Data security

Made by Arghire Gabriel

Content

Introduction

To get an idea, for starters, of this broad and widespread field over the last decade, we'll start with Wikipedia's definition: "Data security refers to the protection of digital data, such as that in databases, from destructive and unwanted actions by unauthorized users, such as cyber attacks or data security breaches (unwanted breaches). " [Wiki01]

Another much more rigorous and specialized definition can be found at an industry company, "Forcepoint", which also deals with the sale of "firewall" software, "cloud" access, IT security products. [Wiki02] Their definition is as follows: “Data security is a set of standards and technologies that protect [users'] data from intentional or accidental destruction, modification or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, logical controls, organizational standards, and other security techniques that limit unauthorized access by malicious users or [harmful] processes. " [FRP]

It is suddenly noticeable how people working in the field have a different vision, a different angle of seeing things. It addresses the issue of security at a deeper level. Thus, they start from the idea that in order to respect the security of users' data, standards must be imposed, which must be respected and punished if they are violated. In fact, as we will see later, the security of users' data is quite superficial, because users, ie consumers of software products, easily expose their data, sometimes confidential, and by the agreement they give on the terms and conditions of use leaves that their data be extracted and used for various purposes, mainly commercially, by displaying targeted advertisements.

Finn Lützow-Holm Myrstad of the Norwegian Consumer Council and co-chair of the Transatlantic Consumer Dialogue (TACD) has taken many steps to tighten the freedom with which applications extract user data and was shocked to find that users are to blame. they too easily agree to it. He also said that the applications offer a service like "Take it or leave", so users are forced to accept the terms and conditions quite malicious, in terms of data security, to use that application and the services it offers. [YT01]

In this context, we wonder if we do not give our consent too easily to have our identity extracted, in cases such as social networks by completing these forms ourselves to show who we are. We are exposed non-stop, so, for anyone who wants to see who we are, what we do, what trips we make and all these things more or less confidential. The question that arises is: can there be a balance, a balance between protecting user data and disclosing and using it for various purposes? We intend to investigate this in the following.

Data security history

To answer the question we will have to travel back in time, see where it started and how it continued to spread viruses and malicious programs, history of people called hackers, all in terms of security of a user's data.

Bob Thomas of "BBN Technologies" believes that the first computer virus was in the early 1970s. This program was transferred through "ARPANET", the forerunner of the Internet. It wasn't harmful, it just generated the message "I'm the creeper, catch me if you can!" (in Romanian: "I'm the worm, catch me if you can!") on DEC PDP-10 computers, but Ray Tomlinson, the man who later invented mail, turned it into a virus that replicates itself. Then he developed an antivirus program called "The Reaper" to delete it.

Now the question arises: how did we get from such an insignificant thing, to the situation today, when there are viruses that cybernetically attack nuclear factories, government institutions and other viruses such as "malware", "ransomware" that attacks even the hardware architecture of a computer, and other cyber attacks plan to extract millions of user data using a particular service, such as the 2013 or 2014 attack on Yahoo, which compromised more than 3 billion user accounts? [DataH03]

So how was such an exponential growth in hacking technologies possible? There are many factors to analyze, but two things are certain: first, the discovery of the most advanced technologies and their transposition on real-life devices, and, second, the number of Internet users. If in 2005 an estimated 1 billion people connected to the Internet, in 2019 the number was estimated at 4 billion people who used the Internet. [Intuit]

The history of data security continues with the episode of 1985, when a computer engineer named Ralf Berger gave a speech in the "Chaos Computer Club" (currently the largest hacker club in Europe), encouraging others to explore this new aspect of programming. In 1986 he was diagnosed with a deliberately released virus called "Brain", which attacks floppy disks. [DataH03]

Two years later, in 1988, a student named Robert Tappan Morris Jr. wanted to count how many computers were connected to the Internet. He created a virus that slowed down computers running this code using valuable resources from the processor and brought the Internet to a standstill. He managed (perhaps unwittingly) to disconnect 10% of the computers connected to the Internet at that time. This virus had consequences in real life. He was the first person to be charged for this action by the “Computer Fraud and Abuse Act.” [DataH01]

In the following years, hackers became more and more refined and aggressive, aiming for different purposes. However, in order not to deviate from the introductory question, we will return to the history of attacks aimed at stealing people's identities.

One such massive attack was in 2012 when a US credit bureau suffered a major data leak. The agency had bought a business called "Court Ventures", which used public records to collect information. Court Ventures sold information to third parties quite often. On third party service was the Vietnamese fraudster service, which provided its customers with the personal information of many Americans, including financial information and social security numbers. The breach lasted over 10 months, after the

acquisition of the "Court Ventures" business. Although the number of records on display is unknown, it is estimated that over 200 million records have been broken. [DataH03]

Another cyber attack comes in 2013, when hackers accessed the servers of the corporation "Target" and stole personal information of over 70-110 million customers of the sales company. This breach resulted in the loss of the company's $ 162 million. The data came from sellers who visited the company's stores for 3 weeks, starting the day before "Thanksgiving". Target was unaware of this attack and did not detect it on its own. It was instead alerted by cardholders, who felt an increase in fraudulent transactions using credit cards used before at [purchase on] Target. [DataH03]

We will continue to show here 3 more breaches of security systems for extracting and distributing user data, and then we will comment on them.

