CHAPTER

24 Virtual Machines and Cloud Computing

Gone are the days of the one-to-one relationship between a computer's operating system (OS) software and its hardware. With *virtualization,* the underlying hardware platforms no longer matter to the OS, thanks to emulators that translate instructions from the software to the machine. In a *virtual machine* (VM), the OS (referred to as a "guest OS" when virtualized) and the software applications that it hosts run on *virtual hardware*.

This creates an interesting security challenge. Most security vulnerabilities that are at risk of exploitation originate from software. In a virtualized environment, everything is software—therefore, the risks are greater. Virtual machines carry their own security risks, unique from those of standalone computer systems and local area networks.

Virtual computers aren't the only platforms based on virtualization technology. Virtual networks, which can emulate just about any router or switch fabric, and virtual storage, which can expand or contract as needed, complete the triangle. Servers, networks, and storage together, all virtualized, make up the world of cloud computing.

Virtual Machines

All of the security settings that are normally applied to Windows and Unix-based systems in the physical world, as described in Chapters 21 and 22, should also be applied to VMs as well. Furthermore, security controls for data storage (outlined in Chapter 11) should be applied to storage networks that are utilized by VMs, including proper logical unit number (LUN) zoning and masking to limit the storage that each virtual server can access.

In addition to securing the VMs themselves, additional steps are needed to secure the virtual environment as a whole. The risks associated with VMs are a superset of those associated with physical servers along with a new set of risks based on the controllability of the individual virtual machines through a centralized management platform (sometimes referred to as a *hypervisor* or *virtual machine monitor*). National Institute of Standards and Technology, or NIST, has published an excellent set of security practices for VMs in Special Publication 800-125. See the "References" section.

Protecting the Hypervisor

The hypervisor is responsible for managing all guest OS installations on a VM server, and the service console provides a centralized location for managing all the servers in a virtual environment. As a result, a compromise of the hypervisor or service console has the potential to inflict significant damage as this would effectively allow all security controls on the virtual servers to be bypassed.

Hypervisor and service console servers need to be properly patched and secured, as well as logically separated through the use of isolated networks with strict access controls. The administration interfaces should reside on a network separate from the virtual machines themselves, one that is inaccessible from all VMs and other application servers on the network. Firewalls should be used to block access attempts from the virtual machines to the management consoles. This setup prevents attacks and malware on VMs from reaching the service consoles and affecting other VMs.

Because the hypervisor has so much power, and consequent damage and abuse potential, its administrative access should be strictly controlled. Administrative access to the hypervisor is like having administrative access to all the VMs it controls.

Any supervisory account for the hypervisor needs to be controlled in the same way you would protect privileged accounts for server and network administrator use. As with those other privileged accounts, consider using alternatives to passwords. A password associated with an administrative account for the hypervisor has the potential to be shared, or written down, despite your policies, threats, and warnings. The password may also be intercepted in various ways, such as by keyloggers or network sniffers. Password secrecy can never be guaranteed. Multifactor authentication—using *tokens* (portable digital one-time password generators), biometrics, and smart cards—is a better choice for hypervisor access. Limit physical access to the hardware as well. Despite any technical defenses that are in place, an attacker with physical access to the machine hardware is going to have an easier time getting into the system. Consequently, limiting physical access to systems makes an attacker's job harder. Chapter 34 covers techniques to accomplish this.

Limiting the number of administrators and their privileges is another practice that can reduce the risks of hypervisor attacks via administrator accounts. Hypervisor administrators should not use the same privileged accounts they also use to manage VMs and other systems, owing to the greater damage potential of hypervisors.

Finally, someone other than the administrator, preferably someone with a security or audit function, should perform a periodic review of administrator activities. This check helps ensure that administrators haven't intentionally or inadvertently reduced system security level, altered the VMs, or cloned images inappropriately.

Protecting the Guest OS

Typically, the hypervisor manages access to hardware resources so that each guest OS is able to access only its own allocated resources, such as CPU, memory, and storage, but not those resources allocated to other guest OSs. This characteristic is known as *partitioning* and is designed to protect each guest OS from other guest OS instances, so attacks and malware are unable to "cross over." Partitioning also reduces the threat of *side-channel attacks* that take advantage of hardware usage characteristics to crack encryption algorithms or implementations. Partitioning, therefore, is considered an important security measure.

If an attacker attempts to "break out" of a guest OS to access the hypervisor or neighboring guest OSs, this is referred to as an *escape*. If an attacker were to escape his or her guest OS and access the hypervisor, the attacker could potentially take over all of the hypervisor's guest OSs.

The hypervisor monitors and tracks the state of its guest OSs, which is a function commonly referred to as *introspection*. Introspection can be integrated with intrusion detection systems (IDS) or intrusion prevention systems (IPS) and security information and event management (SIEM), which are described in Chapter 18, to identify and alert when escape attempts occur.

Protecting Virtual Storage

Guest OS systems can utilize virtual or physical network attached storage (NAS) and storage area networks (SAN) allocated by the hypervisor to meet data storage requirements, as if these storage devices were directly attached to the system. This aspect of security for virtualization is focused on controlling access to the files on the virtual hard drive and the overall configuration of the storage network, which should be done as described in Chapter 11.

Protecting Virtual Networks

Through the hypervisor, virtual machines can also utilize virtualized network environments in the same manner as physical network environments. The hypervisor can present the guest OS with either physical or virtual network interfaces. Typically, hypervisors provide three choices for network configurations:

- **Network bridging** The guest OS has direct access to the actual physical network interface cards (NIC) of the real server hardware.
- **Network Address Translation (NAT)** The guest OS has virtual access to a simulated physical NIC that is connected to a NAT emulator by the hypervisor. As in a traditional NAT, all outbound network traffic is sent through the virtual NIC to the underlying subsystem to get routed to the main network, or directly to other guest OSs.
- **Host-only networking** A guest OS has virtual access to a virtual NIC that does not actually route to any physical NIC. Network packets are translated by the hypervisor from one guest OS to another without any physical network connectivity. Many network protocols can be simulated using hypervisor virtualization software.

