Cloud services: Mitigate risks, maintain availability

Maintain high availability in a cloud environment using cloud service security policy

Judith M. Myerson

March 15, 2011

Businesses and government agencies demand cloud services to provide better security in order to ensure continuous operational availability. To make this a reality, they will need to formulate a cloud service policy on risk mitigation. Learn about cloud service security and how to mitigate risks to cloud services to ensure high uptime availability and security in a cloud environment.

Cloud service security policies focus on different aspects of cloud security, depending to which delivery model scheme you’re referring — SaaS, PaaS, or IaaS:

• Software as a Service (SaaS) policy focuses on managing access to a specific application rented to consumers whether they are private individuals, businesses or government agencies. It should address mitigating risks of SaaS applications that are vulnerable to an attack by a malware application that allocates malicious instance resources. For example, the designated office working hours that the application allows authorized dental assistants to download dental records may be maliciously changed to early morning hours for the convenience of the hackers.

• Platform as a Service (PaaS) policy focuses on protecting data as well as managing access to the applications in a full business life cycle created and hosted by independent software vendors, startups, or units of large businesses. The policy should address mitigating risks of PaaS being used as Command and Control centers to direct operations of a botnet for use in installing malware applications, say, to mess up the dental records.

• Infrastructure as a Service (IaaS) policy focuses on managing virtual machines, as well as protecting data and managing access to the infrastructure of these traditional computing resources underlying the virtual machines in the cloud environment. This policy should address governance framework on mitigating risks to the virtual machines. IaaS has been used as Command and Control centers to direct operations of a botnet for use in malicious updates of the infrastructure within and across the virtual machines.

This article briefly covers important aspects of cloud service security issues and then describes the mitigating risks that are part of a risk assessment program.
Cloud service security
Cloud service security can be threatened by:

- A flawed hypervisor
- Missing threshold policies
- Bloated load balancing
- Insecure cryptography

Let's look at each in more detail.

**Flawed hypervisor**
All cloud service types run on virtual machines on top of an underlying hypervisor that allows multiple operating systems to share a single hardware host. They are accessed by parties of different trust levels: users, tenants, and cloud administrators. For example, a tenant may have a 1000-user license agreement to access certain softwares as services.

When a hypervisor is flawed or compromised, all instance resources and data request queues are compromised. They can maliciously impact threshold policies that are used to monitor the consumption of instance resources and data request queues during spikes in demand for workload. Controls on internal virtual networks that are used to communicate between virtual machines are insufficiently visible to enforce security policies. Duties for network and security controls of virtual machines may not be well separated.

A hacker can become a highly privileged user with administrative controls and get out of a virtual machine and then execute malicious programs on the hypervisor. For example, he may access directory files and maliciously reassign instance resources to another virtual machine. He can cause failure in the mechanisms that separate storage, memory, routing, and reputation between tenants on the same virtual machine.

The hacker can steal sensitive information from residual data that has not been purged from re-allocated instance resources within a virtual machine. The hacker can use a flawed hypervisor to identify the neighbors of a healthy virtual machine and monitor their activity. He can get inside a neighbor's virtual machine and add malicious code to PaaS applications.

**Missing threshold policies**
An end user should evaluate a service provider’s security policy before entering into a relationship. You need to compare the security posture of cloud computing to an on-premise environment and make sure instance resource, user, and data request threshold policies in the cloud are not missing from the security policy.

A resource threshold policy is useful in monitoring how additional instance resources are consumed during spikes of demand for workloads. A user threshold policy checks how many users are concurrently logging in and off a cloud service type and whether they are approaching the maximum number of users as specified in a license.

There are risks to not establishing these policies:
• Without a resource threshold policy, you do not know if instance resources have maliciously reached full capacity causing your cloud service provider to shut down the service without warning.
• Without a user threshold policy, you do not know if the number of concurrent users is approaching the maximum and how many users have not logged off when they are done with the cloud service. Hackers can identify those users.
• Without a data request threshold policy, you do not know the size of the queue of data requests. Hackers can flood the queues with malicious data requests (such as SQL injected requests), causing these queues to reach their maximum capacity.

Bloated load balancing
Load balancing is used to distribute instance resources and data requests. For example, each instance resource should be loaded up to 50 percent of its capacity so that if one instance fails, the healthy ones take over the business transactions from the failed resource instance.

Each queue should be loaded up with data requests up to 50 percent of the queue capacity so that one queue fails, the healthy ones take over the data requests originally destined for the failed queue.

When load balancing of instance resources is maliciously flawed by a malware application in a virtual machine, it can cause the flooding of those resources with malicious transactions filling up each resource to 100 percent of its capacity.

It's impossible to move business transactions from the failed resource instances to the healthy ones. Bloated load balancing cannot be used to implement failover mechanisms, such as instance resource or load sharing redundancy.

Insecure cryptography
Some form of encryption is needed to protect confidentiality and integrity of data. Even if the data is not sensitive or personal, it should be secured with cryptography when transported to and from, and manipulated in, the cloud.

Hackers can take advantage of the advances in cryptanalysis or malicious instance resources to render cryptographic algorithms insecure. They can probe for flaws in a cryptographic algorithm before maliciously modifying them to turn a strong encryption into a weaker one.

