CASE STUDY 11

CLOUD COMPUTING (IN)SECURITY

Cloud computing is reshaping enterprise network architectures and infrastructures. It refers to applications delivered as services over the Internet as well as the hardware and systems software in data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS) which had its roots in Software-Oriented Architecture (SOA) concepts that began shaping enterprise network roadmaps in the early 2000s. IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) are other types of cloud computing services that are available to business customers.

Cloud computing fosters the notion of computing as a utility that can be consumed by businesses on demand in a manner that is similar to other services (e.g. electricity, municipal water) from traditional utilities. It has the potential to reshape much of the IT industry by giving businesses the option of running business software applications fully on-premises, fully in "the cloud" or some combination of these two extremes. These are choices that businesses have not had until recently and many companies are still coming to grips with this new computing landscape.

Security is important to any computing infrastructure. Companies go to great lengths to secure on-premises computing systems, so it is not surprising that security looms as a major consideration when augmenting or replacing on-premises systems with cloud services. Allaying security concerns is frequently a prerequisite for further discussions about migrating part or all of an organization’s computing architecture to the cloud. Availability is another major concern: “How will we operate if we can’t access the Internet? What if our customers can’t access the cloud to place orders?” are common questions [AMBR10].

Generally speaking, such questions only arise when businesses contemplating moving core transaction processing, such as ERP systems, and other mission critical applications to the cloud. Companies have traditionally demonstrated less concern about migrating high maintenance applications such as e-mail and payroll to cloud service providers even though such applications hold sensitive information.

Security Issues and Concerns

Auditability is a concern for many organizations, especially those who must comply with Sarbanes-Oxley and/or Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) regulations [IBM11]. The auditability of their data must be ensured whether it is stored on-premises or moved to the cloud.

Before moving critical infrastructure to the cloud, businesses should do diligence on security threats both from outside and inside the cloud [BADG11]. Many of the security issues associated with protecting clouds from outside threats are similar to those that have traditionally faced centralized data centers. In the cloud, however, responsibility for assuring adequate security is frequently shared among users, vendors, and any third-party firms that users rely on for security-sensitive software or configurations. Cloud users are responsible for application-level security. Cloud vendors are responsible for physical security and some software security such as enforcing external firewall policies. Security for intermediate layers of the software stack is shared between users and vendors.

A security risk that can be overlooked by companies considering a migration to the cloud is that posed by sharing vendor resources with other cloud users. Cloud providers must guard against theft or denial-of-service attacks by their users and users need to be protected from one another. Virtualization can be a powerful mechanism for addressing these potential risks because it protects against most attempts by users to attack one another or the provider's infrastructure. However, not all resources are virtualized and not all virtualization environments are bug-free. Incorrect virtualization may allow user code to access to sensitive portions of the provider's infrastructure or the resources of other users. Once again, these security issues are not unique to the cloud and are similar to those involved in managing non-cloud data centers, where different applications need to be protected from one another.

Another security concern that businesses should consider is the extent to which subscribers are protected against the provider, especially in the area of inadvertent data loss. For example, in the event of provider infrastructure improvements, what happens to hardware that is retired or replaced? It is easy to imagine a hard disk being disposed of without being properly wiped clean of subscriber data. It is also easy to imagine permissions bugs or errors that make subscriber data visible to unauthorized users. User-level encryption may be an important self-help mechanism for subscribers, but businesses should ensure that other protections are in place to avoid inadvertent data loss.

Addressing Cloud Computer Security Concerns

Numerous documents have been developed to guide business thinking about the security issues associated with cloud computing. Even NIST has weighed in on these issues [BADG11]. NIST's recommendations systematically consider each of the major types of cloud services consumed by businesses including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). While security issues vary somewhat depending on the type of cloud service, there are multiple NIST recommendations that are independent of service type. Several of these are summarized in Table C11.1. Not surprisingly, NIST recommends selecting cloud providers that support strong encryption, have appropriate redundancy mechanisms in place, employ authentication mechanisms, and offer subscribers sufficient visibility about mechanisms used to protect subscribers from other subscribers and the provider.

As more businesses incorporate cloud services into their enterprise network infrastructures, cloud computing security will persist as an important issue. Examples of cloud computing security failures have to potential to have a chilling effect on business interest in cloud services and this is inspiring service providers to be serious about incorporating security mechanisms that will allay concerns of potential subscribers. Some service providers have moved their operations to Tier 4 data centers to address user concerns about availability and redundancy. Because so many businesses remain reluctant to embrace cloud computing in a big way, cloud service providers will have to continue to work hard to convince potential customers that computing support for core business processes and mission critical applications can be moved safely and securely to the cloud [HEAV11].

Discussion Points

1. Do some Internet research to identify businesses who have suffered because of cloud security weaknesses or failures. What can companies who are contemplating cloud computing services learn from the negative experiences of these businesses?

2. Do some Internet research on security mechanisms associated with virtualization. How can virtualization be used by cloud service providers to protect subscriber data?

3. Choose one of the following cloud services categories: SaaS, IaaS, PaaS. Do some Internet research that focuses the security issues associated with the selected cloud service category. Summarize the major security risks associated with the cloud service category and identify mechanisms that can be used to address these risks.

Sources

[ARMB10] Armbrust, M., Fox, A., Griffith, R, Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M. "A View of Cloud Computing." Communications of the ACM, Vol. 53, No. 4, April 2010, pp. 50-58.

[BADG11] Badger, L., Grance, T., Patt-Comer, R., and Voas, J. Draft Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology, Special Publication 800-146, May 2011.

[HEAV11] Heavey, J. "Cloud Computing: Secure or Security Risk?" Technorati.com, November 28, 2011. Retrieved online from: http://technorati.com/technology/cloud-computing/article/cloud-computing-secure-or-a-security1/.

[IBM11] IBM Global Technology Services. Security and Availability in Cloud Computing Environments, Technical White Paper, June 2011.

Table C11.1 NIST Cloud Computing Security Recommendations

- Employ best practices for web browser security and patching; strive to minimize browser exposure to potentially malicious websites.

- Require strong encryption for web sessions with cloud provider applications that require data transfers and/or the confidentiality of interactions with other applications. Also require strong encryption for stored data.

- When selecting a cloud provider, consider physical plant security plans and practices at the cloud provider site(s). Develop written plans for recovery from physical attacks at cloud provider sites.

- Investigate the redundancy offered by the provider and choose a provider that is not tied to a specific geographic location in case of natural disasters or other disruptions.

- Use authentication tokens if these are offered by providers. These mitigate the risk of account hijacking.

- Ensure that subscribers have visibility into the authentication and access control mechanisms that the provider infrastructure supports.

- Ensure that subscribers have visibility into the tools that are available for cloud subscribers to provision authentication information, and the tools used to input and maintain authorizations for subscriber users without the intervention of the provider.

- Benchmark current application performance and establish key performance score requirements before an application is moved to the provider's site. Key performance scores typically include responsiveness (response time) for interactive user applications, and bulk data transfer performance for applications that must input or output large quantities of data.

- Request the provider to allow visibility into the operating services that affect user data or operations on that data.