Security devices, such as IDSs or IPSs, can monitor and control network traffic using network bridging and NAT and, to a lesser extent, host-only networking. In the case of host-only networking, introspection can be used to compensate for this lack of visibility.

Regardless of the network configuration, in any environment, networks should be segmented using the best practices defined in Chapter 13.

NIST Special Publication 800-125

NIST Special Publication 800-125 contains detailed recommendations for designing and securing virtual environments to protect the hypervisor, guest OS, virtual storage, and virtual networks. Review of this publication is highly recommended for any VM administrator and virtualization architect.

Cloud Computing

Cloud computing provides a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. It encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends existing IT capabilities.

Cloud computing services are gaining in popularity among businesses that want to save money and improve the efficiency of their computing resource consumption. Although there are substantial benefits to be gained from cloud computing, a number of significant security challenges need to be addressed. For example, all of the major cloud service providers have experienced full service outages, performance issues, and various types of security breaches.

Cloud computing is attractive to small businesses and startup companies that don't have many options for establishing basic computing infrastructure in a fast and cost-effective manner. Implementing a cloud environment may be the only option for a small startup company that doesn't gain much value from equipment ownership. For established businesses, moving services and data to the cloud should be considered on the basis of value versus risk. For high-risk situations, moving services and data to the cloud may not provide sufficient benefits to outweigh the costs associated with the risks. Even for low-risk situations where cloud computing is an attractive choice, continued hosting of specific services and data in-house, for example, to meet regulatory compliance requirements, will be necessary.

Similar to early adoption of Internet services, cloud computing offers cost savings at reduced reliability and security levels. Cloud providers are well-suited for large file-size content, with lots of read access, such as digital content and streaming media, video, and music, as well as for long-term file storage, such as data backups and data archives. All data stored in the cloud is geared toward providing access to geographically distributed and distinct areas. Experts recommend that applications that are inessential to the business or ones that cannot be delivered cost effectively by internal IT departments are well suited to cloud architectures. Video and audio conferencing, collaboration tools, and sales force automation are cited as good examples of services that can be successfully migrated to, or implemented in, a cloud.

When preparing to use cloud services, carefully consider the specific risks associated with operating within a cloud environment. Mission-critical services require extensive thought and planning, particularly around redundancy and the risks associated with service outages. Sensitive data is a more difficult problem that requires additional thought and investigation to provide a suitable work around. Cloud providers offer logical data separation for their customers, but when it comes to knowing exactly where your data is, and protecting it from theft or disclosure, few options are available. The preferred option is to keep your private or sensitive data on your own private network, applying classic security controls to that data to mitigate some of the risk.

Before selecting any cloud computing vendor, perform a vendor security review, and ensure contract language is carefully worded to protect the customer. Select vendors based on their willingness to comply with customer requirements and their dedication to protecting customer information and environments as well as their previous track record in providing cloud services.

Types of Cloud Services

The term "cloud" is thrown around a lot these days, and it's used pretty loosely. Everybody wants to get in on the cloud phenomenon, so there are many types of services that get branded as cloud services. The following are the most common types of services with which we find the term "cloud" associated.

- **Infrastructure-as-a-Service (IaaS)** This type of service allows consumers to provision processing, storage, and networking resources, allowing them to deploy and run their own operating systems or applications in their own cloud environment.
- **Software-as-a-Service (SaaS)** This type of cloud computing delivers a single application through the browser to customers using a multitenant architecture.
- **Utility computing** Companies that offer storage and virtual servers that IT can access on demand. Early enterprise adopters mainly use utility computing for supplemental, non-mission-critical needs, but it is envisaged that one day it may replace parts of the data center.
- **Platform-as-a-Service (PaaS)** This form of cloud computing delivers development environments as a service. You build your own applications that run on the provider's infrastructure and are delivered to your users via the Internet from the provider's servers.
- **Web services in the Cloud** Web service providers offer APIs that enable developers to exploit functionality over the Internet, rather than delivering full-blown applications.
- **Managed service providers (MSP)** One of the oldest forms of cloud computing, a managed service is basically an application exposed to IT rather than to end users. Examples include virus scanning services, e-mail spam filtering services, application monitoring services, and managed security services.
- **Service commerce platforms** Similar to an automated service bureau and most common in trading environments, a service commerce platform is a service hub that users interact with, such as an expense management system, to order travel or secretarial services from a common platform that then coordinates the service delivery and pricing within the specifications set by the user.
- **Internet integration** The integration of cloud-based services mainly serving SaaS providers using in-the-cloud integration technology.

Cloud Computing Security Benefits

On the positive side, cloud computing can provide a higher level of security than traditional distributed client-server computing environments. A well-designed cloud computing infrastructure offers redundancy, transport security, more comprehensive and centralized authentication, as well as better physical and operational security controls.

