A Report on Cloud Security Analysis (Amazon Marketplace & iCloud)

Student ID: 1484052

Student Name: Sankha Subodha Palapotha Liyanage

Student ID: 1485971

Student Name: Jin Tae Kim

Course: ISCG 8047 (Cybersecurity & Cloud Computing)

Lecturer: Bahman Sarrafpour

Due Date: 15th April 2017

Introduction

Cloud Computing refers to a general term for service delivery over the internet through hosted servers; enabling the companies to reserve the services and use the resources as a utility. This includes Virtual Machines, Storage, Applications and provide companies multiple benefits. The end-users can manage workload on-demand; eliminating the requirement to maintain personnel managing computing resources. The scalability is a flexible factor at Cloud computing; where the company can scale the resources depending on demand fluctuation. The users are charged for the resources used during a specific time-period. The Cloud Computing became a widely available and popular worldwide with the growth of Internet and Telecommunications field. Companies are rapidly adopting cloud-computing services due to the features such as on-demand service, resource pooling ability, broad accessibility, measured and calculated services and available high scalable features. At present, most of the people using internet services use cloud services; as many service providers allow users to manipulate the basic functionality and features. Microsoft and Google are two services providing the Cloud-Storage service for free; computing resources are provided by multiple companies including Amazon Cloud Services, IBM, Microsoft Azure and Google Cloud Engine.

With all the above factors, Security of the cloud services are facing threats at a faster growing pace, where the hackers target personal and confidential data of the users. Considering the past few years, several incidents took place where the severity of some incidents were significantly high. The incidents include breaching financial data, private personal data and confidential data due to system weaknesses and vulnerabilities.

Abstract

The report focuses on two recent Cloud-related incidents and discusses in-detail about the incident, possible causes, preventive measures and response measures. The first incident is on Amazon Marketplace (subsidiary of Amazon Web Services) where the hackers gained control over the trader accounts. The second incident reviews the iCloud hack and possible threats posed on the system by hackers.

The report briefs the incidents and discusses about the vulnerabilities and weaknesses of the system. Depending on the incident analysis, hypotheses are built and relates all possible system weaknesses and vulnerabilities related to the scenario. Upon reviewing and hypothesizing, the system is analyzed for weaknesses and vulnerabilities. Depending on the analysis, Preventive Measures with ability to suppress the existing weaknesses are discussed. Response Measures are recorded which aid in mitigating the incident and helps reduce further damage caused to the system.

Keywords: Cloud-Security, Data Leaks, Vulnerability Exploitation, Cloud-Services

Table of Contents

Attack on Amazon Web Services

Incident

The online traders of Amazon Marketplace were attacked by hackers stealing money from their accounts; thousands of merchants are affected by this incident where several traders have lost thousands of dollars. The attack was initiated using the account details sold on the "Dark Web" from a previous hack carried on Amazon Services. (Mann, 2017) The attackers have gained control of the inactive merchant accounts and have posted fake products of non-existence and sold at a value significantly lesser than the current market value. The bank account details of the hacked accounts were changed in favor of the hackers; where the transactions were directly made to hacker's accounts. As Amazon withholds the seller payments until the customer receives the product, and the "full refund guarantee" policy of Amazon Inc. has made the traders lose money over products they never sold. Apart from hacking into dormant accounts and selling non-existent products, the bank account details of traders with a significant turnover were changed and the money from transactions were transferred to the hacker's accounts. Amazon has failed to take preventive measures upon reporting the incident by few traders; taking significant time to respond to events disappointing traders engaged with online trading activities. (Newcomb, 2017)

Amazon Cloud Services and architecture

Started by Jeff Bezos in 1994; the online-book store was registered under the name Amazon.com in 1995. Amazon expanded its services increasing the market-size and capturing different naïve markets. The kindle e-book reader was introduced in late November and this sky-rocketed the Amazon's revenue, thus enabling the company to expand further in the online trading market. Currently, Amazon provides multiple cloud-based services ranging from mobile to server-administration levels. The Amazon provide Cloud-based services popularly known as "AWS". AWS services include components from SaaS, PaaS and IaaS cloud-computing service models providing background for users to implement, deploy and develop while running applications within the cloud-service. some of the provided services are based on Public-Cloud deployment model and are open for public use. AWS provide on-demand computing resources and services for over 1 million clients and includes tech-giants Netflix, Alcatel, Adobe, Bitdefender, Citrix, etc. using the resources. Apple had several services related to iCloud running on AWS services before moving to Google Services in the latter part of 2016. AWS has mere limitations as the platform is built based on Unix kernel. (wikipedia, 2017), (AWSInc., 2017)

Hypothesis for reasons to attack

Information Security reviewers have multiple opinions regarding the incident, but Amazon being a reputable organization, still hasn't taken this breach seriously. Amazon take days to review the hacked accounts and once the problem is resolved, it is already being too late, the trader has almost lost everything. Depending on the scale and vastness of the incident, the security experts have hypothesized following incidents as the key factors regarding the incident.

