The Implications and Effects of Data Leaks

Paul-Andrei PREDESCU, Dragoș BĂLAN
Faculty of Law, "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
predescu.paul48@yahoo.ro, balan.dragos99@gmail.com

Abstract

In the following article we will present how data theft can have serious effects on the personal life of citizens and users of certain applications, and in general on public institutions and countries. In the following we will find out how these data can end up in the hands of hackers, for what purpose they are used and what are the legal implications. In the end we will analyze how the authorities try to limit this phenomenon and how each of us can take protective measures for this purpose.

Index terms: cybercrime, cybercriminal, data breach, data leak, malware

1. Introduction

In order to be able to understand how data leakage occurs, we must have a well-structured system in which information is formed and stored. Thus, cyberspace is the virtual environment, generated by the informational content processed, stored or transmitted, as well as by the processes and operations carried out by the users of the virtual environment, the human resource produces data that passes through different applications having the storage center in several places (Datacenters, PCs, Laptops, Mobile, Cloud).

Another concept related to data leakage is that of cybersecurity. It represents the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, availability, integrity, non-repudiation, authenticity of information in electronic format, of public or private resources and services, in cyberspace. When there is no timely response against threats to cyber infrastructures or human errors occur, data beaches can occur.

A Personal Data Breach is any breach of security that results in the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of Personal Data or access to Personal Data. This includes violations due to accidental and intentional causes. It also means that a breach involves more than just the loss of personal data. A personal data breach can be broadly defined as a security incident that compromises the confidentiality, integrity, or availability of personal data. In other words, a personal data breach occurs whenever personal data is accidentally lost, destroyed, corrupted, or disclosed. If someone accesses or discloses your data without your permission or where the data is not available and the unavailability would have a material adverse effect on the individual [1].

2. How data leaks can occur

When the attacker creates a threat by exploiting vulnerabilities, it leads to risks. These risks can affect the assets causing exposure and thus the data breach has a high chance of occurring. Meanwhile a data leak is caused when an internal source exposes information. Criminals can use a variety of methods to try and break into a network, for example DDoS, Trojans, Malware, disruption via servers/network. Data leaks occur because of an internal problem. They don't usually happen because

of a cyberattack. This is encouraging news for organizations since they can proactively detect and remediate data leaks before they are discovered by criminals [2].

Let's review some of the most common causes of data leaks.

- **Bad infrastructure:** Misconfigured or unpatched infrastructure can unintentionally expose data. Having the wrong settings or permissions, or an outdated software version may seem innocent, but it can potentially expose data. Organizations should ensure that all infrastructure is carefully configured to protect data.
- **Social engineering scams:** While data breaches are the result of a cyberattack, criminals often use similar methods to create a data leak. Then the criminal will exploit the data leak to launch other cyberattacks. For example, phishing emails may successfully gain access to a person's login credentials, which could result in a bigger data breach.
- **Poor password policies:** People tend to use the same password for multiple accounts because it's easier to remember it. But if a credential stuffing attack happens, it could expose several accounts. Even something as simple as having login credentials written in a notebook could lead to a data leak.
- **Lost devices:** If an employee loses a device with a company's sensitive information, it qualifies as a potential data breach. If a criminal gains access to the device's content, it could lead to identity theft or a data breach.
- **Software vulnerabilities:** Software vulnerabilities can easily turn into a huge cybersecurity issue for organizations. It's possible for criminals to take advantage of outdated software or zero-day exploits and turn it into a variety of security threats.
- **Old data:** As businesses grow and employees come and go, companies can lose track of data. System updates and infrastructure changes can accidentally expose that old data [2].

3. The information and interests of hackers

For us to understand the complexity of the hacking world, we have to begin with the beginning and that is, to understand *what a hacker is, how does hacking work, the type of hackers that are currently navigating the web* and *what are the targets of these so-called "cyberpunks" or hackers* [3].

3.1. So what is a hacker?

A definition for this word would be: "A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example, steal information to hurt people via identity theft or bring down a system and, often, hold it hostage in order to collect a ransom."

- To continue the discussion, we have to understand the ***process of hacking***, how does it work, and an answer might be that "hackers use technical skills to exploit cybersecurity defenses. Ethical hackers test for cybersecurity vulnerabilities and may take up hacking as a profession -- for example, a penetration tester (pen tester) -- or as a hobby. The end goal is often to gain unauthorized access to computers, networks, computing systems, mobile devices or internet of things systems. Many professional hackers use their skills to determine security holes in enterprise systems and then advise where companies should boost their security defenses to keep threat actors out. Results can also be deleterious: Malicious hackers may steal login credentials, financial information and other types of sensitive information.

