A Review of Cloud Computing

By: Hope Roskelly

Abstract: Cloud computing offers many benefits to companies. These benefits come at a cost. There are many security threats and vulnerabilities that come along with utilizing cloud computing. However, there are preventative measures that companies can do to protect themselves from these threats and vulnerabilities. There are many pros and concerns that businesses have with cloud computing. Some of these threats and concerns will be remedied through the next few years as the market pushes weak cloud providers out and the big players buy up other cloud providers.

Introduction

Cloud computing has become popular over the years because it is cheaper, faster, and more flexible. It enables business and individuals to access information without concern about the server's physical location. However, cloud computing also raises major concerns for security. They have become targets for hackers, criminals, terrorists, and rouge nations. With all of the pros of cloud computing people are setting aside the concerns about security. Security on the web should not be an afterthought. It needs to be at the forethought as cloud technology is developed and implemented. In this paper I will review the service models that cloud computing offers. I will then move into the security issues, vulnerabilities along with the preventative measures that can be used. I then discuss the pros and concerns that companies have with cloud computing. Lastly, I talk about the impact cloud computing will have on IT jobs, as well as, the future of cloud computing.

Cloud Services

Cloud computing offers the following service models; Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides applications to the clients through the Internet that multiple users can use. The provider is responsible for the administration of these services. The main benefit of SaaS is that all of the clients are running the same software version. This makes new functions easily available to all clients as well. An example of this is web-based email. [8] Some people have been using cloud computing without even realizing it. For example most people use web-based email and do not realize it is part of cloud computing.

PaaS provides an application platform as a service. This refers to providing platform layer resources like operating system support and software development frameworks. [5] This allows clients to create custom software using the tools and programming languages offered by the provider. This also gives clients control over the applications and environment related settings. PaaS makes it so that nothing as to be downloaded onto the local machine. The provider is responsible for the management of the underlying infrastructure. [8]

IaaS provides hardware as a service. For example CPU, disk space or network components. IaaS makes server, storage, and other peripherals devices that are available through the use of the Internet. These resources are made

available through virtualization. This gives the client full control of the virtualized platform. Just like SaaS and PaaS, the provider manages the infrastructure. [8] There are some security issues that are related to every service model that the cloud offers.

Security Issues In SaaS, PaaS, and IaaS

SaaS and PaaS are hosted on top of IaaS. Therefore a breach in IaaS will impact the security of both SaaS and PaaS services. This can also happen the other way around as well. This means that there is a security dependency between them. A problem with this dependency is that a SaaS provider may rent a development environment from a PaaS provider who can then rent an infrastructure from an IaaS provider. Since each provider is responsible for securing their own services, they may all have different security models. This also causes confusion when an attack happens over which service provider is responsible. [5] If you do not know who is responsible then it will be hard to resolve the problem.

SaaS users have the least amount of control over security than any other services models of the cloud. Traditional security models do not effectively protect SaaS from attacks. Therefore, new approaches need to be used. [5] As cloud computing becomes more accepted and implemented security solutions should be tailored to issues specific to SaaS.

There are two software layers that are compromised by PaaS application security: security of the PaaS platform and security of customer applications that are used on a PaaS platform. Due to the use of mashups, PaaS users have to depend on both the security of web-hosted development tools and third-party services. The data for both SaaS and PaaS is associated with an application running in the cloud. Therefore, the security depends on the provider while the data is being processed, transferred, and stored. [5] PaaS offers some great advantages to developers of cloud applications but they have to be aware of the security issues involved.

Users of IaaS have better control of the security than the other services models of the cloud, provided that there are no security holes in the virtual monitor. The user is responsible for setting the security policies correctly because they are in control of the software running on their virtual machines. Virtualization gives users the ability to create, copy, share, migrate, and roll back virtual machines. However, virtualized environments are harder to secure because they add more points of entry and more interconnection complexity. [5] While we have talked about security issues related to each service model for the cloud, there are some over all security threats as well.

Security Threats

The CSA (Cloud Security Alliance) has issued a report on the top threats of cloud computing. The report release in 2013 has nine threats; the report for 2016 has twelve threats. This shows that more and more threats are being discovered for cloud computing. I expect this to continue to grow as more businesses implement this technology.