- Dormant accounts left with active bank accounts, weak user passwords and failing to update them constantly.
- Amazon Web Services system vulnerabilities and User Identification Weaknesses.

Dormant accounts with active bank accounts

Amazon prompts the new user to enter the bank account details at the Amazon account setup instance and remains active if the account exists in the system. As some traders tend to carry out sales during a specific time of the year, (during new year, Christmas, etc.) their accounts remain active without a trader's attention. Hackers targeted the above accounts and sold non-existing items to the customers; where the sold item was marked at a value lesser 50% of the actual value of the item. as the initial step, the bank credentials in the account was switched to one of hacker's bank account and the delivery duration between 14 to 30 days was selected as Amazon withholds the payments to the sellers until the item gets delivered. After the shipping duration, the money is released by Amazon and the hackers got away with the money; swapping back the seller's bank credentials.

Use of weak passwords and failing to update them constantly

Considering the incident, the lack of frequent password changing mechanism has increased the vulnerability of the system. The hackers used credentials available on the black market from a previous data breach on Amazon services and exploited them to gain access to the accounts to carry out the attack. As Amazon allows the user to create a password of minimum 6 characters (not specifically mentioning Upper-case, Lower-case, Alphanumeric characters or symbols to be included), users tend to use weak passwords enabling the hackers to guess the password. It is a human weakness to keep the same password for all the social-media and social-security accounts. Hackers successfully exploited this weakness by trying combinations of username and passwords of the same user from different sources. The lack of a mechanism to constantly update the password has been identified as a system weakness. The only instance I have experienced with password change mechanism is with Sampath Bank (Sri Lanka) where they prompt the users to change their passwords every 3 months. Rarely, companies providing social-media or social-security services request the users to update their passwords; where hackers are given the chance to exploit a user account from data gained by other resources.

AWS System Vulnerabilities

After analyzing the sequence of events that took place, the following system weaknesses were detected.

No constant password update mechanism

The blame for the above breach cannot be directly pointed at users (sellers), but it is a responsibility of the system to protect the sellers (whom they make money from) from scams. The above discussed human error can be minimized by adding a frequent password update mechanism; which would indicate the importance and urge to change the password.

Weak incident handling and mitigating techniques

Considering the fact that the industries are profit-focused, the attacks, system breaches and vulnerabilities are hidden from the users. As Amazon provide services to leading tech-industries (Ex: Adobe, Netflix, Bitdefender, Samsung, Sony), the impact created by a data breach on one division would bounce back on other services as AWS components are centralized. If a vulnerability in one unit is exploited and the resource leakage can be catastrophic. The Amazon services lack a system to notify the users and prompt them to change passwords urgently in-case of a data beach incident. The support center has taken significant time to respond to the reported incidents regarding the malicious activity. This weakness has allowed the hackers to get away easily.

Weak user notification procedures

The account activity is notified to the user via email alerts; a procedure most of the companies follow. The notification method is effective only if the user is actively monitoring the emails. The user is not notified regarding unidentified logins or login attempts carried out on the seller account. The Amazon Marketplace login allows around 10 login attempts and afterwards, it combines with a Captcha puzzle for account security, but no account-lockdown procedure is detected. This weakness has allowed the hackers to try all possible combinations and guesses on the targeted victims' accounts.

User identification weaknesses.

The system lacks two-step authentication (which involves the combination of username and password alongside a confirmation PIN number or a combination of letters to the registered user mobile number). Apart, the system login doesn't involve a security question after a defined number of unsuccessful login attempts; but only verifies if the login attempts are carried out by a human with the aid of a captcha puzzle.

Preventive measures depending on the Hypothesis created

Analyzing the incident, assumptions and hypothesis were created. By applying the preventive measures, another similar situation could be avoided by minimizing the system vulnerabilities and weaknesses; thus, leading to a safer and secure system.

