature, but because of the surge in mobile devices and applications, they affect many people wherever they go.

ENDNOTES

[1] CSA Cloud Vulnerabilities Working Group, "Cloud Computing Vulnerability Incidents: A Statistical Overview," Cloud Security Alliance, 13 March 2013, *https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/*

[2] Essers, L.; "Cloud Failures Cost More Than $70 Million Since 2007, Researchers Estimate," *PCWorld*, 19 June 2012, *www.pcworld.com/article/257860/cloud_failures_cost_more_than_70_million_since_2007_researchers_estimate.html*

[3] US Department of Homeland Security (DHS), Daily Open Source Infrastructure Reports, USA, 2013-2014, *www.dhs.gov/dhs-daily-open-source-infrastructure-report*

[4] Leyden, John; "More VMware Secret Source Splattered Across Internet," *The Register*, 5 November 2012, *www.theregister.co.uk/2012/11/05/vmware_source_code_leak/*

[5] Kovacs, Eduard; "Experts Reveal How Chinese APT Hackers Abuse Dropbox and WordPress," *Softpedia*, 12 July 2013, *http://news.softpedia.com/news/Experts-Reveal-How-Chinese-APT-Hackers-Abuse-Dropbox-and-WordPress-367652.shtml*

[6] Vijayan, Jaikumar; "Attackers Turning to Legit Cloud Services Firms to Plant Malware," *Computerworld*, 2 August 2013, *https://www.computerworld.com/s/article/9241324/Attackers_turning_to_legit_cloud_services_firms_to_plant_malware*

[7] Kovacs, Eduard; "Hackers Abuse Google Cloud Messaging Service in Android Malware Attacks," *Softpedia*, 14 August 2013, *http://news.softpedia.com/news/Hackers-Abuse-Google-Cloud-Messaging-Service-to-Distribute-Android-Malware-375327.shtml*

[8] Kovacs, Eduard; " SoundCloud Users Warned of Spam Shady Software, Scams," *Softpedia*, 22 August 2013, *http://news.softpedia.com/news/SoundCloud-Users-Warned-of-Spam-Shady-Software-Scams-377395.shtml*

[9] Kovacs, Eduard; "Cloud Hosting Company DigitalOcean Hit by DDoS Attack," *Softpedia*, 28 August 2013, *http://news.softpedia.com/news/Cloud-Hosting-Company-DigitalOcean-Hit-by-DDOS-Attack-378713.shtml*

[10] Jackson Higgins, Kelly; "Cybercriminals Now Enlisting Database Cloud Services," *InformationWeek* DARKReading, 11 December 2013, *www.darkreading.com/attacks-breaches/cybercriminals-now-elisting-database-clo/240164662*

[11] Kovacs, Eduard; "Softpedia, OpenSSL Website Hacked Through Insecure Password at Hosting Provider," *Softpedia*, 3 January 2014, *http://news.softpedia.com/news/OpenSSL-Website-Hacked-Through-Insecure-Password-at-Hosting-Provider-413377.shtml*

[12] Kovacs, Eduard; "Man Admits Hacking Former Employer's Systems to Damage Servers and Reputation," *Softpedia*, 9 January 2014, *http://news.softpedia.com/news/Man-Admits-Hacking-Former-Employer-s-Systems-to-Damage-Servers-and-Reputation-415363.shtml*

[13] Peters, Sara; "Zeus Being Used in DDoS, Attacks on Cloud Providers," *InformationWeek* DARKReading, 10 June 2014, *www.darkreading.com/zeus-being-used-in-ddos-attacks-on-cloud-providers/d/d-id/1269554*

[14] Rashid, Fahmida Y.; "Cybercriminals Targeting Cloud-based PoS Systems Via Browser Attacks," *Security Week,* 12 June 2014, *www.securityweek.com/attackers-targeting-cloud-based-pos-systems-browser-attacks*

[15] Greenberg, Adam; "Code Space Shuts Down Following DDoS Extortion, Deletion of Sensitive Data," *SC Magazine*, 19 June 2014, *www.scmagazine.com/code-spaces-shuts-down-following-ddos-extortion-deletion-of-sensitive-data/article/356774/*

[16] Butler, Brandon; "Hackers Found Controlling Malware and Botnets From the Cloud," *NetworkWorld*, 26 June 2014, *www.networkworld.com/article/2369887/cloud-security/hackers-found-controlling-malware-and-botnets-from-the-cloud.html*

[17] Constantin, Lucian; "Attackers Install DDoS Bots on Amazon Cloud, Exploit Elasticsearch Weakness," *Computerworld*, 28 July 2014, *www.computerworld.com/s/article/9249991/Attackers_install_DDoS_bots_on_Amazon_cloud_exploit_Elasticsearch_weakness?taxonomyId=17*

[18] Kovacs, Eduard; "Cybercriminals Abuse Amazon Cloud to Host Linux DDoS Trojans," *Security Week*, 28 July 2014, *www.securityweek.com/cybercriminals-abuse-amazon-cloud-host-linux-ddos-trojans*