A Walk In The Clouds

Security Issues To Watch In Cloud Computing

Some things never change. From when personal computers first came around, you might remember a colleague or a friend showing off his/her “latest” i386 processor-based machine running the “sophisticated” Tank Wars game. At the time, you’d have wished that there were some sort of rental service around that would let you use these high-end machines at a fraction of the cost of buying it and even avoid the pain of watching the next best processor being released a few months after your purchase. Things are the same today, except we now have such a rental service!

Enter – The Cloud! High-end computing is now available as a “metered” service of sorts thanks to cloud computing. The costs involved are low, the technology and computing power is the best available at any given time, and all an end-user needs to connect is a low-end computing device (even a smart-phone or a tablet) with reasonably good Internet connectivity. Thanks to cloud computing, today we have Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Monitoring as a Service (MaaS), Communication as a Service (CaaS), Voice as a Service (VaaS), and essentially Anything as a Service (XaaS).

With the cost-efficiencies that the cloud brings about, organizations the world over should be rubbing their palms in delight. Several organizations have already embarked on a journey to migrate their technical infrastructure to the cloud and several others will likely follow suit. The cloud has some clear arguments in its favor – cost, agility, scalability, reliability, location independence, and overall performance.

However, cloud computing, being a relatively nascent technology, also introduces several information security risks that need special attention. To draw a simple parallel, subscribing to cloud-based services is like getting an electricity connection for your home in a metered manner – you pay for what you use. However, in this case, you wouldn’t be too concerned about your electricity getting mixed with your neighbor’s electricity before reaching your home. Replace electricity with corporate information, though, and it should definitely raise eyebrows.
Information Security – A Clouded Issue

On the face of it, the issue might appear mainly technical. However, we live in highly regulated times and so the legal and regulatory perspectives to cloud computing security make this a cloudy affair. An organization eyeing cloud computing as their next stop should take a long, hard look at the following key issues –

Technically Speaking

• A primary question that an organization needs to ask is – “Where exactly is my data?” The cloud is like a house with multiple tenants. It offers a great deal of computing power but, by itself, it doesn’t offer much in terms of isolation. Organizations need to ask their cloud service provider precisely how they will offer this isolation. How, for instance, will they ensure that data classified “Highly Confidential” is treated that way? What does the cloud service provider do to ensure that classified data is not handled by a server (or cluster) that processes public requests? Is the data encrypted and, if so, what type of encryption is used for data at rest and in transit? What about the physical security of all the facilities?

• Data loss and leakage risks, if not properly addressed, are very high in cloud computing environments. When multiple tenants live in one house, the risk of one tenant’s information falling into another’s hands increases considerably. The question organizations need to ask their cloud service provider is – “How will data loss and leakage risks be minimized to acceptable levels?” How, for instance, will they address these risks at the design-level itself? How will they deal with persistent media? What provisions and safeguards do they have for backup, restore, and storage?

• Logging and monitoring has come a long way and today forms an integral component of an organization’s information security defenses. When moving to the cloud, organizations need to ask their cloud service provider how logging and monitoring will be performed. This is a non-trivial task because we’re now talking about the loosely-coupled cloud environment and not a tightly managed technical infrastructure.

• A cloud service provider has physical machines and computing resources located at some physical location on the globe. This is an important aspect to look into for organizations considering moving to the cloud. What kind of a business continuity plan (BCP) and disaster recovery plan (DRP) does the cloud service provider have in place? Your own BCP and/or DRP would have saved the day for you if your data was in-house; except it won’t be that way once you move to the cloud.

• The cloud is, at the end of the day, a technical implementation that, like any other technical implementation, is bound to have information security vulnerabilities. Organizations need to get lucid clarifications from their cloud service provider as to how their offered cloud will be tested for information security vulnerabilities on an ongoing basis to ensure that the infrastructure on which the organization’s information rests is secure at all times. Also, depending on the cloud service provider to perform these audits and assessments would not be a good idea because then the cloud service provider would be tasked with auditing what it implemented. It is important to remember that a cloud-service provider might want you to believe that its infrastructure rests in iron-clad, multi-layered, facilities on the planet Krypton with Superman himself standing guard outside it. However, these facilities attract hackers like bees to honey. If you were to think from a hacker’s point of view, the target is attractive and the return on investment is high.
Incident Response

- Information security incidents at organizations need to be identified, contained, investigated, and even reported in accordance with regulations and mandates. Challenging as it is to perform this process at an organization; it is almost a breeze if you were to compare it with the challenges involved in doing this in a cloud environment. Organizations need to obtain clarity from their cloud service provider on how they will help and support the entire incident response process that was earlier followed when the infrastructure was in-house. How exactly will the cloud service provider help identify the root causes of the incident? This is more complicated than it sounds because during this incident response process, the cloud service provider would actually need to begin by accepting that its cloud infrastructure was not fully secure.