Prompt users to add strong passwords and use two-step authentication efficiently at system login

Considering the first hypothesis, a procedure to change login credentials frequently can be very effective. Strong passwords are hard to guess and take a significant time to crack. Considering the fact "Humans tend to forget easily", users are unwilling to change their passwords or change between a few selected passwords. Two-step authentication comes in handy during a recent system breach; where the user will require the authorization-code sent to the mobile to login to the account. This will create a secure environment for the users even a third party has login credentials of authorized users.

Temporarily disable inactive user accounts and re-enable them with two-step authentication.

Inactive traders faced the problem of non-existent product sale by hackers. By implementing a system to check the user activity and if a user is detected inactive for a significant time duration, the system can temporarily disable the account. This method will require the users to reactivate their account with two-step authentication followed by security questions; thus, making it hard for unauthorized users to gain control of the account.

Alert user using text messages on abnormal account behavior and allow user to remotely disable the account through a text-message code.

By integrating a system to monitor the account, changes and abnormalities can be detected where they can be notified to the user through a text message. As the present people carry their mobile phone with them, SMS alerts is a convenient method to notify crucial information regarding the account; rather than using the conventional e-mail alert system. The login attempts can be monitored; where an abnormal number might indicate an unauthorized user trying to gain control of the account. The login details can be stored for further reference (not valid for the case study as the hackers can spoof the IP address, MAC address and the location) and malicious activity can be prevented if the user is provided with control over the account. Implementing a system to allow the user to remotely disable the account with a simple text-message code would prevent a catastrophic financial loss to the user.

Response Measures

Considering the incident, multiple hypotheses were built and preventive measures were discussed above. Responsive measures mitigate the incident and helps in reducing further damage preventing exploitation of the weakness. The following key-points are identified as the response measures for the given incident.

Patch the system vulnerabilities and further test for similar vulnerabilities.

The vulnerabilities exploited can be mitigated by changing the system authentication structure; but this takes a significant time. The following are the best practices to be followed until the system security is assured.

Inform users regarding the system weakness and prompt to change login credentials

The companies do not like to expose their system weaknesses to the customers, but alerts regarding the ongoing incident will have the users prepared. Hackers gain control over user accounts through data dumps available on black-market. These data are made available by hackers who hack into servers with vulnerabilities by running exploits. Prompting the users to change the login credentials will secure their accounts as the hackers use credentials from a previous data dump.

Inform traders (users) to be vigilante on the list of items sold

The hackers exploit the dormant accounts by selling non-existent products for a lesser value than the existing market value. By alerting the users to be vigilante on their list of products, the hackers have a minimal chance to add or edit the items to be sold as the users will be notified with their account changes. This measure will allow the user to monitor their account activity and disable the bank account before further financial damage if the account has been hijacked (the hacker can change the existing password disabling user access to the account).

Faster response from Amazon team.

According to the online trader Dennis after reporting the incident, Amazon’s response regarding the incident was “We received a notice and we’ll get back to you when we get back to you. We can’t tell you when or if”. The above response has disappointed traders, some leaving Amazon Marketplace. The account-credential reset has taken days to take down her account; where the hacker has got away with the money for the transactions made. Considering the above facts, a faster response from Amazon team can minimize the damage happening to the merchants. As traders’ activity bring Amazon business in multiple ways, their issues should be prioritized; specially during a security breach incident.

Guarantee money-back for the traders

Amazon provides buyer protection by reimbursing the whole payment if they don’t receive the ordered product. This policy hooks up the traders to fully-refund the customers; in this case, for non-existent items that were sold ripping off the traders. However, Amazon has not guaranteed refund the traders, but Amazon spokesperson Erik Fairleigh has informed “is constantly innovating on-behalf of customers and sellers to ensure their information is secure and that they can buy and sell with confidence on Amazon.com”.

References: (Dunn, 2017), (D'Onfro, 2017), (Dones, 2017) (Dunn J. E., 2017)

Apple iCloud hack threat

Incident

On March 2017, Apple Inc. received threats from a group of hackers who wanted ransom from the company threatening to delete millions of customer data from iPhones, Macs, and iPads if the company fails to pay the demanded ransomware. The London-based hacker group dubbed ‘Turkish Crime Family’ threatened to hack into the company’s customers accounts and erase all the information stored there unless Apple agrees to pay them a ransom in Bitcoin (Whittaker, 2017). The hacker groups claim to have access to over 250 million accounts of Apple customers and were threatening to reset their passwords remotely if the company fails to comply with their ransom demands. The hacker group approached some outlets so as to emphasize their extortion efforts and as Motherboard reported, the hacker group gave Apple Inc. an ultimatum deadline. It was claimed that the hackers did not directly access the customers’ information by hacking Apple’s iCloud, but rather got that information from other services and websites.

