ASH1925012M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:12AM (UTC-0500)
Submission ID: 1782981930
File name: ASH1925012M.pdf (188.29K)
Word count: 2912
Character count: 15251

The most enormous cases of a data breach in the twenty-first century

Joy Bhowmik
ASH1925012M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

an exemplar report.

Abstract

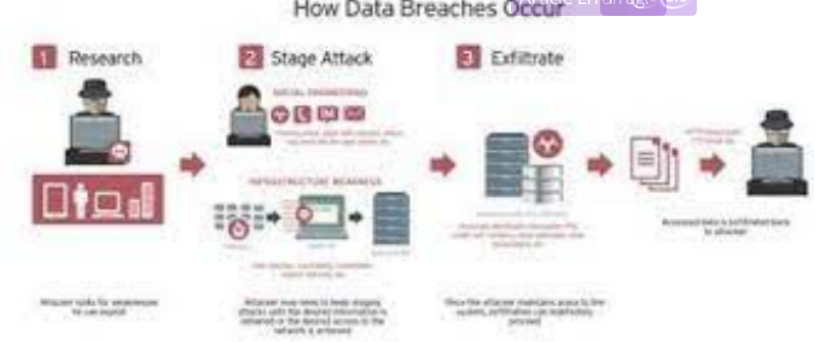
A data breach occurs when information is stolen or removed from a system without the owner's knowledge or permission. Various sensitive information like credit card numbers, client data, trade secrets, and national security information etc. might be stolen during a data breach. A data breach can result in reputation harm to the target firm.If associated records are taken, victims and their clients may face financial consequences.

1 Introduction

A data breach is defined as the detection of protected data leakage from a secure region to a non-secure place. This might happen owing to a database or program's security design flaws, purposeful database hacking, failure to integrate a secure application with insecure application components, and so on. A data breach is an urgent security event and it is important to find a solution to repair the breach as soon as feasible. A data breach includes several phases which are given as follows:

1. Research: After deciding on a target, the attacker searches for flaws in the target's people, systems, or network. This requires the attacker to conduct extensive investigation, which might include monitoring workers' social media profiles to learn about the company's infrastructure.

Figure 1: Phases of data breach.



2. Attack: After scouting a target's vulnerabilities, the attacker initiates contact via a network-based or social assault.

   In a network-based assault, the attacker takes advantage of flaws in the target's infrastructure to launch an attack. SQL injection, vulnerability exploitation, and/or session hijacking are just a few examples of these flaws.

   In a social assault, the attacker infiltrates the target network through social engineering techniques. This might be a maliciously constructed email sent to an employee, specifically tailored to capture the person's attention. The email might be phishing for information, tricking the recipient into providing personal information to the sender, or it could contain a malware attachment that executes when opened.

3. Exfiltrate: The attacker is free to harvest data from the company's network once inside the network. This information might be exploited for extortion. An attacker can utilize the information he gathers to carry out more severe attacks on the target's infrastructure.

2 Background

As organizations of all sizes become more reliant on digital data, cloud computing, and employee mobility, data breaches have gotten a lot of attention. Breaching a company's data has become as simple – or as complicated – as obtaining access to restricted networks, thanks to sensitive corporate data housed on local PCs, cloud servers enterprise databases.

Companies did not start keeping their secured data online when data breaches occurred. Data breaches have existed for as long as people and businesses have stored personal information and kept records. Prior to the widespread adoption of computers, a data breach might be as easy as reading an individual's medical records without permission or coming across touchy files that had now no longer been properly disposed of. Nonetheless, publicly revealed data breaches became more common in the 1980s, and public awareness of the risk of data breaches began to develop in the 1990s and early 2000s.

HIPAA and the PCI Data Security Standard, for example, were designed to set requirements for businesses and organizations managing specific types of sensitive consumer data. These guidelines establish a foundation for the needed protections, storage, and usage procedures for sensitive information, but they do not apply to all industries, and they do not guarantee that data breaches will not occur.

The majority of data breach information focuses on the years 2005 through now. This is partly due to technological advancements and the global expansion of electronic data, making data breaches a major worry for both businesses and individuals. Data breaches nowadays may affect hundreds of thousands – if not millions – of individual consumers, as well as many more individual records, all as a result of a single attack on a single organization.