1. Data Breaches

"A data breach is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so." [3] There can be many causes of a data breach. It can be the result of an attack, human error,

application vulnerabilities, and poor security practices. A data breach is the main concern of most companies considering using cloud computing and for good reason. Cloud providers are easily accessible and have large amounts of data. [3] This makes them an attractive target for attackers.

Data breaches can cause companies to incur large fines, civil lawsuits, and criminal charges depending on the sensitivity of the information that was breached. Data breaches can also damage a company's reputation and cause a loss in business. Cloud providers generally have good security for the parts they are responsible for. However, it is ultimately the customer's responsibility for protecting their data in the cloud. The best way to prevent against a data breach is an effective security program. This should include multifactor authentication and encryption. [3]

2. Insufficient Identity, Credential and Access Management

The lack of scalable identity access management systems, failure to use multifactor authentication, weak passwords, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates can result in data breaches and attacks. Keys must be kept appropriately secured. They should also be rotated periodically. Identity management systems need to update resources when personnel changes occur. When a legacy system that only requires a password is used, the authentication system needs to support policy enforcement. This should include verification of a strong password and organization-defined rotation period policy. [3]

Companies should be careful when considering placing all of their passwords in a centralized spot because it is a high-value target for attackers. If a company chooses to go this route they should have monitoring and protection of identity and key management as a high priority. [3]

3. Insecure Interfaces and APIs

Users use a set of software user interfaces (UIs) or application programming interfaces (APIs) to manage and interact with cloud services. The security of the APIs is important because the security and availability of general cloud services depend on them. APIs and UIs are usually the most exposed part of the system. Therefore, these need to be protected from the Internet where they will be the targets of heavy attacks. [3]

Users must understand the security that providers have integrated into their models. If the user relies on a weak set of interfaces and APIs they will be exposed to security issues related to confidentiality, integrity, availability and accountability. Companies need to utilize threat modeling applications and systems, security-specific code reviews, and penetration testing to ensure their security is adequate. [3]

4. System Vulnerabilities

"System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system or disrupting service operations." [3] Bugs have been a problem since the invention of the computer. However, multitenancy allows systems from various organizations to be placed close together, along with shared memory and resources. This creates a new surface for attackers. Simply keeping systems updated will do a lot to keep the system secure. This is especially important for organizations that are

highly regulated. These organizations need to be able to handle patching quickly. [3]

5. Account Hijacking

Attackers use methods such as phishing, fraud and exploitation of software vulnerabilities. The cloud adds a new threat to this because if an attacker gains access to your account they can eavesdrop, manipulate data, falsify data and redirect clients to illegitimate sites. This gives them the ability to use your company's reputation to launch attacks. The best way to prevent this is to prohibit the sharing of account credentials and utilize two-factor authentication techniques. All accounts and account activities should be traceable to a human owner. [3]

6. Malicious Insiders

"A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."[3] The systems that are on the security provided by the cloud provider are at a greater risk. However, not all malicious insiders are trying to be malicious. Some are employees who accidentally cause a negative impact on the company while doing their jobs. [3]

7. Advanced Persistent Threats

"Advanced Persistent Threats (APTs) are a parasitical form of cyber attack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them." [3] The most common points of entry for APTs is spearphishing, direct hacking systems, USB with attack code, penetration through partner networks, unsecured or third-party networks. They can literally blend into the network traffic. [3]

APTs can be difficult to detect and eliminate. However, proactive measures such as awareness programs can defend against these types of attacks. Employees should be trained to think before they open an attachment or a link. [3]

8. Data Loss

There are many causes of data loss; attacks, accidental deletion, or a natural disaster are some of the causes. Companies should follow best practices in business continuity and disaster recovery. They should also have a daily data backup and maybe even offsite storage. It is not just up to the cloud provider to protect against data loss. Companies need to be mindful of their encryption keys. If the company looses an encryption key then the data will also be lost. Some of the solutions that providers offer are geographic redundancy, data backup, and premise-to-cloud backups. Companies should consider the security risks they are taking to allow providers to backup and protect their data. Companies may want to do this in-house or do both if the data is highly critical. [3]

9. Insufficient Due Diligence

Companies need to be sure that they do not rush into using cloud computing. If a company does not do their due diligence when choosing their cloud technologies and providers they can

expose themselves to commercial, financial, technical, legal, and compliance risks. This also includes companies that are thinking about merging with a company that uses the cloud or are thinking about using the cloud. [3]