Also in 2013, all 3 billion Yahoo emails from customers became victims of cybercrime. The breach was discovered during a review provided by the 2014 law. Andrew Komarow, head of the investigation for InfoArmor and hired by Yahoo, found evidence that a darkweb seller (in Romanian, the dark Internet) offered for sale a list of over 1 billion Yahoo accounts for about $ 300,000. [DataH03]

Another case comes in 2016, in mid-October, when more than 412 million accounts in the "FriendFinder Network" were broken into, and hackers collected 20 years of intelligence information. data, stored on 6 databases, containing names, email addresses and passwords. The 6 databases also contained adult content and occasional dating sites, such as "Adult Friend Finder", "Cams", "Penthouse" and "Stripshow". Most passwords were poorly protected by a hashing algorithm and were easily found later. [DataH03]

And the last case we will present dates from 2015, about a database of citizens who voted. It contained the votes of 191 million voters and was exposed to the free Internet, meaning that anyone could have access to this disclosed information. It is not known how many people accessed the information that was exposed. The problem was the result of a human error. The database was configured incorrectly and left open on the Internet. Personal information - email addresses, names, party affiliations, birth dates and more - of all registered citizens who voted for 50 countries, including the District of Columbia. [DataH03]

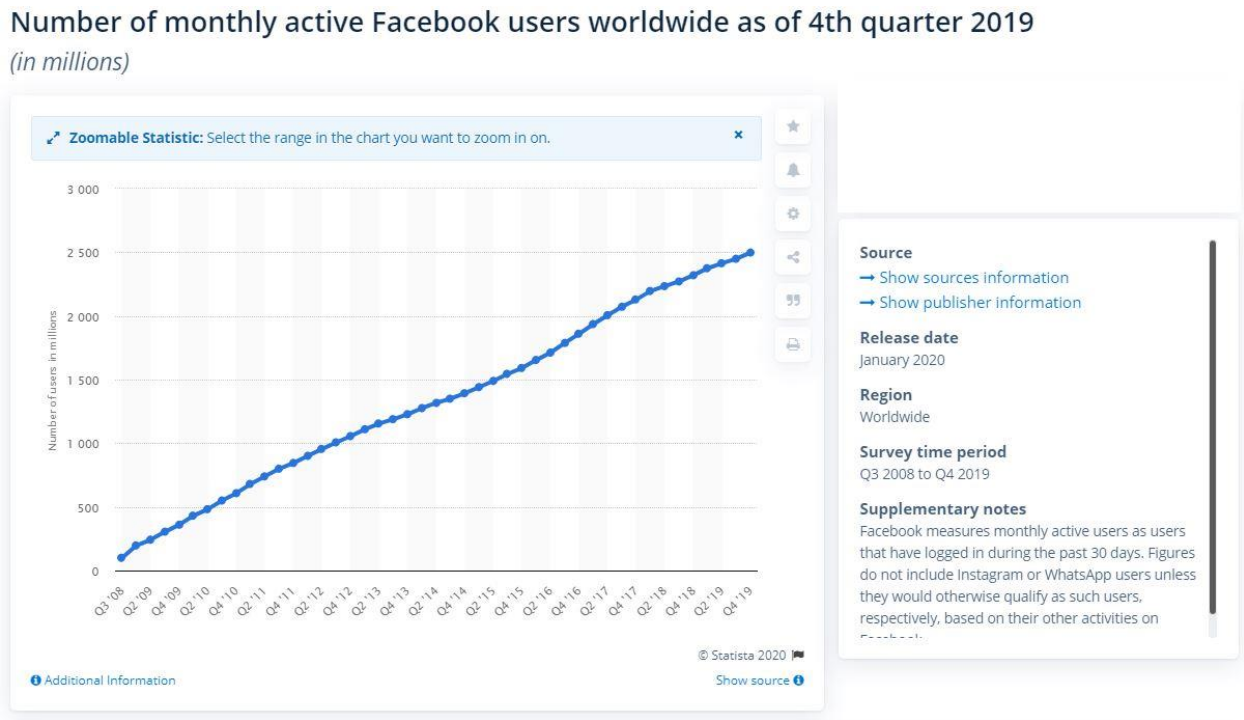
We will expose other cases of data leaks. Until then, let's conclude what we learned from them and then comment on them.

Security breaches can occur for a variety of reasons, from the loss of a device with unencrypted information to the accidental opening of private information on a website to the general public. The number of scandals and breaches in the data security of some institutions or businesses has steadily increased from year to year. Measures are always taken by organizations to increase their data security. It has become a billion-dollar industry. Unfortunately, cybercriminals are always finding new ways and techniques to infiltrate a business database, and human error is a true reality. The information wanted by hackers includes names, social security numbers, birth dates and other personal information used to steal identities. Discipline, a plan and a defensive way of thinking are needed to prevent such data leaks. [DataH03]

As you can see, in almost all cases hackers break into companies' security systems and extract user data, to sell it for money, as was the case with Yahoo, when a darkweb seller offered for sale a list over 1 billion Yahoo accounts for about $ 300,000.