3 Some methods of data breach

There are many methods of occurring a data breach. Some common strategies of data breaches are given below:

- Hacking: Because particular assaults are typically required, it's no wonder that unlawful hacking is the main supply of statistics breaches. Malware and SQL injection, for example, is usually best feasible whilst a crook has to get entry to a company's network. The wide range of actions that illegal hacking involves may surprise you. Although it's normally linked with computer programming, Verizon discovered that stolen credentials were the most prevalent illegal hacking tactic.
- Error caused by humans: Breaches aren't always the result of nefarious behavior. According to Verizon, a staff error caused more than one out of every five instances. Sensitive material was delivered to the wrong individual, which was the most prevalent mistake. Sending an email to the incorrect person,

attaching the wrong document, or providing a physical file to someone who shouldn't have access to it are all examples of this.

- Leak of information by an insider: In this method data is stolen by a trusted individual or a person of authority with access credentials.
- Social engineering: According to Verizon's analysis, about a quarter of data breaches are the result of fraudsters just appearing as if they belong.You've definitely heard of phishing, which involves cyber thieves sending malicious emails that appear to be legal, but Verizon also warned of financial pretexting.Pretexting is similar to phishing in that it involves criminals contacting their targets under false pretenses in order to get their personal information (financial information).Pretexters, on the other hand, approach victims by phone as well as email, and instead of copying a real organization's website, they simply ask for the target's financial information.Once they obtain the information, the criminals can conduct fraud, sell the data, or request information about the victim's account history from a third party (such as the victim's bank or a supplier that the victim's company uses).

4 Top cases of data breach in the twenty-first century

- Yahoo(August 2013)

  The event, that passed off in 2013, become 1st in public determined via way of means of the company in December 2016. it clearly become in the interior of being sold via way of means of Verizon on the time, and it clearly become concept that a hacker gang had acquired the account info of over one billion of its subscribers. Yahoo express however a year later that the actual variety of consumer bills uncovered become 3 billion. Yahoo equal the updated estimate didn't constitute a logo new "safety concern" which it clearly become causing emails to all or any "affected consumer bills." In spite of the attack, the Verizon deal become completed, albeit at a decrease price. "Verizon is dedicated to the nice stages of obligation and openness, and we proactively get to make certain the safety and safety of our customers and networks in an exceptionally dynamic global of cyber threats," Verizon's CISO Chandra McMahon express on the time. Our funding in Yahoo lets in the company to retain taking essential safety precautions while conjointly making the maximum of Verizon's facts and resources." while the attackers received get right of entry to to account facts like safety queries and solutions and plaintext passwords, price card and financial institution expertise wasn't acquired, in step with the investigation.

- Alibaba(November 2019)

  Using crawler software that he invented, a developer working for an affiliate marketer harvested consumer data from Alibaba's Chinese shopping website,

Taobao, over an eight-month period, including usernames and cellphone numbers. Although each were sentenced to 3 years in jail, it seems that the developer and his employer were gathering information for their personal use rather than selling it on the black market.

- LinekIn(June 2021)

  In June 2021, facts related with seven-hundred million LinkedIn individuals became launched on a dark web site, affecting more than 90% of the company's user base. Data scraping strategies have been used by a hacker recognized as "God User," who exploited the site's (and others') API earlier than liberating a primary facts series of approximately 500 million consumers. While LinkedIn claimed that the incident turned into a contravention of its phrases of carrier instead of a statistics breach due to the fact no sensitive, private personal data was exposed, a scraped data sample posted by God User contained information such as email addresses, Phone numbers, geolocation records, genders, and different social media details, giving malicious actors masses of statistics to craft convincing, follow-on social engineering assaults withinside the wake of the leak, as warned through the UK's NCSC.