10. Abuse and Nefarious Use of Cloud Services

Cloud Computing models are exposed to malicious attacks because of poorly secured cloud service deployments, free cloud trials, and fraudulent account sign-ups. Attackers can launch DDos attacks, email spam, phishing campaigns, mining, large–scale automated click fraud, brute-force compute attacks, and hosting of malicious or pirated content. This can cause cloud services to become unavailable, business disruptions and loss of revenue for other sites that are on the same cloud platform. [3]

11. Denial of Service

"Denial-of-service (DoS) attacks are attacks meant to prevent users of a service from being able to access their data or their applications." [3] This is accomplished by causing the targeted cloud service to consume large amounts of finite system resources. Attackers can also cause a significant system slowdown to the point that it does not respond. This is called a distributed denial-of-service (DDoS). Asymmetric application-level DoS attacks allows an attacker to take out an application with a single small attack payload. This payload can be less than 100 bytes. In some cases, a DDoS attack can be a smokescreen for an attack happening in another part of the environment. [3]

12. Shared Technology Vulnerabilities

Scalability in the cloud is offered through shared infrastructure, platforms, and applications. Cloud technology was developed without having to change the off-the-shelf hardware and software. These may not have been designed for the isolation properties that are needed for a multitenant architecture, re-deployable platforms, or multicustomer applications. This creates vulnerabilities that can be exploited by attackers. To help prevent a breach companies should use multi-factor authentication, Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection Systems (NIDS). [3]

Vulnerabilities of Cloud Computing

Along with security threats there are also vulnerabilities associated with the use of the cloud. These are vulnerabilities that are technology-based but they also affect the security of the cloud as well.

- Lack of employee screening and poor hiring practices
- Lack of customer background checks
- Lack of security education

Cloud Technology utilizes existing technologies such as web services, web browsers, and virtualization. It is for this reason that any vulnerability that is associated with these technologies affects the cloud. [5] Now that we have talked about the threats and vulnerabilities, we will talk about the pros and concerns of cloud computing.

Pros And Concerns of Cloud Computing

Cloud computing offers many advantages to companies and individuals. The pros of using cloud computing are:

- Flexibility: cloud technology is great for companies with growing or fluctuating bandwidth. [11]
- Disaster Recovery: Cloud technology helps small businesses save large upfront costs for backup and recovery of their systems. [11]
- Automatic Software Updates: Cloud providers handle the regular software and security updates for you. [11]
- Capital-Expenditure Free: Cloud technology gets rid of the cost of hardware. Companies can simply pay as they go. [11]
- Increased Collaboration: Cloud technology enables teams to access, edit and share documents at anytime, from anywhere. [11]
- Work From Anywhere: With cloud technology you can work anywhere there is an Internet connection. Some cloud providers even offer mobile apps.
- Document Control: With cloud technology you have only one version of a document instead of multiple versions flying around emails. [11]
- Security: You no longer have to worry about loosing data due to a lost laptop. Cloud computing allows you to access your data from any machine and can be remotely wiped from a lost laptop. [11]
- Competitiveness: Cloud technology allows small business to be able to compete with big businesses. [11]
- Environmentally friendly: The scalability of cloud technologies enables companies to use only the energy that it needs. [11]

As you can see there are many pros to moving to cloud computing but there are also some concerns. The concerns of using cloud computing are:

- Security
- Performance
- Availability
- Hard to integrate with in-house IT
- Not enough ability to customize
- Worried on-demand may cost more
- Bringing back in house may be difficult
- Regulatory requirements prohibit cloud
- Not enough major suppliers yet

As you can see companies have many concerns about implementing cloud technologies. [10]

Impact of Cloud Computing On IT Jobs

How much has cloud technology really been accepted by the business world? “RightScale is showing 93 percent of businesses using cloud technology in some form or another.” [2] This shows that most businesses are already using cloud technology. “According to RightScale’s State of the Cloud report, which surveyed 930 IT professionals about their current adoption and future plans involving cloud computing, 88 percent of businesses are using public cloud technology and 63 percent are using private cloud. Eighty-two percent have a hybrid cloud strategy, up from 74 percent in 2014, a clear indication that the cloud has quickly become an essential ingredient of modern IT. “[2] With so many businesses accepting the cloud I began to wonder how this was going to affect IT jobs.

