Security Risks of Cloud Computing

Joey Ray
ITEC 452
jray24@radford.edu

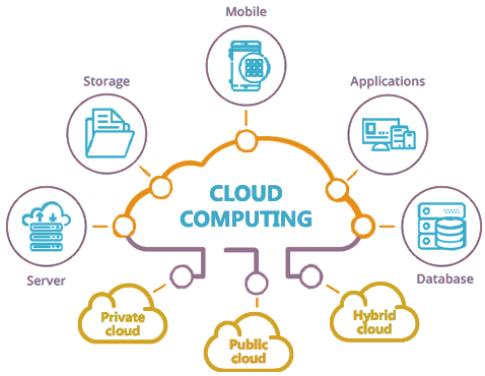
***Abstract*— Cloud Computing is the backbone of building reliable and sustainable companies in today's day in age. It's what makes companies work flow together in an efficient and timely manner. This is why making sure these features are properly secure is extremely important not only for big companies, but everyday people too.**

Keywords—computing, cloud, security, technology, IT

I. Introduction

Cloud computing is an internet based delivery system that allows access to data in a fast, reliable, secure fashion. There are three types of clouds that are commonly used: public cloud, private cloud, and a hybrid cloud. Each of these clouds has a specific reasoning for their use. Public clouds are used for things like public servers and storage that can used by anyone at the appropriate cost. Private clouds are used by individual companies that are the only ones with access to them (besides the providing company), commonly used to store private company data. A hybrid cloud can be used as a link between public and private clouds making an easy connection between datacenters and servers used by a company. [1]

Public clouds can support multiple customers are looking for the same thing such as: Dropbox, email providers, Microsoft Office, and VMWARE. Private clouds support one client that has private access to their services mostly used datacenter, some examples of private clouds are Amazon Web Services and Windows Azure.



[4]

II. Cloud Security

A. Basic Security

With all this important data being stored and used primarily via the internet there needs to be an abundance of security protocols. A few basic security protocols that are used include data masking, firewalls, access control, threat intelligence, and recovery systems. Without these security implementations company's important data could be breached and compromised which would be detrimental and cost them fortunes.

Cloud security is all about securing data for the clients. Companies look for cloud-based services that have top security protocols and a solid backup plan incase anything were to go south. To do this these providers go through a ten-step process to ensure maximum security: [2]

1. Governance, risk and compliance processes
2. Audit operational and business processes
3. User privileges
4. Securing data
5. Enforcing privacy policies
6. Application Security
7. Securing network connections
8. Physical security
9. Manage terms in cloud service agreement
10. Understanding security for exit process

III. Ten Step Process to Security [2]

A. Governance, risk and compliance processes

Organizations usually have set security and privacy procedures that are in place to protect the company's assets. The governance is put in place to ensure that the company's responsibilities, authority and communication are all set and clearly stated.

The risks in cloud computing are different that regular information technology environments due to the cloud being virtual and web-based. All the control of the cloud service is the service providers responsibility. The interfaces in-between the providers and the customers. As well as the rights to ownership of the data being stored, along with access rights to that data in the cloud.

There is a widely used international standard of compliance when it comes to the cloud which is ISO/IEC 27001. [3] "It ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts...". [3]

B. Audit operational and business processes

Cloud services need appropriate auditing to ensure that the security meets the expectations of the customer, these audits are the basis for customer assurance that everything within the providers service is properly controlled. The auditors can either be on the customer or providers side while maintaining an independent status.

These audits should be automated through a means of a standard access to the audits, so that ensure timing and remove human costs with processing. This can be done through various types of web applications or automated application programming interface.

C. User Privileges

Making sure the users of the cloud service have the matching verified authentication of access is one of the key factors of security. Such as only trusted employees should

have proper access to certain information that is store in the company's datacenter, everyone in the company doesn't need that authentication.

There needs to be a secured access management system that monitors all access to a service no matter the status level of the applicant logging on. With this in place the company will be able to tell if someone is on or has access who isn't supposed to. On top of the access management system there should be some sort of authentication of the person's identity to verify that the person is really who the person says they are. This can be achieved by adding a level of security to logging onto the service by some sort of dual-factor authentication.

D. Securing Data

Securing data is a huge deal in the IT world whether it be on a cloud-based service or not, it's all about making sure that the clients data is properly secured. There's many risks when thinking about data protection such as: data privacy, tampering with data, holding onto unnecessary data longer that the company needs (overcrowding), disclosure of data, and risk of losing data without access of regaining it.

Most protocols used for securing data is not new to the IT field, simply building on old techniques improving them over time. A couple data protection solutions that have been used over the years are: data isolation, encrypting proper elements, and controlling who has access to different data.