- Facebook(April 2019)

  In April 2019, it become found out that datasets from Facebook apps have been uncovered to the general public internet. The records associated with extra than 530 million Facebook customers and protected telecellsmartphone numbers, account names, and Facebook IDs. However, years later (April 2021) the records become published for free, indicating new and actual crook motive surrounding the records. In fact, given the sheer range of telecellsmartphone numbers impacted and quite simply to be had at the darkish net due to the incident, protection researcher Troy Hunt introduced capability to his HaveIBeenPwned (HIBP) breached credential checking webweb page that could permit customers to affirm if their telecellsmartphone numbers have been protected withinside the uncovered In a weblog post, Hunt said, "I'd never meant to make phone numbers" "I was of the opinion that it didn't make sense for a variety of reasons. All of that altered as a result of the Facebook data. Because there are over 500 million phone numbers but just a few million email addresses, greater than 99 percent of individuals were missing out on a hit when they should have been."

- Yahoo(2014)

  Yahoo makes its second entry on this list, following an assault in 2014 that was unrelated to the one mentioned above. State-sponsored attackers obtained information from 500 million users, including names, email addresses, phone numbers, hashed passwords, and birth dates. Yahoo took early corrective action in 2014, but it wasn't until 2016 that the information were made public when a stolen database was sold on the black market.

- Adult Friend Finder(October 2016)

  In October 2016, cyber-thieves stole 20 years' worth of subscriber data from the adult-oriented social networking site The FriendFinder Network, which was spread over six databases. Given the touchy nature of the company's services, which encompass informal hookup and person content material web sites like Adult Friend Finder, Penthouse.com, and Stripshow.com, the facts breach of extra than 414 million accounts, which covered names, e-mail addresses, and passwords, had the ability to be specially unfavorable for victims. Furthermore, the great majority of the passwords released were hashed using the notoriously weak SHA-1 technique, with an estimated 99 percent of them decrypted by the time LeakedSource.com published its study on November 14, 2016.

- NetEase(October 2015)

  Email addresses and plaintext passwords belonging to 235 million accounts were purportedly sold by dark web marketplace seller DoubleFlag in October 2015, NetEase claimed that a supplier of mailbox services through the likes of 163.com and 126.com. While there is evidence that the data is authentic (several HIBP users confirmed a password they use is in the data), the Chinese breach has been classified as "unverified" owing to the difficulties of conclusively proving it.

- LinkedIn(June 2012)

  LinkedIn makes its second entry on this list, this time in regard to a breach it had in 2012, when it stated that attackers had acquired unassociated passwords of 6.5 million users. They uploaded them on a hacker site in Russia. The complete nature of the tragedy become now no longer uncovered till 2016, though. The identical hacker who offered MySpace's records become determined to promote the e-mail addresses and passwords of a hundred sixty-five million LinkedIn contributors for simply five bitcoins (about $2,000 on the time). LinkedIn said that it had been made aware of the hack and that all impacted users' passwords had been changed.

- Dubsmash(December 2018)

  Dubsmash, a New York-primarily based totally video messaging provider, had 162 million e-mail addresses, usernames, PBKDF2 password hashes, and specific private information inclusive of dates of delivery stolen in December 2018, and all of this became finally bought at the Dream Market darkish net marketplace the subsequent December. The facts became a part of a bigger series that covered MyFitnessPal (extra on that below), MyHeritage (ninety-two million), ShareThis, Armor Games, and the relationship app CoffeeMeetsBagel.

- Adobe(October 2013)

  Hackers took around three million encrypted consumer credit card details and login data for an indeterminate number of user accounts, according to Adobe, which reported the theft in early October 2013. Adobe up-to dates their

estimate some days later to consist of the IDs and encrypted passwords of 38 million "energetic users. Brian Krebs, a security writer, later stated that a file released just days before "seems to incorporate greater than one hundred fifty million logins and hashed password combos received from Adobe. After weeks of investigation, it changed into determined that the assault had found out patron names, passwords, as well as debit and credit card information. Adobe agreed to pay $1. 1 million in criminal costs and an unknown sum to customers in August 2015 to settle prices of Customer Records Act violations and unfair enterprise practices. The sum paid to clients changed into expected to be $1 million in November 2016.

- My Fitness Pal(February 2018)

  Around a hundred and fifty million precise e-mail addresses, IP addresses, and login credentials consisting of usernames and passwords saved as SHA-1 and bcrypt hashes were exposed in February 2018 by diet and fitness app MyFitnessPal (owned by Under Armour). The subsequent year, the statistics have become to be had for buy at the darkish net and elsewhere. The employer admitted the breach and said that it has taken steps to warn customers approximately it.