Additionally, cloud computing providers can offer specific security services at a lower cost and with more consistency than organizations can do on their own. Some of these services include

- **Centralized data** Data leakage through laptop data loss and backup tape loss could conceivably be reduced by cloud computing using thin client technology.
- **Monitoring** Centralized storage is easier to control and monitor.
- **Forensics and incident response** With IaaS providers, a dedicated forensic server can be built in the same cloud as the corporate servers but placed offline, ready to be used and brought online as required. It can also reduce evidence acquisition time, allowing immediate analysis of compromised servers. In addition, servers can now be cloned and the cloned disks instantly made available to the Cloud forensics server.
- **Password assurance testing** For organizations that routinely crack passwords to check for weaknesses, password cracking times can be significantly decreased.
- **Logging** Effectively unlimited storage for logging, with reduced concerns about insufficient disk space being allocated for system logging.
- **Testing security changes** Vendor updates and patches, as well as configuration changes for security purposes, can be applied using a cloned copy of the production server, with low-cost impact testing and reduced startup time.
- **Security infrastructure** SaaS providers that offer security technologies to customers share the costs of those technologies among their customers who use them.

Security Considerations

When evaluating the need for cloud computing services, you should consider private data and public data separately. Private data, such as client information, requires stricter security controls than public data that is intended to be shared with a larger Internet audience. Organizations should make a slow transition to cloud computing rather than trying to push everything into the cloud at one time. The focus should be on addressing one, or a few, key business pain points or opportunities for which cloud computing is appropriate. Cloud computing is well suited to standardized applications because one of its key benefits is standardization. Customization should be limited to simplifying deployments and optimizing the long-term benefits of cloud computing. Organizations that are currently leveraging cloud computing to streamline their business processes and systems so they can minimize the amount of integration needed to use cloud platforms are realizing the greatest benefits today.

Performance is another important factor to consider. Public clouds are accessed over the Internet and face the bandwidth limitations provisioned by their respective Internet service providers. Scaling to larger Internet bandwidths can significantly increase the overall ownership cost of cloud solutions. Carefully consider time- or bandwidth-dependent services before they become candidates for cloud migration; they should be stress-tested as part of a proof of concept (POC) evaluation.

Review the potential cost savings of cloud environments. Although service providers are currently pricing their services attractively, that may change. Data proliferation within the cloud will cause costs to rise continually. Cloud vendors introduce their services with very low, attractive pricing; however, experience with service providers has shown that costs can

increase over time beyond the point where outsourcing is more cost effective than insourcing. While this is not necessarily a security issue, it is an important point to keep in mind.

Cloud computing also raises some additional concerns that need to be addressed, beyond those of traditional data centers. For instance, knowing and controlling the location of data is important for many reasons, not the least of which is regulatory. In traditional MSP and ASP models, the location of customer data is known, owing to individual servers being physically housed in specific data centers with minimal interaction from service providers. In contrast, cloud service providers have many data centers and leverage virtualization of servers, network, and storage to provide elastic environments that can be scaled on demand. Finding the physical location of data can be very difficult as it can move around without warning. For example, VMware has a feature called Distributed Resource Scheduler, which continuously monitors utilization across guest OSs and allocates available resources among virtual machines, providing capacity expansion by automatically migrating live virtual machines to different physical servers. If those physical servers are located in different geographic locations, particularly if these locations are outside of the United States and in risky locales, the location of data can become a concern. Ensuring the integrity and confidentiality of data when the cloud infrastructure physically resides in another country, especially those hostile to the U.S. can be difficult, if not impossible.

For sensitive and private data, colocation is also a concern. Cloud computing providers typically store data from multiple customers on the same hardware infrastructure, stating that suitable controls are in place to provide logical separation of data for different customers; however, you may not be able to validate whether a competitor is able to access your data, either intentionally or accidentally. Some vendors do not provide traditional data backup services, and colocation of data on shared media in cloud environments where backups are performed can also be a concern, especially in situations where you would like to terminate your contract with the cloud provider.

Any sensitive or confidential information placed into a cloud environment should be protected beyond the security features of the cloud service itself (which typically include such features as role-based access controls and firewalls). The level of protection should be determined by the sensitivity and value of the data itself. At a minimum, sensitive data in the cloud should be encrypted—and advanced data protection techniques such as Information Rights Management (described in Chapter 9) may be called for, depending on your assessment of the data's risk. Avoid putting highly secret data into the cloud (such as high-value intellectual property, trade secrets, and legally risky personal and financial information) if the risk of exposure is greater than the cost savings and value of the cloud service.

Figure 24-1 provides a graphical representation of the key challenges and issues that IT professionals consider to be most relevant to cloud services. Security, availability, and performance are the top three concerns. Any organization considering cloud services should consider mitigating these risks with the security controls described in the following sections.

A report from Pew Internet and American Life Project indicates that cloud computing applications, such as web-based e-mail and other web applications, are raising new privacy concerns. The report *Use of Cloud Computing: Applications and Services* found that 69 percent of online Americans use webmail services, store data online, or use software programs such as word processing applications whose functionality is located on the Web. At the same time, "users report high levels of concern when presented with scenarios in which companies may put their data to uses of which they may not be aware." For example, 90 percent of respondents said that they "would be very concerned if the company that they use to store

Figure 24-1 IDC survey of 244 IT professionals about their views of cloud services

their data was sold it to another party," 80 percent of respondents said "they would be very concerned if companies used their photos or other data in marketing campaigns," and 68 percent of "users of at least one of the six cloud applications say they would be very concerned if companies who provided these services analyzed their information and then displayed ads to them based on their actions."

Figure 24-2 shows what some organizations are doing about these risks.