- Digital forensic investigations that ensue following an information security breach or incident pose another significant challenge. Organizations need to consider how evidence will be preserved and what that evidence will be considering that the cloud does not offer much visibility into it as, say, a normal workstation would. How will evidence be collected from the machine image since there is no longer the luxury of working with the full disk? How will evidence be collected from data resting in the Random Access Memory (RAM) or slack space considering that these areas are no longer well-defined and could be spread across hundreds of machines? How will routing information be collected?

- One significant challenge during incident response that organizations will face is that of gleaning information from auditing and monitoring logs. Organizations using the cloud will need to take note of the fact that analyzing an ocean of data, available from the heavy and comprehensive logs that clouds can generate, is not an easy task. To add to the woes, consider a case where cloud-based anti-virus software identified an infected file, but the computing was done by another, remote computer. Situations like these can be a nightmare for an incident response team.

People and Processes

- People are often considered the weakest link in information security. An aspect that cannot be overlooked in the cloud perspective is precisely this weakest link – what is sometimes known as the “human firewall”. Organizations would do good to find out more about the people and the processes that work behind the scenes of their cloud service provider. What does the cloud service provider do to test the “human firewall”? What controls are enforced on individuals that have access to the cloud service provider’s customer data? In a situation where an employee turns rogue, it could mean serious consequences for all organizations hosted with the cloud service provider because an insider is a serious threat to information security considering he/she has detailed knowledge of internal processes and “knows his/her way around”.

- Another important consideration for organizations eyeing the cloud is to investigate what their cloud service provider does to train its employees in information security. A malicious employee is bad enough, but an unaware employee is not any better.
Legal and Regulatory Angles

- Cloud computing is offered to several customers around the globe. These customers sometimes include malicious ones—a case in point being the infamous Zeus botnet. The ease of registration and anonymity offered by cloud computing providers makes matters worse. Organizations need to consider the potential issues that they would have to deal with if their cloud service provider were to house even one such customer who proves to be a handful. The cloud service provider would probably remain stuck in a legal net for a while. Its customers, still unsure on whether their data was breached, would then be faced with the task of migrating to a new provider.

- Organizations with a keen eye for issues like the one just described might look at stringent contractual and service level agreements with cloud service providers. These agreements, however, need to incorporate issues like regulatory requirements, third-party service provider oversight, right to audit the cloud infrastructure, clear wording on liability, intellectual property, end-of-service considerations and responsibilities, record-keeping requirements, data jurisdiction, and the cloud service provider’s compliance with internationally recognized standards.

- Electronic Discovery (E-Discovery) is quite a normal task when regular workstations hosted in-house in an organization are involved. When a cloud comes into the picture, organizations will then be faced with identifying where the information is stored, how it is backed up, and how it is secured. The E-Discovery rules assume that the physical examination of storage devices, media, and just about anything stored electronically is possible. This will change completely with the cloud which will add a whole new dimension to electronically stored information. Organizations need to consider that if they are, at any point, involved in litigation, E-Discovery will be a demanding task.

The Right Expertise

Cloud computing technology has taken the world by storm. The advantages are undisputed and surely need to be harnessed. The cloud is undoubtedly the jet fuel that the world has been looking for to propel organizations into the next generation of efficient and technology-powered business. However, the information security issues that have followed cloud computing are serious and need to be carefully considered and addressed by organizations that are looking to take advantage of the cloud.

With the right information security expertise backing an organization’s advance into the cloud, there is clearly no stopping the organization’s progress into this new world of opportunities.

Take a walk in the cloud, but watch your step!
ENTERPRISE RISK MANAGEMENT: AT A GLANCE

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services

IT Security
Regulatory Compliance
IT Audit
Computer Forensics
Risk Management
Attestation

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Qualified Security Assessor (QSA)
Approved Scanning Vendor (ASV)

Some of our Clients

ABN-AMRO Private Banking
Bacardi-Martini, Inc.
Bancafe International
Banco Industrial de Venezuela
Banco ITAU
Bank United
Caja Madrid Bank
Carnival Cruise Lines, LLC
CitiBank
Coconut Grove Bank
Commerce Bank
E-data Financial
Florida International University
Florida Power & Light Company
Heico Aerospace
Helm Bank
Knight Ridder
Nova Southeastern University
Rinker Materials
Rudy, Exelrod & Zieff, LLP
Seabourn Cruise Line
TecniCard, Inc.
The International Bank of Miami
TransAtlantic Bank
U.S. Century Bank

For more information visit:
www.emrisk.com
email info@emrisk.com
phone 305.447.6750
800 Douglas Road, North Tower, Suite 940
Coral Gables, FL 33134