Customers are at more at stake when it comes to data protection, the cloud providers only can do so much when it isn't in their hands. The customers are responsible for making sure they set the right requirements and access control to make sure they do their part.

[20 pg.20]

E. Enforcing Privacy Policies

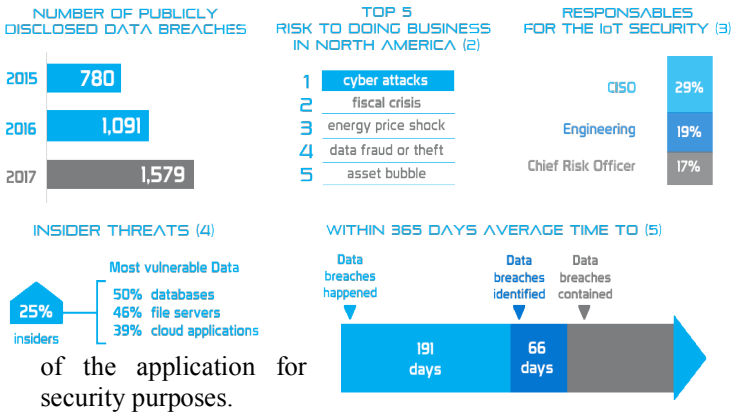
Privacy protection is rapidly growing all over the globe with laws and regulations being formed every year. Privacy policies meaning rules that are set within a company stating that personal won't be sharing, accessing, giving other people access etc. and if they do break any of the privacy policies than that person can be prosecuted in the proper ways. Some cases the person at fault will be prosecuted in a court of law.

Coming to privacy policies in a cloud service it becomes a little different. If data is being cross platformed by a third party that company is responsible for the security of that data and is liable for the same privacy policies that the owning company has. Making sure your firm has proper privacy policies can save a company from disaster and in some cases save individuals their jobs.

F. Application Security

Companies that rely on specific applications to run a majority of their daily jobs need to make sure that those applications have the proper security from outside threats as well as threats within the firm. A big security risk for most company's around the world are something as simple as spam emails which an employee clicks on and then the outside threat is in. Within a cloud-based server development of applications may not have all the same perks as an application built outside the cloud. There needs to be engineers that are capable of starting the build from the bottom, making sure not to use any outside templets and being able for the customers to lose some of their control of the application for security purposes.

[5]



G. Securing Network Connections

On a cloud-based service provider the network must be able to handle its network-based security, monitoring network traffic and to be able to block untrusted traffic. The network security needs to be able to stop attacks before they get into the company's network, being ready for attackers trying to break in with malicious mail or attempting a denial of service attack and shutting down the network. Some attacks that companies don't see are in the authentication pages, when someone is attempting to log in, in some cases that information can give away or lead to data spillage about other clients.

Again, a lot of these security risks rely on the customers doing their part. They need to know the internal network and the requirements for that network. Such as, making sure all cabling and virtual ports are secure and in correct place, VPN's are properly locked, and authentication is required to access.

H. Physical Security

The physical security is roughly the same all around the IT world. Basic security around and in the building assuring that everything and everyone are where and working as they should be, things like:

- Gate or fence around the perimeter keeping others out
- Security guards at the front of the building
- Fire protocols: fire extinguisher, fire escapes, proper fire proofing equipment in server rooms
- Protection against other weather threats, floods, hurricane (if necessary), and earthquakes
- Security cameras making sure nothing is stolen from the property
- Making sure old equipment is disposed of properly so there is no data that may be compromised
- Having the proper backup equipment in case of any of these emergencies

All of these physical security features may seem basic and redundant, but it the long run any of these could potentially save the company if there were a disaster.

I. Manage Terms in Cloud Service Agreement

There are always two sides to cloud computing no matter the case, the cloud user and the cloud provider. With that being the case there needs to be terms that need to be in place that specifies terms and initially create a contract between the two. This contract is put into place for the sole reason of reliability, if the provider gets breached or notices a breach in the system they are obligated to contact the client in a set period of time to inform them about the breach, no matter of significant of the breach.

After they inform the client of the breach the next step is to start the rebuild process if necessary. Start looking at the security measures (steps 1-8) to see if anything is reported missing, any suspicious activity recorded, or any breaches in the network. After they find and solve the situation at hand, they need fix it and then test the fix they did to ensure that it will not happen again.

If for any reason the provider lacks on informing the client about the breach, then the provider will be panelized for the incident. The agreement made between the client and provider has to be drawn up cleanly and fairly because it has a very important role.

J. Understanding Security For Exit Purposes

Preparing for the exit process of an employee. When an employee is terminated and has to begin the 'moving out' process and has been working with the cloud for his/her work, there needs to be an exit process that is safe and protected.