Hackers can go further by finding out the latest version of cryptographic algorithms and then on their own machines do reverse-engineering to learn how the algorithms work.

Mitigating risks to cloud services
In a cost-effective manner, you can mitigate risks by applying security controls so you can lower the probability that an asset's vulnerabilities can be exploited and lead to threat implementations.

Before you attempt to mitigate risks, you need to identify assets to be protected. The simplest risk assessment approach is to:
1. Identify the assets
2. Analyze the risks
3. Apply security countermeasures
4. Conduct post-run or -event evaluations

A key concept to remember is that you can loop back through the steps at any stage to incorporate variables that were added later or that you were unaware of.

Start by identifying assets — hardware, software, network components, personnel, users, documentation, facilities; those and other assets that are directly part of a cloud service type. When you identify them, attempt to mitigate risks, and discover you have excluded certain assets, you can always return to this first step to update the inventory of assets and then repeat the second step.

If, during the third step of analyzing security countermeasures, you discover that certain risks have not been addressed, you can return to the second step to include them and to determine the loss potential or probability of each risk that a threat will exploit vulnerabilities. You can return to the first step from the third step to update an inventory of assets to be protected.

In the fourth step, you periodically reassess risk assessment program as impacted by new risks, cost-effective security controls, emerging infrastructure technologies, and new legislations.

Let's look at each step in more detail.

**Step 1. Identify assets**

Both the cloud consumer and provider need to identify hardware and software assets and estimate the cost to replace each asset. They should maintain and periodically update an inventory of assets that can change as a result of organization restructuring, more energy-efficient technologies, better failover mechanisms, and new legislations on exports of data privacy across the boundaries of jurisdictions.

The number of hardware and software assets a consumer needs to identify when renting service from a SaaS provider are far fewer than when the consumer has more control using a PaaS model and to a greater extent, IaaS.

Now, let's take a look at what assets need to be identified for each cloud service type.

**SaaS assets**

Since the only control the cloud consumer has is accessing the application from his desktop, laptop, or a mobile device, the assets he needs to identify are mobile devices operating systems, applications, and default programs. For this reason, it is important to limit your inventory of device assets to programs and applications for use with SaaS. It is not a good idea to mix programs for personal use (like downloaded games) with programs you need to access SaaS on the same device.

At minimum, the following assets should be controlled by a cloud provider:
• Operating systems
• Hardware
• Network infrastructure
• Access management applications
• Instance resources
• SaaS application upgrades and patches

The consumer is not responsible for identifying them.

**PaaS assets**
The assets the cloud consumer needs to identify are those he can control: All the applications in a full business life cycle for the platform (for example, spreadsheets, word processors, backups, billing, payroll processing, and invoicing).

At minimum, the following assets should be controlled by a cloud provider in a PaaS setup:

• Operating system
• Hardware
• Network infrastructure
• Instance resources

The cloud consumer is not responsible for identifying these assets.

**IaaS assets**
The assets the cloud consumer needs to identify are those he can control: The operating systems, network equipment, and deployed applications at the virtual machine level. The consumer can scale the number of instance resources and virtual servers or blocks of storage area up or down.

The cloud consumer cannot control the infrastructure and the underlying components. The provider needs to identify those assets.

**Step 2. Analyze risks**

A risk is the loss potential or probability that a threat will exploit vulnerabilities of a cloud service. If no cost-effective countermeasures are in place, the cloud service is susceptible to vulnerabilities that could launch a threat if exploited.

The loss potential of risks to the assets depends on the impacts of a risk to each asset (that is, between none or zero for documentation assets that are always available to users and a high rating of 0.96 for instance resource assets in the cloud environment with no adequate countermeasures). The loss potential of risks to the assets also depends how frequent the threat can take place in one-year time frame.

**How vulnerabilities can be exploited**
Let's take a look at a simple example of how the following vulnerabilities can be collectively exploited by a hacker to launch an attack against the assets of instance resources. The vulnerabilities are:
• Threshold module missing from the application
• Residual data inside instance resources
• Insufficient network-based controls in virtualized networks
• Inadequate privileged user monitoring

A good application is divided into modules that interact with one another to perform a task or a sequence of tasks; this makes it easier for a developer to add a module to the application by reusing existing module or adding new ones. When an application is missing a threshold module — set below the maximum capacity of instance resources and another level for data requests — the consumer and provider have no way of knowing if instance resources or data requests have reached the maximum capacity. They do not know if the hacker has created the malicious virtual machine on the same physical server that houses healthy virtual machines until it is too late (for example, until after a denial of service attack occurs). The hacker accomplishes this by flooding the malicious virtual machine’s neighbors with malicious instance resources and malicious data request queues. He lures the victim to increase the number of virtual machines until they reached the maximum capacity of the physical server.

Residual data occurs when instance resources previously allocated are not purged completely of the data before they are re-allocated to the same or different user. Instance resources include memory, cache, process, sessions, thresholds, and storage resources. A hacker looks for inside instance resources to get a victim's personal information.

