International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Anatomy of Data Breaches and Its Impact on Security

Anshu[1], Monika Sharma[2]

[1]M.Tech Scholar, Computer Science Department, TIT & S, Bhiwani, India
[2]Assistant Professor, Information Technology Department, TIT & S, Bhiwani, India

Abstract: ***In cloud computing, the word cloud is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services - such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet [14]. Every user access cloud services through internet without knowing the security aspects. Today security threats are increasing rapidly and data breach is top of them. Breach in the security of any component in the cloud can be both disaster for the organization and the provider. In this research paper we focus on main security issue in cloud like data breach, different forms of data breaches and how it occurs in cloud. It also explore where major breaches occur in cloud in past years.***

Keywords: cloud, data breaches, security

1. Data Breaches

The term data breach means when an unauthorized user or hacker or an attacker attacks an authorized data, access or retrieves it by an individual or service without the permission. A data breach results in loss of sensitive, protective or confidential data.

A data breach is also known as a data spill or data leak. [1]. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

A single breach can cause significant loss. In cloud computing data breach is the major security problem today. In the year 2013 cloud security alliance conducted a survey and come up with the result that data breaches is the top vulnerability in the cloud.

There are many different ways by which data breach can occur. Some of common causes are described below:

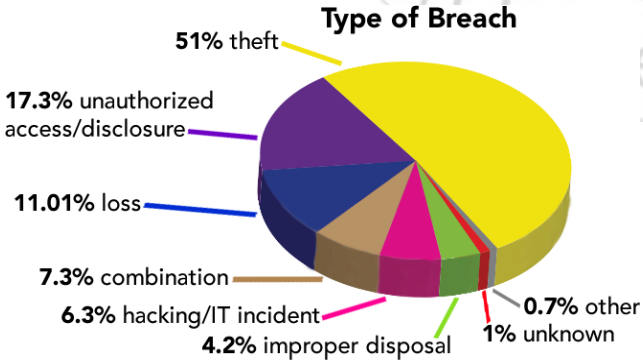

Figure 1: Types of breaches

1) Physical loss: When someone stolen your laptop, external hard disk or flash drive. The data in those can be stolen or attacker might corrupt that data.
2) Insider threat: Insider threat means within your organization or your any close friend. So the phrase "keep your friends close, and your enemies closer" could not be more relevant [2]. It is broadly divided into two categories i.e. accidental breach or intentional breach
   a) Accidental breach: also called as employee error when an employee by mistake sends data to wrong receipts, and by not understanding security protocols and procedures.
   b) Intentional breach: when employee misuses its power and sends secrete data to unauthorized person.
3) Weak security control: it occurs due to many reasons like- organization has less security policy or the user has weak password are some of weak security controls.
4) Malicious attack: it is an attempt to forcefully abuse or take advantage of someone's computer, whether through computer viruses, social engineering, phishing, or other types of social engineering. The top attack method used were:

a) Malware
b) Hacking

1. How Data Breaches Occur:

A typical data breach occurs in three phases:

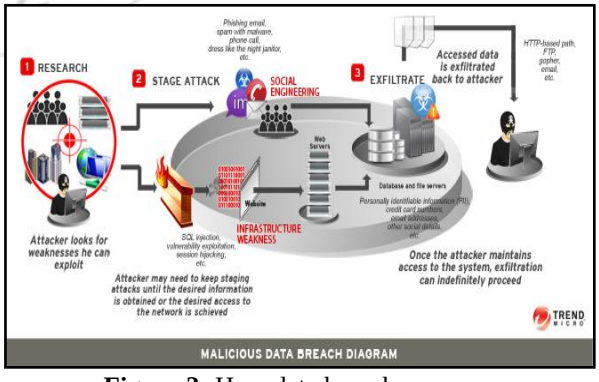

Figure 2: How data breaches occurs

Phase 1: Research

The attacker tries to find out the security weakness of the organization. The target could be any person or any organization.