The ‘Turkish Crime Family’ further cited that Apple should pay them $150,000 in Bitcoin or Ethereum. The hacker group was believed to have accessed about 627 million accounts from iCloud.com, mac.com and me.com. However, Apple denied the security breach and argued that the iCloud information might have been acquired from previous hacking events that affected firms such as Yahoo (Whittaker, 2017). The company also advised the iCloud users to change their passwords to reduce their chances of being exposed to the said security breach. Additionally, Apple spokesperson told Fortune that the company is keenly monitoring iCloud so as to prevent unauthorized users from accessing user accounts and was working with relevant law enforcement agencies to identify the people involved (Whittaker, 2017). The company further encouraged the iCloud users to use the two-factor authentication approach protect their accounts from authorized and malicious users.

Possible causes of Apple iCloud hack threat

Although Apple Inc. denied the allegation that their iCloud server had been hacked by the Turkish Crime Family, some tangible evidence that tries to support the hacker’s claims are available. The iCloud user’s credentials had been remotely accessed without the knowledge of the company. The access was through other means which linked to a vulnerability of the company’s iCloud server. Although the hackers were working on the recycled public data to authenticate their claims of the iCloud data breach, it has been confirmed by other security investigative bodies that the attack could have possibly occurred. Over 70,000 user passwords showed a match in the database of the previous leaks (Whittaker, 2017). This indicates that there was a possibility the hackers had gained access to the critical data of the company users and their threat was serious. Some of the possible causes include the following.

Vulnerability created from previous database attack leaks

The previously hacked databases of users of companies such as LinkedIn provided a loophole the hackers used to launch their data break threat on Apple iCloud database. Since most of the users often have similar passwords they use on other platforms, it makes it easy for the attacker to launch attack claims. When the incident occurred, there was a confirmation that over 70,000 iCloud user passwords had about 99% match in other previously hacked databases. Such a match could make these users more vulnerable to other attacks, and the company has confirmed the system weakness. On the same note, Apple was skeptical on the claim that its iCloud database had been hacked and 556 million of its iCloud users were at risk of losing their valuable data as a result of the incidence (Whittaker, 2017). The company also confirmed that although the claim had not been verified, there was a possibility for the hackers to take advantage of the vulnerabilities exploited from previously hacked accounts.

Data leaks

Although cloud computing databases are considered some of the most secured databases currently available, these databases are prone to data leaks just like any other database a company can have. It is more susceptible to internet based threats since it is remotely monitored by a third party and not the company itself. Apple considers its database as some of the most secured databases in the planet but the possibility of data leaks from the company database may be true, and this might have been the cause of the hacking threat. The attackers may have targeted the networking interfaces enabling them to capture the network traffic within the iCloud database enhancing their exploit (Brandom, 2017). Companies must be able to protect their users from such kind of attacks preferably by using SSL or TLS encrypted communication platforms.

Sub-standard cryptographic key management systems

Attackers can take advantage of the company’s inability to store their database encryption keys thus allowing them to gain access to the company’s database. In light of the iCloud hack threat, Apple could have possibly messed in storing its database encryption keys that would probably enable the hackers to gain access to the iCloud user’s accounts in the company’s databases (Brandom, 2017). The attackers often look for any form of vulnerability within the business, and once they identify a potential vulnerability, they take advantage of the weakness and launch an attack on the company's database.

Under-deployed two-factor authentication

Cloud databases are considered some of the most convenient and secure databases currently available in most companies. It allows users to access their data or information from anywhere with the face of the planet and from any device. These databases are prime targets for hackers today than ever before. Attackers often take advantage of the vulnerability created by either the company or the third-party database managers (Rhodes-Ousley, 2013). Since iCloud is entirely run and managed by Apple, the company might have under-deployed their user two-factor authentication security techniques which could restrict access to cloud-based data for the company.

Preventive measures

Proposed preventive measure for vulnerability created from previous database attack leaks

Vulnerability created from the previous data breaches may impact negatively on the company's database since it provides a loophole through which the hackers may crack into the database. Since this type of attack occur as a result of the use of single password for multiple accounts, the following are some of the most effective preventive measures the company can take to protect its users (Whittaker, 2017).