Cloud Computing Risks and Remediations

Bringing together the data center and the cloud raises important issues and concerns common to both environments that must be addressed:

- **Availability** Cloud services can be thought of as being comparable to the Internet itself. On the Internet, availability issues are managed by using redundant service providers so a failure at one provider will not result in a loss of service. A common approach is to assume that the service will eventually fail and to plan accordingly. Continuity becomes important in this scenario. SLAs are published by the cloud providers and are their responsibility. Remediation is typically a cash refund or payment prorated based on the cost of the service, not the cost of losses due to business downtime. These SLAs are also affected by Internet reliability—if a customer's or provider's Internet link goes down, accessing data is impossible and there is no remediation.
- **Data persistence** What happens to data when it is deleted from the cloud?
- **Patriot Act ramifications** The U.S. government has the right to monitor and capture all traffic from a service provider on demand. If a service provider is subpoenaed for data under its control, the provider must comply regardless of the customer's knowledge or objections.
- **Compliance ramifications** Some government regulations do not allow cloud computing.
- **PCI compliance** Requires that you know and can demonstrate exactly where and on what physical server your data resides.

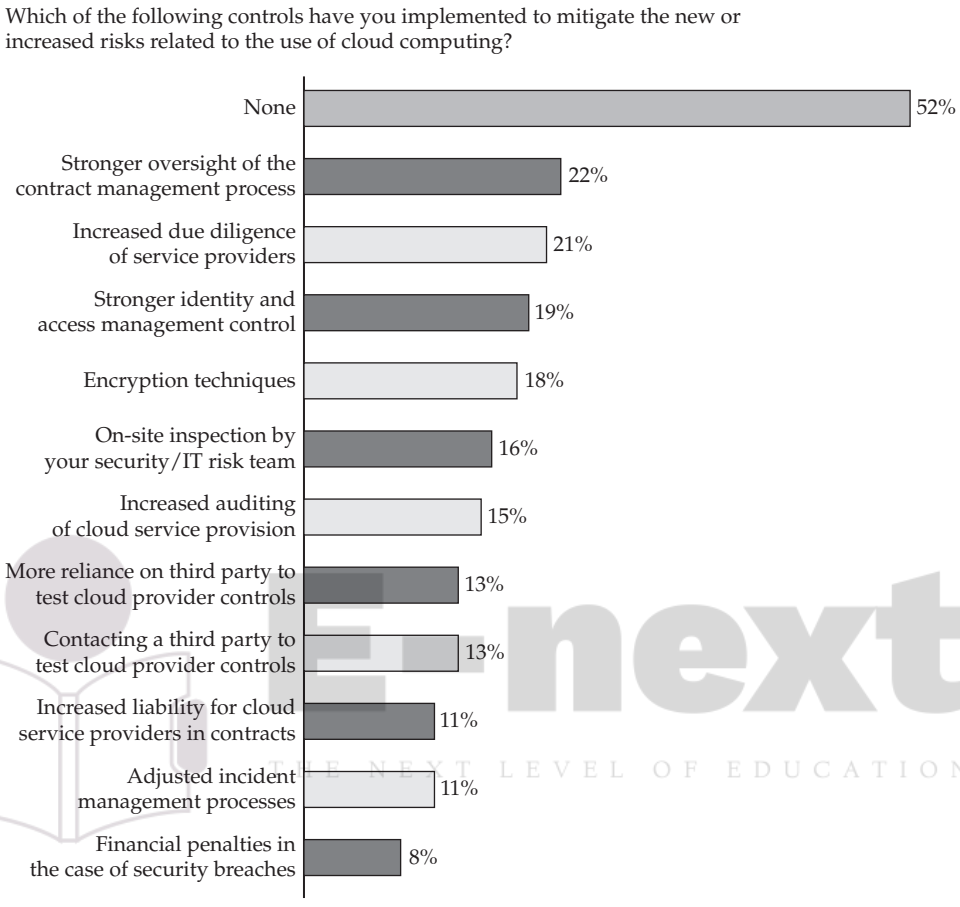

Figure 24-2 E&Y survey of controls used to mitigate cloud security risks

- **Migration** You may need physical-to-cloud and cloud-to-physical capability to move data into the cloud from your local computing environment, or vice versa.
- **Confidentiality** The responsibility for controlling data in a cloud environment is shared between the cloud provider and the customer. Isolating data is only as effective as the virtualization technologies used to build the cloud and the controls and practices implemented by the providers. Any data that an organization is concerned about keeping private should be housed in a private network or private cloud, not in a public cloud.

Cloud Computing Security Incidents

There are a few web sites, typically run by security professionals, that keep track of incidents and events that impact cloud computing providers, such as outages, security issues, and breaches. The information they track helps form a picture of the real-world risks associated with cloud services.

Table 24-1 shows a sample of security incidents that occurred in cloud services, tracked by the Cloud Computing Incidents Database (CCID). Note that a significant number of incidents in this table relate to service outages; therefore, service availability needs to be carefully considered when designing a cloud solution. If the service is mission-critical, you need to consider how to compensate for reliability problems.

These examples are helpful in forming an overall picture of the types of incidents common to cloud services, their severity, and their extent. Table 24-2 shows some data from cloutage.org, an Open Security Foundation service that tracks cloud incidents.

Provider	Incident Type	Incident Subtype	Affected	Notes
Google	Outage	502 error	Unknown number of users	Lasted more than 24 hours
Google	Security	Session hijacking	Some Thai users	Limited to ISP(s) in Thailand
Google	Outage	Performance degradation	All	Datastore writes experienced elevated latencies and error-rates.
Google	Security	User impersonation	All SSO users	Malicious service provider could impersonate a user at other service providers.
FlexiScale	Outage	Disaster recovery	All	Full extended outage
Google	Outage	Change management	Many	Users unable to use web mail due to issues with loading contacts between 14:00 and 16:00 PT.
Nirvanix MediaMax	Data loss	Closure	20,000	Data claimed to be safe but inaccessible.
AWS	Outage	Design fault	All	Full outage for eight (weekend) hours.
Apple	Outage	Migration	All	Scheduled outage window exceeded during upgrade to MobileMe
Apple	Outage	Scheduled outage	All	Full outage (except mail) during upgrade to MobileMe 18:00–00:00
Amazon	Outage	Degraded performance	Small subset of instances	Result of a customer creating a large number of firewall rules and instances.
AWS	Outage	Authentication failures	All	Early morning outage (04:31–06:48 PST) caused by authentication service overload.