Phase 2: Attack

When attacker finds out the target person/organization weakness next step is to attack it. Now the attack could be network based or social attack.

a) Network based attack: the attacker uses the weaknesses in the target's infrastructure to get into its network. These weaknesses may include (not limited to) SQL injection, vulnerability exploitation, and/or session hijacking.
b) Social attack: the attacker uses social engineering in order to infiltrate the target's network. This may involve a maliciously-crafted email to one of the employees, tailor-made to catch that specific employee's attention. The mail could be a phishing mail, where the reader is fooled into supplying personal information to the sender, or one that comes with attached malware set to execute once accessed.[3]

Phase 3: Exfiltrate

When the attack is successful it allows the attacker to exfiltrate. The attacker extracts and transmits data back to him. This data can be proprietary or sensitive in nature or can comprise credentials that he may need for another attack or to get higher privileges inside his target's network. [4]

2. Previous Year Record of Data Breaches

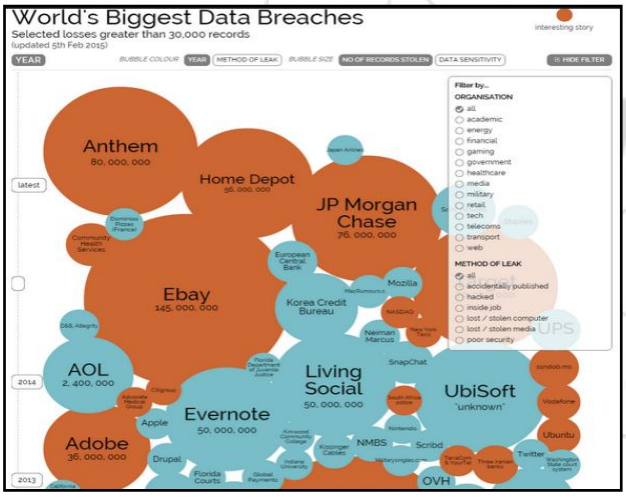

Figure 3: Record of data breaches [13]

4.1 Year 2010

1) AT&T Server/Apple iPad Emails: 114,000 Records Breached

An AT&T security breach exposed at least 114,000 e-mail addresses of iPad 3G customers, including those of high ranking government and military officials. The breach is done by a group of hackers, known as Goatse Security, by exploiting a security flaw on an AT&T Web application that enabled them to obtain a list of customer e-mail addresses in exchange for a personal ID, known as the ICC-ID by running an automated script.

2) Millennium Medical Management Resources: 180,111 Records Breached

Data is breached from MMMR, which handles billing for emergency health care physicians. Data is stolen from portable hard drive which contains patient's records from 2003 to 2006. It included names, diagnosis, medical records, Social Security numbers and health insurance information.

3) U.S. Army Reservists, Serco: 207,000 Records Breached

A laptop stolen from a government contractor in May contained the names, addresses and Social Security numbers for more than 207,000 U.S. Army reservists and their dependents.

4) AvMed Health Plans: 1.2 Million Records Breached

AvMed Health Plans and its clients became victims of a massive data breach when the theft of two company laptops compromised the information of as many as 1.2 million Floridians with Avmed Health Insurance, including current and former subscribers and their dependents. The personal data included names, addresses, phone numbers, Social Security numbers and other protected health information.

4.2 Year 2011

1) Sony

Sony suffered over a dozen data breaches, stemming from attacks that compromised Sony PlayStation Network, Sony Online Entertainment, and Sony Pictures, among other Sony-owned websites[5]. Sony customers are now at risk from attackers using the stolen password data to access their accounts on other sites.

2) Epsilon

It is a cloud-based email service provider, which fell to a spear-phishing attack. The breach affected data from 75 of Epsilon's clients. Conservative estimates are that 60 million customer emails addresses were breached.

3) RSA

One of the most high-profile breaches of 2011 didn't involve consumer information, but rather one of the world's most-used two-factor authentication systems [6]. After attackers breached the systems of EMC's RSA in April, stealing information relating to its SecurID system.

4) Sutter Physicians Services

Data from both Sutter Physicians Services and Sutter Medical Foundation was breached in November when a thief stole a desktop computer from the organization, which contained about 3.3 million patients' medical details--including name, address, phone number, email address and health insurance plan name--stored in

encrypted format. "The security lapse occurred on two levels: both the data itself (being unencrypted) and the physical location (stored in an unsecure location)[7].

5) Tricare and SAIC

In September, backup tapes containing SAIC (Science Applications International Corporation) data were stolen from the car of a Tricare employee. The breach led to a $4.9 billion lawsuit being filed, which aims to award $1,000 to each of the 5.1 million people affected by the breach. "The Tricare/SAIC breach is significant because not only are the victims at risk of medical identity theft, but financial identity theft as well.

4.3 Year 2012

1) University Of North Carlolina

The data benchers stole bank accounts and social security numbers for roughly 350,000 students, staff and faculty members. This is occurred, due to misconfigured security settings.

2) LinkedIn

Social networking powerhouse, LinkedIn, was tapped for approximately 6.5 million unsalted SHA-1 hashed passwords posted to the Internet. Even also the hackers published them publicly in order to use the buddy system.