When an employee leaves they are going to need to be able to retrieve their data from the cloud and make sure that the data is deleted from their part of the cloud. Vice versa for the providers part as well, they are going to need to make sure there are no copies of that data anywhere on their side of the cloud, no backups, copies, anything.

After the employee leaves there is going to be a need for another privacy act, ensuring that since the ex-employee is no longer an active employee that the privacy act stays in play. For any information that is vital to the company's performance will need to stay confidential if necessary.

Once these steps have been completed and reviewed the employee will have safely had a clean exit.

K. The Length of Ten

As seen above the ten-step process to making sure a cloud-based service is secured is a long and lengthy process. If all of these processes are completed correctly the company at hand will have a strong and safe work environment for its employees to be working on.

IV. Future of Cloud Computing

A. Increase in Storage

Over the years of cloud computing no one can really predict the future of the cloud, we can only make predictions. As seen in the last years the complexity and size of storing data in the cloud has increased tremendously.

Therefor it is safe to assume that over the next couple years the storage size will increase allowing companies to store unbelievable amounts of data on the cloud provider.

[6]

B. Performance of the Internet

Going along side with the Internet of Things the internet is going to be growing rapidly with the help of cloud computing. We as daily internet users expect to have access to fast, high quality, and reliable internet access when we log on our computers. In the next couple years, we can expect to see this come true.

C. Modular Software

Software development is going to need to go places in the future due to the size and complexity of modern day programs becoming larger. Applications will be able to have been stored on a cloud-based server, reducing the price of software production.

D. Internet of Things & Cloud Computing

Over the internet there are an abundance of machines talking to each other, processing requests, and handling data. The Internet of Things helps speed up the process with real time Data Analytics through cloud computing.

E. Stats Show Future Changes

"The cloud computing market is growing at 22.8 percent and will exceed $127.5 after 2018. By 2018, 62% of all CRM software will be cloud-based. Moreover, 30% of all application spending is for software as a service-based applications". [6] As 2019 is coming to an end cloud-servers are more popular than ever, expanding at rapid rates.

F. Cloud Services Improving

Cloud-computing and the services being provided to clients is becoming easier to use and easily manageable. With easier use and user-friendly interfaces, it opens up to table to more company's. The cloud will be used for more than half of the workload.

G. Security

No matter what field of work we talk about there is always room to improve and handle security better. So future security in cloud services could be handling attacks more efficiently, stopping them sooner, building stronger firewalls etc.

H. Economic

With using cloud services will really limit the need for all the unnecessary hardware, saving company's money in

the long run. There's no need for replacement, repairs, and damages done to that said hardware, since it will be replaced by web-based services.

V. Conclusion

The use of cloud computing in today's world is just the beginning and will soon be seen everywhere. Therefor there is going to be a strong need of security making sure all of the data on those cloud services are strongly protected. Going through the processes of:

1. Governance, risk and compliance processes
2. Audit operational and business processes
3. User privileges
4. Securing data
5. Enforcing privacy policies
6. Application Security
7. Securing network connections
8. Physical security
9. Manage terms in cloud service agreement
10. Understanding security for exit process

We will be able to achieve a great foundation of ensuring that the cloud is as secure as we can make it. It is going to be fascinating to see where cloud computing takes us within the next decade.

References

[1] "What is cloud computing?" [Online]. Available: https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ Accessed: Dec. 5th, 2019.

[2] "10 steps to Securing Your Journey to the Cloud" [Online]. Available: https://blog.trendmicro.com/10-steps-to-securing-your-journey-to-the-cloud/ Accessed: Dec. 5th, 2019.

[3] "ISO/IEC 27001" [Online]. Available: https://www.iso27001security.com/html/27001.html Accessed: Dec. 5th, 2019.

[4] Picture from: https://www.google.com/search?q=cloud+computing&rlz=1C5CHFA_enUS710US713&source=lnms&tbm=isch&sa=X&ved=2ahUKEwijsK2Ui5_mAhXNUt8KHQcCBzcQ_AUoAnoECBMQBA&biw=1363&bih=798#imgrc=pavDuyGf4OWmaM:

[5] Picture from: https://www.google.com/search?q=application+security&rlz=1C5CHFA_enUS710US713&sxsrf=ACYBGNRbK-oQNQ-QKafKHbzCR7vk6c8W_A:1575580715653&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjI_fvGt5_mAhXpm-AKHWT6AIIQ_AUoAnoECBMQBA&biw=1363&bih=749&dpr=2#imgrc=eY95KEZJzlOJvM:

[6] "Future of Cloud Computing -7 Trends & Prediction about Cloud" [Online]. Available: https://data-flair.training/blogs/future-of-cloud-computing/ Accessed: Dec. 5th, 2019.