Table 24-1 Known Cloud Computing Security Incidents (from CCID)

Date reported	Provider	Service	Incident type	Summary
1/30/2009	Ma.gnolia	Ma.gnolia	Data loss	Ma.gnolia suffers major data loss, data gone for good
3/13/2009	Microsoft Corporation	Sidekick	Data loss	Microsoft Sidekick outage left customers without access to service and lost data
4/28/2010	Paychex, Inc.	Payroll 401(k) and Employee Benefits	Data loss	Payroll and 401k servicing company erroneously merges account data of two businesses
8/9/2010	Evernote Corporation	Evernote	Data loss	A small percentage of Evernote users' data lost
11/1/2010	DreamHost	Web Hosting	Denial of Service	DreamHost Cardiff distributed denial of service attack
11/4/2010	Intuit.com	Web Hosting	Denial of Service	www.websites.intuit.com denial of service attack
11/17/2010	Sitelutions	DNS	Denial of Service	Sitelutions suffers distributed denial of service attack
1/21/2011	Whirlpool	Forum	Denial of Service	Whirlpool Forum hit with distributed denial of service attack
2/28/2011	Google, Inc.	Gmail	Data loss	Google deletes users' messages
3/18/2011	Heroku	Cloud Hosting	Outage	Network connectivity issues cause increased errors on Heroku
3/21/2011	Heroku	Cloud Hosting	Outage	Heroku new relic deployment notification outage
3/23/2011	Netflix	Netflix Streaming	Outage	Netflix streaming and web site down
3/24/2011	Expedia	TripAdvisor	Attack	TripAdvisor member data stolen in possible SQL injection attack
3/25/2011	Twitter, Inc.	Twitter	Outage	Twitter experiences delays in delivering to Facebook and SMS
3/25/2011	Heroku	Cloud Hosting	Outage	Heroku users experience HTTP 503 errors
3/25/2011	Twitter, Inc.	Twitter	Outage	Twitter experiences tweet delivery delay
3/25/2011	Heroku	Cloud Hosting	Outage	Heroku shared database experienced hardware failure
3/25/2011	Heroku	Cloud Hosting	Outage	Heroku users unable to provision new dedicated databases

(continued)

Table 24-2 Known Cloud Computing Security Incidents (from Open Security Foundation/Cloutage.org)

Date reported	Provider	Service	Incident type	Summary
4/21/2011	Amazon Web Services	Amazon Elastic Compute Cloud (Amazon EC2)	Outage	Companies lost service because of server problems in the Amazon data center
4/21/2011	Sony	PlayStation Network	Outage	PlayStation Network outages
1/21/2012	DreamHost	Web Hosting	Attack	DreamHost database hack forces mass password reset

Table 24-2 Known Cloud Computing Security Incidents (from Open Security Foundation/Cloutage.org) *(continued)*

Looking at just this data alone, you can see that the majority of incidents are outages. This observation is important because it means organizations that are considering cloud solutions should think about how to mitigate the impact of service unavailability. The other two categories—data loss and attacks—are more rare, but potentially more significant. What is the impact if your organization's data is exposed due to accidental or intentional issues, or when you lose your data and can't get it back? Figure 24-3 shows the breakdown of cloud incidents by type, based on a couple of sources. This breakdown is representative of the overall experience of cloud-related incidents.

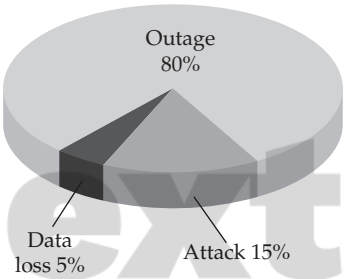

Figure 24-3 Breakdown of cloud security incident types

In the next section, we discuss these and other risks, and provide some recommended remediations for "working around" potential problems.

Cloud Security Technologies

Cloud computing providers offer several security services to remediate some of the risks inherent to the cloud environment. You should carefully consider which controls will offset the risks in your particular scenario. Controls used include

- Communication encryption
- File-system encryption
- Auditing
- Traditional network firewalls
- Application firewalls
- Content filtering
- Intrusion detection
- Geographic diversity

Vendor Security Review

Perform a third-party vendor security review to validate the security practices of cloud computing providers that you are considering. Examples of vendor attributes to review include

- Physical security
- Backups and/or data protection
- Administrator access
- Firewalls
- Hypervisor security
- Customer and instance isolation
- Intrusion detection and anomaly monitoring
- Data transmission security
- Data storage security

Risk and Remediation Analysis

The risks associated with cloud computing—the "convergence" of data center and Internet architectures—include the set of risks associated with traditional data centers combined with those of Internet-based services, added to a new set of risks that arise from the convergence of private and public environments.

The following categories of risks are divided according to the classic "CIA" triad of Confidentiality, Integrity, and Availability—the concepts that information security professionals are tasked with protecting. Within each identified risk, where possible, we attempt to apply security controls consistent with the three *D*s of security—Defense, Detection, and Deterrence—in an effort to mitigate risks using the principle of layered security (also known as defense-in-depth).

Confidentiality Risks These risks are associated with vulnerabilities and threats pertaining to the privacy and control of information, given that you want to make the information available in a controlled fashion to only those entities that need it, without exposing it to unauthorized parties.

Data leakage, theft, exposure, forwarding The loss of information such as customer data and other types of intellectual property through intentional or unintentional means. There are four major threat vectors for data leakage: theft by outsiders, malicious sabotage by insiders (including unauthorized data printing, copying, or forwarding), inadvertent misuse by authorized users and mistakes created by unclear policies.