Will the cloud be the end of some IT jobs? So far it seems that for the next few years cloud technology will act as a complement to on-premises systems instead of being a replacement. [7] As

more organizations switch to the cloud there will be less staff needed to manage and provision the IT infrastructure. However, there will be new IT jobs created. “There are not going to be fewer people involved in IT, but they will be involved in IT in different ways.”[6] Some are predicting that that there will be more collaboration and outsourcing of work. They are also predicting that there will be more specialization. Jobs have been changed, created, and eliminated over the years as technology has grown. There was the “corporate re-engineering” boom after email and networking was created. There was also the shift to outsourcing and offshoring after the creation of the dot-com bubble. [4] IT jobs continued to boom after these technologies were implemented into the businesses world. Therefore, even though some IT jobs may be eliminated, others will be created or changed. “Experts believe that numerous organizations will not allow their sensitive data to be stored on the cloud for another 10 years.”[1] For now it seems there will still be a place for IT departments in organizations.

The Future of Cloud Computing

With the many strengths and weaknesses of Cloud Computing, does it have a place in the future? There are some things that need to be done for cloud computing to live up to its potential. Obviously some of the security concerns need to be addressed. Some of the best ways to solve these concerns is for cloud providers to build trust with their clients, become more transparent, and develop standards. Other problems will fix themselves over the next few years. “The market mechanism automatically leads to survival of the fittest, no matter the adapted and designed products or lowest priced model.” [9] More and more providers will either be bought by larger companies or will fizzle out due to competition. This will solve some of the issues of having so many different providers offering different services of the cloud, which in turn is causing different security models that was discussed earlier.

Conclusions

Cloud computing as a long way to go before it will meet its full potential. There are many security problems that need to be addressed and some that are just inherent. However, there are preventative measures that can be put into place. There are also many pros and concerns that companies need to consider before they decide to use cloud computing. Cloud computing will impact both the business world and the IT jobs in it. However, there will still be plenty of IT jobs. There will simply be some changes in jobs; some jobs will be eliminated, others will be supplemented by job creation. Lastly, cloud computing has a bright future as the market weeds out the weak cloud providers and the others get bought up by the big players.

References

[1] Devanney, P., Quilliam, W., DuVal, C. W., & Santos, N. ". (2016). Offsite information storage: Cloud computing and cyber security issues. *International Conference on Accounting and Finance (AT). Proceedings,* , 75. doi:10.5176/2251-1997_AF16.37

[2] Florentine, S. (2016, Jan 5). *Cloud adoption soars, but integration challenges remain.* Retrieved July 16, 2016, from CIO: http://www.cio.com/article/3018156/cloud-computing/cloud-adoption-soars-but-integration-challenges-remain.html

[3] The Threats Working Group (2016, Feb 1). *The Treacherous 12-Cloud Computing Top Threats in 2016.* Retrieved July 16, 2016, from CSA: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf

[4] Hardy, Q. (2014, Nov 24). *How will cloud computing impact your job? Find out.* Retrieved July 16, 2016, from New York Times: http://economictimes.indiatimes.com/magazines/panache/how-will-cloud-computing-impact-your-job-find-out/articleshow/45258709.cms

*[5] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1-13. doi:10.1186/1869-0238-4-5

[6] Heath, N. (2012, May 28). *Revealed: The jobs that will be wiped out by cloud computing.* Retrieved July 16, 2016, from TechRepublic: http://www.techrepublic.com/blog/cio-insights/revealed-the-jobs-that-will-be-wiped-out-by-cloud-computing/

[7] Jennings, C. (2008, June). *The end of the IT department-is it in the cloud?* Retrieved July 16, 2016, from Computer Weekly: http://www.computerweekly.com/feature/The-end-of-the-IT-department-is-it-in-the-cloud

*[8] Kaur, A., & Bhagat, N. (2014). A Review On Cloud Computing Security Issues. *International Journal of Advanced Research in Computer Science, 5*(7)

[9] Penzel, D., Kryvinska, N., Strauss, C., & Gregu, M. (2015). The future of cloud computing: A SWOT analysis and predictions of development. Paper presented at the 391-397. doi:10.1109/FiCloud.2015.102

*[10] Shah, H., Anandane, S. S., & Shrikanth. (2013). Security issues on cloud computing. *International Journal of Computer Science and Information Security, 11*(8), 25.

[11] UK, S. (2015, Nov 17). *Why Move To The Cloud? 10 Benefits of Cloud Computing.* Retrieved July 16, 2016, from Salesforce UK & Ireland Blog: https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html