3) Yahoo

More than 400,000 plaintext passwords were lifted from Yahoo and subsequently posted on the Internet. While most of the passwords seem to have been taken from the Yahoo voice services.

4) Global Payments: $84.4 million data breached

Credit card processor Global Payments at the end of March disclosed a breach that exposed 1.5 million consumers to fraud. The breach, which was under scrutiny by federal investigators, exposed credit card numbers, user PINs and other data but not credit card holders' names, addresses or social security numbers.

4.4 Year 2013

1) Zendesk Breach

Zendesk, which provides customer support messages to users of Twitter, Tumblr and Pinterest, announced a data breach in February that impacted its clients. The breach exposed thousands of email addresses and support messages from users of the services.

2) Twitter Breach

Twitter recently rolled out support for two-factor authentication to bolster the security of its user base [11]. Attacker exposed the usernames, email addresses and encrypted passwords of 250,000 users.

3) Vendini ticketing

Hackers focused last spring on breaking into the Vendini ticketing system in use by various organizations in order to steal customer financial data.

4) Piedmont HealthCare

Social Security numbers, on 10,000 job applicants was stolen due to a hacker and at the same time, Presbyterian Anesthesia Associates there disclosed a hacker apparently exploited a vulnerability flaw in its website to gain access to a database of information on about 10,000 patients who had their credit-card information stolen.

4.5 Year 2014

1) Social media giants Facebook, LinkedIn, among others, get hacked…repeatedly.

Twitter, Pinterest and Tumblr inadvertently suffered a breach after their customer service provider, Zendesk, got hacked [10]. No passwords were compromised but thousands of user emails were obtained and likely would have been used in email phishing scams to get more personal information.

Hackers stole usernames and passwords for nearly 2 million accounts at Facebook, Google, Yahoo, LinkedIn, Twitter and 93,000 other websites. That breach was a result of malware installed on user computers that swiped log-in credentials for thousands of sites for over a month. Facebook accounts were compromised the most, followed by Google, including Gmail and YouTube.

2) Nearly 40 million Target customers' credit and debit card numbers were stolen in midst of holiday shopping rush.

Cyber-thieves stole Target store shoppers' credit card numbers and debit card PINs—the four-digit number used to access bank accounts[9].

3) Adobe breach snowballs into multi-network security risk.

Adobe reported that 3 million customers' credit card information was stolen. A source code leak also exposed almost 40 million user emails and passwords [8]. But the breach's affect spanned beyond Adobe's Photoshop users.

4) System bug exposes 6 million Facebook users' personal data in yearlong breach.

Facebook said the leaks, which began in 2012, were the result of a technical glitch that was corrected in June.

4.6 Year 2015

1) Anthem Inc

The nation's second largest health insurer disclosed that hackers had broken into its servers and stolen Social

Security numbers and other personal data from all of its business lines. Given the company's size, this breach could end up impacting tens of millions of Americans.

2. Conclusion

With the immense growth in the popularity of cloud computing security have become important concerns. The objective of this paper is to understand how and what type of data breaches occurs in cloud. In this paper we also discuss how the organization affects from these data breaches. Future work will include the prevention against these data breaches.

References

[1] Definition - What does Data Breach mean
[2] http://www.oriontech.com/wp-content/uploads/2015/02/Orion_LogoMark-Favicon.png
[3] Most Common Causes of Data Breaches - Orion Blog.htm
[4] Data Breach - Definition - Trend Micro USA.htm
[5] Anatomy of a Data Breach - Threat Encyclopedia - Trend Micro USA.htm
[6] http://www.informationweek.com/news/security/client/230500044
[7] http://www.informationweek.com/news/security/attacks/229301337
[8] http://www.informationweek.com/news/security/government/229700300
[9] http://bits.blogs.nytimes.com/2013/11/12/adobe-breach-inadvertently-tied-to-other-accounts/
[10] http://thinkprogress.org/economy/2013/12/23/3101291/target-breach-highlights-lack-uniform-consumer-protections/
[11] http://newsfeed.time.com/2013/12/13/youve-made-it-your-leaked-linkedin-password-is-now-hanging-in-n-art-gallery/
[12] https://blog.twitter.com/2013/keeping-our-users-secure
[13] Worst Data Breaches - The Court Ventures hack of 2012 appears to be the biggest hack in history, in terms of number of records stolen."
[14] http://en.wikipedia.org/wiki/Cloud_computing