Prompt users to use strong passwords

Prompting users to have strong passwords that cannot be accessed by attackers and consider having different passwords for different accounts. Users should not have same passwords for multiple accounts since the attackers may use same passwords of the previously hacked accounts to launch an attack on accounts. In credential stuffing, attackers take advantage of users who use same passwords to access other multiple accounts. The company should advise their users to consider deploying different passwords in any case they have other online accounts.

Use Two-factor authentication

Two factor authentication and password encryption would also help prevent the occurrence of the attack on database. Two-factor authentications provide maximum security of account passwords making it hard for the attackers to launch an attack on the databases of the company. Most vulnerability exploits occur as a result of weak passwords and lack of two-factor encryption; allowing the attacker to launch an attack on the database easily.

Residual risk

Although two-factor authentications are some of the immediate response to prevent further occurrence of the incidence, the major risk to this response is that it can be vulnerable to the network based man-in-the-middle attack. This may include fraudulent cryptographic certificates. This certificate may be injected into the company's trusted certificate database; thus, compromising the listed root certificates allowing the attacker an easy access to the database.

Proposed preventive measure for data leaks

Avoiding data leaks require the company to consider deploying security mechanisms within its database infrastructure. The following are some of the most efficient ways of preventing data leak vulnerability.

SSL and TLS encrypted communication

The two mechanisms are cryptographic protocols which enhance communication security within a computer network. Secure Socket Layer and Transport Layer Security improves data security by establishing encryption link between the client and the server. The two techniques also encompass conventional symmetric cryptography that enhances the encryption of data transmitted over a communication link. Therefore, making it impossible for the attackers to launch their attack on the database as the communication between the client and the server is secured and encrypted.

Deploying endpoint security

Endpoint security through a secure connection is essential in enhancing database security within the company. Apple should consider strengthening their endpoint security protection by ensuring that the entire login is secured and remote control and authentication monitoring are deployed; which will further enhance 'data-security' factor of the company

Residual risk

The main risk associated with the two responses is the danger of the man in the browser attacks which usually occur where the attacker can mimic the user's display browser making the user think everything is secured, but in the real sense, the attacker is stealing the data from the user.

Proposed preventive measure for sub-standard cryptographic key management systems

Within the context of the cryptosystem, cryptographic key management is essential for enhancing data security. The following are some of the most effective preventive measures in the case of substandard cryptographic key management strategies.

Redesigning cryptographic protocol

Apple should consider redesigning its cryptographic protocol and user procedures so as to enhance data security. On the same note, cryptographic keys, critical servers, and login protocols should be monitored and improved to adequately provide database security for the company (Rhodes-Ousley, 2013). Attackers often look for the companies with stored cryptographic keys, where they can exploit the system and access the database of the company creating a loss to the company.

Key management solution

This is one of the most important approaches for managing cryptographic keys under different conditions under the machine to machine communication. Deploying efficient key management solutions allow the company to effectively keep itself out of the attack; where the keys are well stored and managed within the company.

Residual Risk

The main risks associated with database encryption as an effective response to attack threats. Considering the infected company applications that have legitimate iCloud database access rights could still access the databases infecting the company’s confidential data. (Brandom, 2017). Moreover, super-users and malicious insiders with unlimited access rights can exploit the security protocols and disable encryption security controls rendering the database vulnerable to the attackers.

Proposed preventive measure under-deployed two-factor authentication

Two-factor authentication is critical, and is one of the most reliable methods for enhancing the security of the databases by restricting unauthorized access to the database. To fully deploy two-factor authentications the following procedures has to be followed.

1. Encourage access to the database information using dual-factor authentications by users. Making dual factor authentications a mandatory requirement among users. This step will help protect both users and the company from malicious attacks (Ousley, 2013). Apple should consider restricting access to its iCloud database by implementing the efficient use of dual factor authentication.

2. Making dual factor access authentication a mandatory step when setting the remote passwords and other account passwords for their iCloud data.

Residual risk

One-time passwords in the form of two-factor authentication may not be quite effective in providing access security since they can be disabled in the company network. Once the two-factor authentication has been disabled, it becomes tough to detect any form of unauthorized access.

Responsive measures

It is important for the company to develop a response plan in cases of security violation or an attack threat. Having a proper response plan will enable the company to response more effectively and help mitigate the damage caused by the data breach. Apple is one of the biggest and most respected companies in the world and as such, the company should be able to create a response plan to help mitigate incidence of attack on the company's important infrastructure. Effective response will enable the company to fix the various flaws that may occur as a result of the attack. This will help the company to identify other vulnerabilities that may exist within the information technology infrastructure. The following are some of the possible response measures that Apple can opt to take.