Defense: Employ software controls to block inappropriate data access through a data loss prevention (DLP) solution. Avoid placing sensitive, confidential, or personally identifiable (PII) information in the cloud.

Detection: Use water-marking and data classification labeling along with monitoring software to track data flows.

Deterrence: Establish clear and strong language in contractual agreements with service providers that specifies how data privacy will be enforced and maintained.

Residual risk: Data persistence within the cloud vendor environment in relation to multiple untraceable logical disk storage locations and vendor administrative access that exposes private data to administrators.

Espionage, packet sniffing, packet replay The unauthorized interception of network traffic for the purpose of gaining information intentionally, using tools to capture network packets or tools to reproduce traffic and data that was previously sent on a network.

Defense: Encrypt data at rest as well as data in transit through the use of strong encryption technologies for file encryption (e.g., PGP), as well as network encryption between servers and over the Internet (e.g., TLS, SSL, SFTP). Preference should be given to cloud providers that offer link-layer data encryption.

Detection: Not much can be done today to find out when somebody has intercepted your data; however, an IDS capability can help to identify anomalous behavior on the network that may indicate unauthorized access attempts.

Deterrence: Transfer the risk of unauthorized access to the service provider using specific contract language.

Residual risk: Data can be stolen from the network through tools that take advantage of network topologies, network weaknesses, compromised servers and network equipment, and direct access to network devices.

Inappropriate administrator access Using privilege access privileges levels generally reserved for system administrators that provide full access to a system and all data that system has access to, in order to view data or make changes without going through the system's authorization processes. Administrators have the capability of bypassing all security controls, and this can be used to intentionally or mistakenly compromise private data.

Defense: Minimize the number of service provider administrators for each cloud service function—server, network, and storage (definitely fewer than ten administrators and preferably fewer than five administrators). Also ensure that a thorough background check is performed to screen service provider personnel. Perform a vendor security review to validate these practices before engaging or signing with a cloud vendor.

Detection: Review the cloud provider's administrative access logs for their internal infrastructure on a monthly or quarterly basis. Review the provider's list of administrators on a biannual basis.

Deterrence: Select only those cloud providers that can demonstrate robust system and network administration practices that are also willing to agree with customer conditions.

Residual risk: Because administrators have full control, there is a possibility that they will intentionally or accidentally abuse their access privileges, resulting in the compromise of personal information or service availability.

Storage persistence Data may remain on a hard drive long after it is no longer required and also potentially after it has been deleted. As this data may be deleted but not strongly overwritten, it is at an increased risk of future data recovery by unauthorized individuals.

Defense: Insist that vendors maintain a program that includes Department of Defense (DoD) disk wiping when disks are replaced or reallocated. Dead disks should be degaussed or destroyed to prevent data disclosure.

Detection: You can't do much to find out when your data persists on a disk that has been taken offline.

Deterrence: Establish disk wiping practices before selecting a vendor and ensure that contract language clearly establishes these requirements.

Residual risk: Data can remain on physical media long after it has been deleted.

Storage platform attacks Direct attacks against a SAN or storage infrastructure, including the use of a storage system's management control, can provide access to private data, bypassing the controls built into an operating system because the operating system is out of the loop.

Defense: Ensure that vendors have implemented strong compartmentalization and role-based access control on their storage systems and that access to the management interface of vendor storage systems is not accessible via the customer network.

Detection: Implement IDS for the storage network and review storage system access control logs on a quarterly basis.

Deterrence: Ensure that the cloud service provider has strong legal representation and a commitment to identifying and prosecuting attackers.

Residual risk: Data can be stolen directly from the SAN and you may find out about it after the fact or not at all.

Misuse of data People who are authorized to access data also have the opportunity to do anything with that data, including actions that they are not permitted to perform. Examples include employees who leak information to competitors, developers who perform testing with production data, and people who take data out of the controlled environment of the organization's private network into their unprotected home environment.

Defense: For employees, use security controls similar to those in private data networks, such as DLP, role-based access controls, and scrambling of test and development data. Block the ability to send e-mail attachments to external e-mail addresses.

Detection: Use water-marking and data classification labeling along with monitoring software to track data flows.

Deterrence: Use a security awareness program along with penalties and sanctions to deter people from transferring data from a controlled environment to an uncontrolled environment.

Residual risk: People can find ways around controls to put data into uncontrolled environments where it can be stolen or misused.

Fraud Illegally (or deceptively) gaining access to information that a person is not authorized to access. Fraud can be perpetrated by outsiders but is usually performed by trusted employees.

Defense: Use checks and balances along with sufficient separation of duties to reduce the dependence on single individuals. Ensure that business processes include management reviews and approvals.

Detection: Perform regular audits on computing system access and data usage with special attention to unauthorized access.

Deterrence: For employees, ensure that there is a suitable penalty process. For service providers, transfer risks through the use of contractual language.

Residual risk: Fraudulent practices can result in significant reputation and financial damages.

Hijacking The exploitation of a valid computer session—sometimes also called a *session key*—to gain unauthorized access to information or services in a computer system, in particular, the theft of a magic cookie used to authenticate a user to a remote server. For example, the HTTP cookies used to maintain a session on many web sites can be stolen using an intermediary computer or with access to the saved cookies on the victim's computer. If an attacker is able to steal this cookie, the attacker can make requests as if he or she is the genuine user, gaining access to privileged information or changing data. If this cookie is a persistent cookie, then the impersonation can continue for a considerable period of time. Any protocol in which state is maintained using a key passed between two parties is vulnerable, especially if it's not encrypted. This also applies to the cloud environment's management credentials; if the entire cloud service is managed using session keys, the entire environment can be taken over through the effective use of a session hijacking attack.