Insufficient network-based controls in virtualized networks occur when security controls that work on network level may not work in an IaaS network infrastructure. This limits authorized administrator access to the infrastructure. A hacker takes advantage of the fact that the IaaS administrator cannot apply standard controls such as IP-based network zoning in virtualized networks. IaaS providers may not allow network-based vulnerability scanning because they have no way of distinguishing friendly network scans from attack activity. There an also be insufficient controls to distinguish traffic on real networks from virtualized networks (for example, communication between two or more virtual machines on top of the hypervisor on the same server).

Inadequate privileged user monitoring occurs when the provider inadequately monitors malicious activities by a hacker who has gained access to virtual machines from the hypervisor in the guise of a privileged user with administrative access controls. As an example, a hacker with this access can create malicious instance resources and queues of data requests without the provider noticing what the hacker is doing. Another example is maliciously reassigning instance resources from a healthy instance resource from one virtual machine as malicious instance resources to another virtual machine.

A potential ranking of the seriousness of exploits
Of course, you have to develop your own system or ranking loss potential of the different types of exploits, but I rank the loss potential of various exploits in the following order of priority:

• How a hacker can get in
• What he is looking for
• What tools he has

For example, a hacker can enter in the guise of a privileged user with administrative access controls and perform malicious activities that a legitimate system administrator did not initially notice. The hacker can also get in by sending SQL injections to find file names and can look for residual data in those files.

Once he is inside a virtual machine, he can use a hacker's tool to launch malicious network scanning attack activity in the guise of friendly network scans. The attack activity can include listing of modules within each application. If the hacker discovers this application does not contain threshold modules, he can use or create a tool to create instance resources until they reach the maximum capacity.

Step 3. Apply security countermeasures

The next step in risk assessment is relatively easy in concept and, like so many things, a bit more difficult in real life — to find out if countermeasures to mitigate risks are cost-effective so that benefits are higher than the costs of implementing countermeasures. The probability of the risks that threats will exploit vulnerabilities are lowered and ROI is increased.

This next point is important: If a countermeasure is found not to be cost-effective, the residual risks remain and these risks cannot be mitigated. You need to learn to live with them and spend no more money on them. This is one of the hardest concepts to embrace in risk assessment/mitigation: That some risks are too costly to mitigate for the benefits it provides.

However, if there are too many residual risks and too few cost-effective countermeasures, you should repeat the steps of risk assessment for several reasons:

• If this is one of your first attempts at risk assessment/mitigation, you might want to repeat the exercise a few times to sharpen your skills at identifying the assets, analyzing and understanding the risks, and determining the full breadth and depth of potential countermeasures and the various ways they can be applied.
• You also want to keep your eye out for new countermeasures and cloud infrastructure technologies that bring more benefits than they cost.
• Alternatively, you should consider buying insurance to transfer some residual risks if it is cheaper than implementing a countermeasure.

Some countermeasure examples that I've mentioned in this article include:

• Ensuring instance resource, user, and data request threshold policies are in place.
• Purging residual data from instance resources before they are re-allocated.
• Implementing plans for failover mechanisms, business continuity, and disaster recovery.
• Monitoring privileged users; checking the background and logging activities of these users and the health of physical monitoring servers, networks, and other components of the infrastructure.
• Educating consumers and providers on the benefits of risk mitigation and countermeasures.
Step 4. Conduct post-evaluations

While risk assessment should be done periodically every three years, risks may need to be reassessed more often if the following conditions occur:

- New cloud service technologies arise that can impact software, hardware, and network assets.
- New vulnerabilities and new threats emerge.
- New countermeasures become available that can effectively mitigate risks previously categorized as residual.
- New risk mitigation approach is conceived.
- Major impacts resulting from organizational changes (like mergers) on assets in all categories.
- Major changes in laws and compliance regulations across jurisdictions.

In fact, if you're in charge of handling risk assessment and mitigation for your organization's cloud services, you should probably check the infostream for information on these conditions about once a week. Consider establishing a newsfeed for new threats and vulnerabilities.

In conclusion

Mitigating risks to cloud services while maintaining high uptime availability requires proactive risk planning to resolve the issues of what assets to identify for each cloud type, what risks to analyze, what countermeasures are cost-effective, and what to evaluate after risks are mitigated. Your team of developers, users, and business analysts need to work together to reduce residual risks to cloud services. The team will find resolving the issues make their job of mitigating risks to cloud services much easier.
Related topics

• The author discusses threshold policy in the articles "Balance workload in a cloud environment: Use threshold policies to dynamically balance workload demands" and "Cloud computing versus grid computing: Service types, similarities and differences, and things to consider."
• The author discusses proactive vs. reactive ways of making application changes when you migrate them to the cloud in the article "Change app behavior: From in house to the cloud."
• In the developerWorks cloud developer resources, discover and share knowledge and experience of application and services developers building their projects for cloud deployment.
• More developerWorks resources that match this article can be found at SOA and web services at developerWorks and industries at developerWorks.
• See the product images available on the IBM Smart Business Development and Test on the IBM Cloud.
• The next steps: Find out how to access IBM Smart Business Development and Test on the IBM Cloud.

© Copyright IBM Corporation 2011
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)