- Many hackers aim to exploit either technical or social weaknesses to breach defenses. Technical weaknesses may include vulnerabilities in software or other exploitable weak spots. To exploit social weaknesses, hackers may attempt to manipulate social outcomes through false pretenses, such as impersonating a co-worker or other individual to gain financial or login information. Hackers may also use their technical skills to install dangerous malware, steal or destroy data, or disrupt an organization's services.
- Hackers of all types participate in forums to exchange hacking information and tradecraft. There are numerous hacker forums where ethical hackers can discuss or ask questions about hacking. Many of these hacker forums offer technical guides with step-by-step instructions on hacking.
- In contrast, dark web sites often host forums and markets for threat actors or criminal hackers, which serve as a means of offering, trading and seeking out unlawful hacking services.

Scripts, and even specially tailored software programs, are frequently used by criminals who don't usually have the technical skills to penetrate corporate networks. For the purpose of obtaining information on the functioning of the target system, this software can have access to network data. These scripts can be found on the Internet, for anyone who is typically an entry level hacker. Hackers with limited skills are sometimes called *script kiddies*, referring to their need to use malicious scripts and their inability to create their own code. Advanced malicious hackers might study these scripts and then modify them to develop new methods [3].

3.2. What are the types of hackers navigating the web?

In the past, the security community informally used references to hat color as a way to identify different types of hackers, usually divided into five main types. A few of these terms have been replaced to reflect cultural changes.

- Ethical hackers or authorized hackers -- previously known as white hat hackers -- strive to operate in the public's best interest rather than to create turmoil. Many ethical hackers who work doing pen testing were hired to attempt to break into the company's networks to find and report on security vulnerabilities. The security firms then help their customers mitigate security issues before criminal hackers can exploit them.
- Threat actors or unauthorized hackers -- previously known as black hat hackers -- intentionally gain unauthorized access to networks and systems with malicious intent. This includes stealing data, spreading malware or profiting from ransomware, vandalizing or otherwise damaging systems, often in an attempt to gain notoriety. Threat actors are criminals by definition because they violate laws against accessing systems without authorization, but they may also engage in other illegal activity, including corporate espionage, identity theft and distributed denial-of-service (DDoS) attacks.
- Gray hat hackers fall somewhere between ethical hackers and threat actors. While their motives may be similar to those two groups, gray hats are more likely than ethical hackers to access systems without authorization; at the same time, they are more likely than threat actors to avoid doing unnecessary damage to the systems they hack. Gray hat hackers may offer to repair vulnerabilities they have found via their own unauthorized actions rather than using their expertise to exploit flaws for illicit profit, even though they aren't typically - or primarily - motivated by money.
- Red hat hackers, also called eagle-eyed or vigilante hackers, are similar to ethical hackers. Red hat hackers intend to stop unethical attacks by threat actors. While red hat hackers may have a similar intent to ethical hackers, they differ in methodology, as red

hat hackers may use illegal or extreme courses of action. Often, red hat hackers will deploy cyber-attacks toward the systems of threat actors.

- Blue hat hackers, also known as vengeful hackers, use hacking as a social weapon. Frequently, it is used as a means for revenge against a person, employer or other organization. Hackers who post personal and confidential data online to ruin reputations or attempt to gain unauthorized access to email and social media accounts are classified as blue hats.
- Script kiddies are amateur, inexperienced hackers who attempt to use pre-written scripts in their hacking efforts. Often, these are fledgling hacking enthusiasts who cause little damage.
- Hacktivists are organizations of hackers that use cyber-attacks to affect politically motivated change. The purpose is to bring public attention to something the hacktivist believes might be a violation of ethics or human rights. Hacktivism attacks may attempt to reveal evidence of wrongdoing by publicizing private communications, images or information [3].