Defense: Look for solid identity management implementations from service providers that specifically address this risk using strong, nonguessable session keys with encryption. Use good key management processes and practices and key escrow and key recovery practices as a customer so employee departures do not result in the inability to manage your service.

Detection: Routinely monitor logs for access to cloud resources and their management interface to identify unexpected behavior.

Deterrence: Not much can be done to deter attackers from hijacking sessions outside of aggressive legal response.

Residual risk: Attackers can impersonate valid users of cloud services or even use administrative credentials to lock you out or damage your entire infrastructure.

Integrity Risks These risks affect the validity of information and the assurance that the information is correct. Some government regulations are particularly concerned with

ensuring that data is accurate. If information can be changed without warning, authorization, or an audit trail, its integrity cannot be guaranteed.

Malfunctions Computer and storage failures that can cause data corruption.

Defense: Make sure the service provider you select has appropriate RAID redundancy built into its storage network and that creating archives of important data is part of the service.

Detection: Employ integrity verification software that uses checksums or other means of data verification.

Deterrence: Owing to the nature of the data and the fact that there is no human interaction, little can be accomplished.

Residual risk: Technology failures that damage data may result in operational or compliance risks (especially Sarbanes-Oxley).

Data deletion and data loss Accidental or intentional destruction of any data, including financial, company, personal, and audit trail information. Destruction of data owing to computer system failures or mishandling.

Defense: In the cloud environment, ensure that your critical data is redundantly stored and housed with more than one cloud service provider.

Detection: Maintain and review audit logs that relate to data deletion.

Deterrence: Maintain education and awareness programs for individuals who access and manage data. Ensure that appropriate data owners are assigned who have full authority and control over data.

Residual risk: Once critical data is gone, if it can't be restored it is gone forever.

Data corruption and data tampering Changes to data caused by malfunction in computer or storage systems, or by malicious individuals or malware. Modification of data with intent to defraud.

Defense: Utilize version control software to maintain archive copies of important data before it is modified. Cloud services offer virtually unlimited data storage, meaning you can keep virtually unlimited copies of prior versions. Ensure that all virtual servers are protected by antivirus (AV) software. Maintain role-based access control for all data based on the principle of least privilege and the role or job function based on the need-to-know principle.

Detection: Use integrity-checking software to monitor and report on any alteration of key data.

Deterrence: Maintain education and awareness programs for individuals who access and manage data. Ensure that suitable data owners are assigned who have authority and control over data.

Residual risk: Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

Accidental modification Perhaps the most common cause of data integrity loss, changes made to data either because the individual thought he or she was modifying something else or because of incorrect input.

Defense: Utilize version control software to maintain archived copies of important data before it is modified. Cloud services offer virtually unlimited data storage; therefore, you can store and maintain virtually unlimited copies of prior versions. Ensure that all virtual servers are protected by AV software. Maintain role-based access control to all data based on the least privilege principle, pursuant to job function and need to know.

Detection: Use integrity-checking software to monitor and report on alterations to key data.

Deterrence: Maintain education and awareness programs for individuals who access and manage data. Ensure that appropriate data owners are assigned who have full authority and control over data.

Residual risk: Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

Phishing Often perpetrated through e-mail, the act of tricking a victim into giving out personal information is a common tactic of "social engineering." For example, sending out an e-mail that looks like it came from a legitimate company that directs a user to log in and provide credit card information.

Defense: Employ anti-phishing technologies to block rogue web sites and detect false URLs. Use multifactor authentication for customer-facing systems to ensure that users are aware when they are redirected to fake copies of your web sites. Send periodic informational updates and educational materials to customers explaining how the system works and how to avoid phishing. Never send e-mails to customers that include or request personal details, including customer IDs or passwords.

Detection: Use an application firewall to detect when remote sites are trying to copy or emulate your web site.

Deterrence: Maintain education and awareness programs for individuals who use and store personal information about employees or customers.

Residual risk: Significant reputation risk owing to exposure in the public media or allegations of personal data loss commensurate with the business risks of losing backup tapes or a compromise of a database containing customer information. Bad publicity can lead to both long- and short-term loss of corporate reputation.

Availability Risks These risks are associated with vulnerabilities and threats pertaining to the reliability of services, given the need to use services reliably with low risk and incidence of outage.

Denial of service A denial of service (DoS) attack or distributed denial of service (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. It frequently involves saturating a target machine with many communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. Cloud services can be especially vulnerable to volumetric DDoS attacks, in which large numbers of computers flood the cloud networks and servers with more data than they

can handle, causing them to grind to a halt. Application-based DDoS attacks against cloud services are also particularly effective when they target specific applications (like web servers or databases) within the cloud infrastructure. In addition, distributed reflection denial of service (DRDoS) attacks, which are more "efficient" in that they cause victim systems to retransmit the packets used to flood the network, work well in cloud environments. Cloud providers are targeted specifically by attackers who want to take out more infrastructure in a single attack than can be done by attacking individual organizations or computers, especially if the providers have well-known names that bring "glory" to the attackers or are subject to the vengeance of hactivists or hacking groups.

Defense: Select a service provider that has solid protection against network-based attacks. Implement firewalls and network filtering at the network perimeter of the cloud infrastructure (primarily the Internet access point) to block attacks and hostile networks using a network blacklist. In addition, use redundant providers because an attack against one provider's environment may not affect another.

Detection: Select a service provider that performs and monitors intrusion detection on a 24×7 basis and sign up for any appropriate additional services relating to this capability.

Deterrence: Work with the service provider's legal department to ensure that attackers are found and prosecuted.

