International Journal of Recent Trends in Engineering & Research

Security of Cloud Computing-A Review

Amita Raval
Research Scholar, Department of Computer, India

Abstract: Cloud computing, also known as 'on-demand computing', is a kind of Internet-based computing, where shared resources, data and information are provided to computers and other devices on-demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources.

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing.[3][4][5] Companies can scale up as computing needs increase and then scale down again as demands decrease.

INTRODUCTION

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers.[1] Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community).[1] There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).[6] The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

CLOUD SECURITY CONTROLS

- Deterrent controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. (Some consider them a subset of preventive controls.)

- Preventive controls
  Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.
- Detective controls
  Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue.[2] System and network security monitoring, including interruption detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.
- Corrective controls
  Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

CLOUD SECURITY THRETS

Cloud computing has grabbed the spotlight at this year's RSA Conference 2013 in San Francisco, with vendors aplenty hawking products and services that equip IT with controls to bring order to cloud chaos. But the first step is for organization to identify precisely where the greatest cloud-related threats lie. To that end, the CSA (Cloud Security Alliance) has," the cloud computing threats for 2013[3].

1. First on the list is data breaches. To illustrate the potential magnitude of this threat, CSA pointed to a research paper from last November describing how a virtual machine could use side-channel timing information to extract private cryptographic keys in use by other VMs on the same server. A malicious hacker wouldn't necessarily need to go to such lengths to pull off that sort of feat, though. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other clients' data as well.

The challenge in addressing this threats of data loss and data leakage is that "the measures you put in place to mitigate one can exacerbate the other," according to the report. You could encrypt your data to reduce the impact of a breach, but if you lose your encryption key, you'll lose your data. However, if you opt to keep offline backups of your data to reduce data loss, you increase your exposure to data breaches.

2. The second-greatest threat in a cloud computing environment, according to CSA, is data loss: the prospect of seeing your valuable data disappear into the ether without a trace. A malicious hacker might delete a target's data out of spite -- but then, you could lose your data to a careless cloud service provider or a disaster, such as a fire, flood, or earthquake. Compounding the challenge, encrypting your data to ward off theft can backfire if you lose your encryption key.
   Data loss isn't only problematic in terms of impacting relationships with customers, the report notes. You could also get into hot water with the feds if you're legally required to store particular data to remain in compliance with certain laws, such as HIPAA.
3. The third-greatest cloud computing security risk is account or service traffic hijacking. Cloud computing adds a new threat to this landscape, according to CSA. If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. "Your account or services instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks," according to the report. As an example, CSA pointed to an XSS attack on Amazon in 2010 that let attackers hijack credentials to the site.
   The key to defending against this threat is to protect credentials from being stolen. "Organizations should look to prohibit the sharing of account credentials between users and services, and they should leverage strong two-factor authentication techniques where possible," according to CSA.
4. Fourth on the list of threats are insecure interfaces and APIs. IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. "This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency," the report notes.
5. No. 6 on the list is malicious insiders, which can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From IaaS to PaaS to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. In situations where a cloud service provider is solely responsible for security, the risk is great. "Even if encryption is implement, if the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack," according to CSA.
6. Six on the list is cloud abuse, such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Another example might be a malicious hacker using cloud servers to launch a DDoS attack, propagate malware, or share pirated software. The challenge here is for cloud providers to define what constitutes abuse and to determine the best processes for identify it.
7. Seven on the list of top security threats to cloud computing is insufficient due diligence; that is, organizations embrace the cloud without fully understanding the cloud environment and associated risks. For example, entering the cloud can generate contractual issues with providers over liability and transparency. What's more, operational and architectural issues can arise if a company's development team isn't sufficiently familiar with cloud technologies as it pushes an app to the

cloud. CSA's basic advice is for organizations to make sure they have sufficient resources and to perform extensive due diligence before jumping into the cloud.

8. Eight CSA has pegged shared technology vulnerabilities as the ninth-largest security threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way. "Whether it's the underlying components that make up this infrastructure (e.g. CPU caches, GPUs, etc.) that were not designed to offer strong isolation properties for a multi-tenant architecture (IaaS), re-deployable platforms (PaaS), or multi-customer applications (SaaS), the threat of shared vulnerabilities exists in all delivery models," according to the report.

   If an integral component gets compromised -- say, a hypervisor, a shared platform component, or an application -- it exposes the entire environment to a potential of compromise and breach. CSA recommends a defensive, in-depth strategy, including compute, storage, network, application, and user security enforcement, as well as monitoring.

REFERENCES

1.Srinavasin, Madhan (2012). *"'State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment"*. ACM ICACCI'.
2.Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.
3. *"Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.*
4. *"Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.*
5.*Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.*
6.http://www.infoworld.com/article/2613560/cloud-security/cloud-security-9-top-threats-to-cloud-computing-security.html