3.3. What type of information do hackers look for?

There are various types of information that hackers can steal from your business. Make sure you're protecting these in particular:

- **Personal data**
  This includes Social Security numbers, financial information, birth dates, and other sensitive personal data. To hackers, these are quite valuable; in 2019 alone, there were 13 million recorded identity theft incidents. While passport information sells for the most amount of money, Social Security numbers are the most valuable to hackers, as these can be used for tax fraud, opening credit accounts, and other malicious activities. Your business may not collect Social Security numbers from your clients, but their financial data may be easily stolen.
- **Digital infrastructure**
  Hackers are aware of the high costs of a proper IT infrastructure, so they will resort to stealing another business's IT system to save money. Potential indicators of such an attack include network slowdowns, rapid decrease of storage space, and unknown devices connecting to your network. Over time, this will result in additional costs and lower business productivity.
- **Corporate accounts**
  Hackers can also steal your employees' corporate account data through phishing and malware attacks. They can use the information to solicit personal and financial information from your customers, conduct business email compromise attacks, disrupt your operations, or steal.
- **Intellectual property (IP)**
  Your IP is one of the most important aspects of your business. Without it, you won't be able to offer something unique to your customers and stand out from the competition. This is exactly why hackers might want to steal your IP. If they get their hands on your confidential data, they might sell it in the black market and expose your company's business plans, product ideas, and the like. For instance, a hacking group called the Advanced Persistent Threat 10 attacked the networks of more than 45 technology companies and government agencies in the USA to steal sensitive information regarding new and developing technologies. Two hackers from the group were indicted for conspiracy to commit computer intrusion, wire fraud, and aggravated identity theft [4].

4. The set of international norms

Because cybercrimes have become more and more present in every person's life and they can even affect states, international organizations are trying to regulate this problem.

Thus, in 1997, G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment. G8 also mandates that all law enforcement personnel must be trained and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis [5].

In 1990 the UN General Assembly adopted a resolution dealing with computer crime legislation. In 2000 the UN GA adopted a resolution on combating the criminal misuse of information technology. In 2002 the UN GA adopted a second resolution on the criminal misuse of information technology [5].

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cybersecurity issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS). In 2003, Geneva Declaration of Principles and the Geneva Plan of Action were released, which highlights the importance of measures in the fight against cybercrime. In 2005, the Tunis Commitment and the Tunis Agenda were adopted for the Information Society [5].

The Council of Europe is an international organisation focusing on the development of human rights and democracy in its 47 European member states.

In 2001, the Convention on Cybercrime, the first international convention aimed at Internet criminal behaviors, was co-drafted by the Council of Europe with the addition of USA, Canada, and Japan and signed by its 46 member states. But only 25 countries ratified later. It aims at providing the basis of an effective legal framework for fighting cybercrime, through harmonization of cybercriminal offenses qualification, provision for laws empowering law enforcement and enabling international cooperation [5].

General Data Protection Regulation (GDPR) is applicable as of May 25th, 2018, in all member states to harmonize data privacy laws across Europe.[6] GDPR puts the individual as the central element and obliges to protect their data through appropriate measures.

4.1. The GDPR principles:

- Legality, fairness and transparency - data should be processed legally and fairly to the data subject. Explanations should be given to the person in a language they can understand, without legal jargon.
- Purpose limitation - the data will not be used in any other way than that presented to the individual.
- Data minimization - only necessary data will be processed.
- Accuracy - updated data will be kept.
- Integrity and confidentiality - the data will be protected by appropriate measures.
- Responsibility - processes will be documented and compliance with the above principles will be demonstrated [6].

4.2. The rights of the natural person:

- The right to information - the person must be informed, among other things, about what data is processed, why, for what purposes, to whom it is transmitted and what rights he has.

- Right of access - the individual has the right to access their own processed personal information.
- The right to rectification - the person has the right to obtain the rectification of incomplete and inaccurate information concerning him.
- The right to erasure - in some situations, the individual has the right to request the deletion of data that is no longer needed.
- The right to restriction of processing - restriction of processing when there are grounds.
- The right to portability - the right of the person to request data portability from one operator to another.
- The right to object - the right of the person to object to the processing, when there are grounds.
- The right not to be subject to automated decision-making, including profiling - the person has the right to human intervention in the case of important decisions concerning him.
- The right to lodge a complaint with the Supervisory Authority - when she is dissatisfied with the way in which her data is processed or when her rights have not been respected.
- The right to go to court - to obtain material and/or moral damages if damage has resulted [6].

5. Legal effects of data theft

Just like any crime, cybercrimes produce certain legal effects and involve the responsibility of the people. On the one hand, we have the criminal liability of the person or persons who stole or tried to steal the data, and on the other hand, we have the responsibility on the companies towards the users because they hat to do all the diligence to protect their information.