5 Conclusion

With our increasing reliance on the internet, data exchange creates a risk of data breach. An attacker attempts to exploit system flaws in order to misappropriate data. There may be an alternative technique that may be used to reduce the likelihood of a data leak. We can use best practices to reduce data breaches and data loss.

Acknowledgements

This research is conducted in direct supervision of the Software Evaluation and Re-Engineering Research (SERER) Lab.

Notes: It is common that you will want to acknowledge the contribution of others to your work, even though these might not have been sufficient to warrant being a co-author.

Consider who might have provided valuable discussions, funding support, or moral support for the work.

BTW, you don't have to start each section on a new page. I have done that here for clarity, but it isn't usually needed.

A Appendices

This is a short appendix, just included as an example.

Notes: An appendix can be used to include material that is important, but not needed in the main body of the text, and which it might detract from the main point of the report.

A common example is code. You should not include code in the main body of a report unless it is particularly important or revealing.

However, for the convenience of your supervisors who may wish to examine the code, and for your own benefit (in having a self-contained document), you may wish to include the code in an appendix. If so, have a look at the `listings` package for LaTeX. For Matlab, there is also a `matlab-prettifier` package that may work more easily for you.

References

Notes: A critical component of the work is the list of references. We have discussed their use earlier – here I simply make some notes on their presentation.

This is one of the hardest parts to get just right. BibTeX can help a great deal, but you need to put a good deal of care in to make sure that

- the references are in a consistent format;
- all information is correct; and
- the information included is in the correct style for the intended audience.

Details *really* matter in this section. It's easy to lose marks in this section.

ASH1925012M

ORIGINALITY REPORT

55%	29%	0%	42%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	v1.overleaf.com Internet Source	9%
2	www.csoonline.com Internet Source	5%
3	Submitted to Fiji National University Student Paper	5%
4	Submitted to Taylor's Education Group Student Paper	4%
5	Submitted to University of West London Student Paper	3%
6	de.overleaf.com Internet Source	3%
7	Submitted to Rivier University Student Paper	3%
8	Submitted to Hong Kong Baptist University Student Paper	3%
9	Submitted to University of Bolton Student Paper	3%

10	Submitted to Turiba University Student Paper	2%
11	Submitted to Florida State University Student Paper	2%
12	Submitted to Middle East College of Information Technology Student Paper	2%
13	global.oup.com Internet Source	1%
14	Submitted to Technological Institute of the Philippines Student Paper	1%
15	Submitted to Ain Shams University Student Paper	1%
16	Submitted to University of Wollongong Student Paper	1%
17	Submitted to St John Bosco College Student Paper	1%
18	Submitted to University of Huddersfield Student Paper	1%
19	Submitted to National College of Ireland Student Paper	1%
20	www.coursehero.com Internet Source	1%

21	Submitted to University of Greenwich Student Paper	1%
22	Submitted to UT, Dallas Student Paper	1%
23	Submitted to Study Group Australia Student Paper	1%
24	www.grc.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925012M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

PAGE 3

PAGE 4

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word. Consider using the article **the**.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 5

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 6

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Missing "," You may need to place a comma after this word.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word.

Sentence Cap. Remember to capitalize the first word of each sentence.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Dup. You have typed two **identical words** in a row. You may need to delete one of them.

Possessive This word may be a plural noun and may not need an apostrophe.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Possessive You may need to use an apostrophe to show possession.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Run-on This sentence may be a run-on sentence. Proofread it to see if it contains too many independent clauses or contains independent clauses that have been combined without conjunctions or punctuation. Look at the "Writer's Handbook" for advice about correcting run-on sentences.

Missing "," You may need to place a comma after this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 8

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

PAGE 9

Confused You have used **to** in this sentence. You may need to use **two** instead.

Wrong Form You may have used the wrong form of this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word. Consider using the article **the**.

Missing "," You may need to place a comma after this word.

PAGE 10

Prep. You may be using the wrong preposition.

Confused You have used **A** in this sentence. You may need to use **an** instead.

Possessive You may need to use an apostrophe to show possession.

PAGE 11