Providing immediate notification whenever there is suspicious login to iCloud user account from an unrecognized web-browser. By notifying this to the user, he will be able to have an eye on the account login activity.

Enhancing the use of two factor authentication. As discussed above, implementing two-factor authentication will provided added security to the account. By combining finger-print scan feature, this step can provide significantly easy-use to the user and added security to the account.

By enhancing the user notification during data restoration provides added functionality to the user as he/she has the ability to monitor their own account activity within the company's iCloud database.

As suggested, by implementing encryption algorithms and strengthening the processes used will provide hard-to crack, unique procedures for encrypted data and cryptographic keys.

By implementing Intrusion Detection and Intrusion Detection Systems within the database will provide added security for the users; thus, enabling the system administrators to monitor the account activities efficiently and with ease.

Conclusion

By analyzing the reports, the incidents occur due to vulnerabilities and weaknesses in the systems. We can conclude the incidents in cloud services can be avoided if the systems were tested for vulnerabilities by penetration testing. As cloud services are widely used, the security is a major factor and following best practices and mitigation techniques can reduce the impact on user data. The security must be considered from two aspects; from server-end and client-end. The client has the responsibility of maintaining secure passwords and keep track of the account for malicious behavior. The server management has the responsibility to maintain the security and monitor user-accounts for malicious behavior. The preventive measures can be followed to tighten the server security and prevent vulnerability exploitation by malicious users. The response measures can be followed in case of a data breach; which will minimize the impact on confidential data and prevent further exploitation of the weakness. By maintaining cooperation between the service provider and users, an incident can be easily detected and mitigated with minimal damage.

References

AWSInc. (2017, May 26). *Amazon Web Services (AWS) - Cloud Computing Services*. Retrieved from Amazon Web Services, Inc: https://aws.amazon.com

Dones, J. (2017, May 28). *Amazon.com's Third-Party Sellers Hit By Hackers*. Retrieved from Fox Business: http://www.foxbusiness.com/markets/2017/04/10/amazon-coms-third-party-sellers-hit-by-hackers.html

D'Onfro, J. (2017, May 28). *Amazon account hijacking: how to defend yourself against fraudsters*. Retrieved from Techworld: http://www.techworld.com/security/amazon-account-hijacking-how-defend-yourself-against-fraudsters-3644152/

Dunn, J. (2017, May 25). *Amazon account hijacking: how to defend yourself against fraudsters*. Retrieved from Techworld: http://www.techworld.com/security/amazon-account-hijacking-how-defend-yourself-against-fraudsters-3644152/

Dunn, J. E. (2017, May 29). *Watch out for fraudsters attacking Amazon Marketplace accounts*. Retrieved from Naked Security: https://nakedsecurity.sophos.com/2017/04/19/watch-out-for-fraudsters-attacking-amazon-marketplace-accounts/

Mann, S. (2017, May 24). *Amazon Scammers Are Using This Trick to Make Millions*. Retrieved from Inc.com: https://www.inc.com/sonya-mann/amazon-fraud-scam-sellers.html

Newcomb, A. (2017, May 24). *Hackers are using a simple method to rip off Amazon sellers.* Retrieved from NBC News: http://www.nbcnews.com/tech/tech-news/amazon-s-third-party-sellers-get-ripped-hackers-n744741

wikipedia. (2017, May 25). *Amazon Web Services*. Retrieved from En.wikipedia.org: https://en.wikipedia.org/wiki/Amazon_Web_Services

Brandom, R. (2017). Hackers promised an iCloud apocalypse — but probably can't deliver. The Verge. Retrieved 6 June 2017, from https://www.theverge.com/2017/3/28/15092076/apple-icloud-hacking-threats-turkish-crime-family-credential-stuffing

Chandrashekhar, A. M., Ahmead, S. T., & Rahul, N. (2015). Analysis of Security Threats to Database Storage Systems. International Journal of Advanced Research in data mining and Cloud computing (IJARDC), 3(5).

Chou, T. S. (2013). Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3), 79.

Hackett, R. (2017). Apple Responds to Hacker's Threat to Wipe Millions of iPhones. Fortune.com. Retrieved 6 June 2017, from http://fortune.com/2017/03/22/apple-iphone-hacker-ransom/

Rhodes-Ousley, M. (2013). Information security the complete reference. McGraw Hill Professional.