Residual risk: As most DoS attacks originate from other countries and can be hard to detect and track, there is little that you can do about the ones that get through an environment's defenses.

Outage Any unexpected downtime or unreachability of a computer system or network.

Defense: The primary defense against any service outage is redundancy. Ensure that environments can be automatically switched to a different provider during an outage. Additionally, employ a solid disaster recovery plan to be ready for extended outages.

Detection: Employ monitoring tools to monitor the availability and response time of the cloud environment continuously.

Deterrence: Outages are expensive. Calculate the cost of downtime and make sure the contract with the service provider allows compensation for real costs incurred, not just remuneration for the cost of the service itself.

Residual risk: Because outages generally occur because of software problems, little can be done to stop them from happening.

Instability and application failure Loss of functionality or failure of a computer or network owing to problems (bugs) in the software or firmware. Freezing, locking, or crashing of a program causing unresponsiveness.

Defense: Ensure that the vendor applies all software updates for its infrastructure on a frequent basis. Do the same for all customer-owned virtual systems.

Detection: Implement service monitoring to detect and alert when an application does not respond correctly.

Deterrence: Use legal language to clearly set the expectation that the service provider will maintain a stable environment.

Residual risk: As the instability of applications and infrastructure generally occurs as a result of a software problem, little can be done to stop them from occurring.

Slowness Unacceptable response time of a computer or network.

Defense: Using redundant providers and Internet connections, set up the architecture so application access will automatically switch to the fastest environment. Also ensure service providers have implemented high capacity services with automatic expansion of resources.

Detection: Monitor response time of applications on a continuous basis and ensure that alerts have an out-of-band path to support staff so response problems don't stop alerts from being delivered.

Deterrence: Establish contract language with service providers that provides penalties in the form of compensation to you for unacceptable response times.

Residual risk: Latency or slow responses can be thought of as a form of outage and, as such, being caused by software and capacity issues, can persist despite best efforts.

HA failure The discovery that a device that was supposed to fail over doesn't actually take over when it should.

Defense: Monitor the health of secondary systems or all systems in an HA cluster.

Detection: Perform periodic failover testing.

Deterrence: Not much can be done from a service provider perspective to guarantee that customer systems will switch over when they are supposed to.

Residual Risk: Sometimes a primary device slows down to the point that it becomes unresponsive for all practical purposes, but because it's not officially "down" according to the software, the backup system doesn't take over.

Backup failure The discovery that those data backups you were relying on aren't actually any good.

Defense: Leverage provider elasticity to avoid the use of traditional offline (tape or optical) backups.

Detection: Frequently perform recovery testing to validate the resilience of data.

Deterrence: Establish a data-loss clause in the contract with the service provider so they are obligated to assist with unforeseen data loss.

Residual risk: Backups fail, but multiple recovery paths can eliminate most of the risk. The practice of backing up data has been around for a long time, and consequently it's one of the most reliable security practices. As long as data is appropriately replicated, it can live forever, so most of the residual risk in this case would be due to substandard data replication practices or lack of attention to this matter.

Summary

Virtual machines present greater risks than old-fashioned standalone computers, because they provide computing environments that are based on software, which has inherent vulnerabilities, and because virtual machines are controlled by a master operating system known as the hypervisor. Attacks against vulnerabilities in the software that runs the guest operating systems or the hypervisor itself can lead to compromises in one, many, or all virtual systems in your infrastructure. For that reason, special consideration must be given to the virtual environment. Securing the hypervisor is of paramount importance—it needs to be isolated from the guest OSs and administrative access to it needs to be strictly controlled. The guest OSs themselves need to be protected with standard security software, as well as secure configurations within the virtual environment. Virtual storage and networks deserve the same consideration.

Cloud computing takes many forms, but they all have one thing in common—the Internet. And because cloud services are housed on the Internet, they carry all the risks inherent in the Internet as well as additional risks associated with the proximity of other users of the service, especially if any of those other users are malicious. In this chapter, we covered the different risks of cloud computing, and some countermeasures that can mitigate some of those risks. Along with confidentiality risks that come from putting private data in the cloud, and integrity risks associated with the loss of direct control of data, the cloud also presents availability risks, because the Internet is an inherently unreliable medium. Real incidents that have been tracked by various agencies prove that service outage is the most commonly experienced security issue with commercial cloud services. Redundancy is the best way to mitigate those availability risks, just as with any other Internet service.

References

Barrett, Diane, and Greg Kipper. *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments*. Syngress, 2010.

Bauer, Eric, and Randee Adams. *Reliability and Availability of Cloud Computing*. Wiley, 2012.

Chuvakin, Anton et al. *The Cloud Security Rules*. CreateSpace, 2011.

European Network and Information Security Agency. *ENISA Cloud Computing Information Assurance Framework*. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/

Halpert, Ben. *Auditing Cloud Computing: A Security and Privacy Guide*. Wiley, 2011.

Hoopes, John. *Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting*. Syngress, 2008.

Krutz, Ronald, and Russell Dean Vines. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley, 2010.

Mather, Tim, and Subra Kumaraswamy. *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly, 2009.

National Institute of Standards and Technology. *Special Publication 800-125, Guide to Security for Full Virtualization Technologies*. http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

National Institute of Standards and Technology. *Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing*. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

National Institute of Standards and Technology. *Special Publication 800-146, Cloud Computing Synopsis and Recommendations*. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075

Ottenheimer, Davi, and Matthew Wallace. *Securing the Virtual Environment: How to Defend the Enterprise Against Attack*. Wiley, 2012.

Rittinghouse, John, and James Ransome. *Cloud Computing: Implementation, Management, and Security*. CRC Press, 2009.

Winkler, Vic. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Syngress, 2011.