The legal ramifications of a data leak can be government fines, penalties, and in extreme circumstance, jail time, are some of the consequences of not protecting personally identifiable information adequately.

One ramification many don't consider is the cost of litigation associated with a breach. Many of the associated lawsuits can end up as class-action lawsuits, potentially multiplying the total cost of the breach exponentially [7].

Settlements can be harsh - depending on the judge or jury. For large breaches, settlements over $100 million are not out of the question, especially when dealing with healthcare information. Another cost of a breach includes having to pay the plaintiff's legal bills, which can be extremely high [7].

A cyber-attack on your business that exposes personal or confidential data could have several nasty consequences for your business, including:

- financial loss from stolen funds or a loss of income from an inability to operate your business as usual.
- claims being made by customers, for example where you have not complied with your privacy policy.
- claims for breach of contract if you do not meet your contractual obligations to comply with data protection legislation.
- regulatory fines for non-compliance with GDPR or the Data Protection Act 2018.
- reputational damage as consumers lose faith in your ability to securely process their data [8].

6. How we can protect our data

In order for us to have our data protected while we use our devices on the Internet we can use some safety precautions so as for our personal information not to end up in the wrong hands. Some advice that is widely used is for us to:

- **Create strong passwords**: For example, a strong password should contain at least 12 characters and contain a combination of lower and upper case letters, numbers and if possible symbols.
- **Never use the same password on multiple accounts**: Having multiple passwords makes it harder for hackers to gain access to your personal information.
- **Don't log in on personal account on free or public Wi-Fi**: Open networks make it really accessible for people to look into your activity and accounts.
- **Install an antivirus and keep it updated**: New viruses are created all the time and so to have and extra layer of protection is always good to have an antivirus installed and up-to-date.
- **Don't click on pop-ups and virus warnings**: These warnings and now called "scareware" which are fake security alerts that when you click them, they guide you to install a program to remove the virus in your computer, but the link contains viruses.
- **Be wary of phishing email**: These emails are sent to thousands of people, pretending to be from banks, companies, online shops, that try to send you on their website where you are asked to write down your personal information.
- **Store personal and financial information securely**: Never access such information in internet cafes or public computers [9].

7. Conclusion

Cybercrimes as we have seen in recent years have become more and more frequent and pose a real threat to our personal and financial information. Attacks can vary in many different ways from simple emails that try to insert malware in your personal devices if you click on them to full scale attacks on websites owned by enterprises.

This paper wanted to show the problem of the damage that those attacks do is in most cases is quite substantial not once for example did people lose their identity, credit cards information or even social security numbers to data breaches by hackers. This is why we have to be extra careful with our presence on the internet and take extra steps of precaution when navigating the web. The governments took note of the risks that can occur while handling this type of information and so adopted the well-known GDPR that protects our personal information on the Internet in a way that the data should be processed legally and fairly to the data subject. Even explanations should be given to the person in a language they can understand, without legal jargon.

Other steps that we can take to protect ourselves on the internet is to use different passwords for the accounts we have, minimalize the information we share on social media, never click on links or pop-ups that warn us that we have been infected with viruses and use an antivirus and keep it up to date.

References

[1] Information Commissioner's Office 'Personal data breaches'. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

[2] Glossary ‘What Is a Data Leak? How They Happen and How To Prevent Them’ [Online] Available: https://abnormalsecurity.com/glossary/data-leak.
[3] Wesley Chai and Linda Rosencrance, “What is a hacker“. May 2021 [Online]. Available: https://www.techtarget.com/searchsecurity/definition/hacker.
[4] Ron Samson Jr. “Data Stealing; What Information is a Priority for Hackers?”. 2022 [Online]: https://www.clearnetwork.com/why-do-hackers-keep-stealing-the-same-consumer-data/.
[5] International cybercrime. 20 June 2022. Wikipedia. Available at: https://en.wikipedia.org/wiki/International_cybercrime.
[6] Intersoft consulting: https://gdpr-info.eu/.
[7] The legal ramifications of a data breach: https://www.ironmountain.com/resources/general-articles/t/the-legal-ramifications-of-a-data- breach.
[8] Clive Mackintosh, “Legal consequences of a cyber-attack”: Date: 9 March 2022. Available at: https://harperjames.co.uk/article/legal-consequences-of-a-cyber-attack/.
[9] ‘30 ways to love yourself online – A beginner‘s guide to Personal Data Privacy’. Available at: https://www.privacy.gov.ph/30-ways/.