We ask ourselves: does the blame belong only to companies that do not have such good security and cannot defend themselves from the inevitable attacks of hackers? The answer is that, for the most part, yes. For such data leaks, companies are accused of not being able to keep customers' confidential data safe, while losing their trust. But if these attacks are inevitable, are security measures taken? The answer depends on each company. Let's take a closer look at the "Facebook - Cambridge Analytica" scandal of 2018. Facebook said that the data company Cambridge Analytica obtained unauthorized access to up to 87 million user data, most users being from the United States . [Wired01] It is known that any data leak of a company, especially the largest and best known in the world, leads to loss of user confidence. That's what happened. Facebook even received a £ 4 billion fine for this unpleasant event. [TG01]

But, doing some research, I was surprised at the importance that Facebook users gave or seem to have given. I searched for a report on the number of Facebook users and found the following graph: [ST01]



The title of the report is "The number of active monthly Facebook users worldwide by the fourth quarter of 2019". The Facebook scandal erupted in early 2018. Looking closely at "Q2 '18" to "Q4 '19", ie from the second quarter of 2018 to the fourth quarter of 2019, I noticed that the number of active monthly Facebook users has steadily increased. The graph shows, however, a small cap on that number at the time of the scandal, but even then the number was still growing. That is, the active monthly users were almost the same as before the scandal started, and then followed by the same increase in the number of active monthly users.

What is highlighted in this chart and what can we conclude? Facebook users do not care too much about the security and / or disclosure of their personal information. A Facebook profile includes, if fully completed, the user's first and last name, profile picture, date of birth, residence, studies, friends, locations visited and more. In other words, the Facebook profile is a (complete) history of the user's life and which he publicly shares with his friends AND Facebook. That is, all pictures, messages and everything that a particular user posts on his profile and communicates with other users is retained in the company's database.

And now we wonder why big companies don't care so much about data security? Maybe because users don't even care who holds their information and where it goes next. On the other hand, the fine received for misleading users that their data is kept secure is too small compared to the profit the company makes by using user data.

The introductory question was: can there be a balance, a balance between protecting user data and disclosing and using it for various purposes? Ironically, it may exist, but it does not exist. If customers of a service are disinterested in protecting confidential data, why would the company be interested in developing a good defense system against possible cyber attacks or, more specifically, data leaks? The money that the company obtains by owning user information could destroy any balance between data protection and disclosure.

What does this finding lead us to? If users do not realize how easy it is to sell their personal lives and what consequences this may have, various organizations are beginning to take steps to protect users and limit access to companies and the various services they offer by extracting user data.

Data protection regulations

We now intend to explore various actions and legal regulations for the protection of users of applications and services. At a TEDx conference [YT01], Finn Lützow-Holm Myrstad of the Norwegian Consumer Council and co-chair of the Transatlantic Consumer Dialogue (TACD), which I mentioned in the introduction, is investigating a doll named Cayla, which was voted the toy of the year 2014 in countries around the world. The doll connects to the internet and uses voice recognition technology to answer the child's questions, just like a friend. This doll, however, does more than that. All these conversations, even the discussion of the members of a house is recorded, are sent to the company to which they belong. "This case alarmed me, because it is my duty to protect the rights of consumers in my country," said Mr. Finn. [YT01] To play with Cayla and access its features, an application must be downloaded. Parents must agree to the terms "changing without news". Child, friend and family records can be used for targeted advertising. And all this information can be sent to third parties.

If we take a step back, we notice how easily users' personal information is distributed to third parties. And how easily users agree with this. In fact, the conclusion is that using an application of this kind is like saying a "Yes" or a "No", which allows the use of services offered, such as "Take or leave". For this reason, users have no choice. They must agree to terms and conditions that they most likely disagree with. We will continue this after the speech.

"And that was not all. Anyone with a smartphone with this application can connect to Cayla from a certain distance ". Mr. Finn went on to say that he or any stranger can connect to the doll while he is outside the room where Cayla and her friends are. Then he imagined a conversation in which a man on the street connected to the doll and talked to the person in the house near the doll. The person asked if his mother was around, and when the person in the house (i.e., the child, in real life) answered that his mother was away at the store, the person on the street asked if he wanted to go out to play. with him, and the answer was yes.

Continuing, Mr Finn said he had published a report in 20 countries around the world, exposing the significant security flaw and many other issues. After this intervention, Cayla was banned in Germany, taken off the shelves of Amazon and Walmart and ended, with a smile on her face, saying that she is now resting peacefully at the German Museum of Espionage in Berlin.

This doll, which was not so unpopular, given that the 2014 doll had been voted, not only sent data to third parties, but was also a danger to the safety of children talking to the doll. And it starts from how the application can be used, how it is designed. So we tend to believe that it was not the parents who were responsible for the abduction of their child? Not true. They agreed to the terms and conditions of the application. "But what could he have done?" We asked ourselves.

Somehow, Mr. Finn also came to this question. He continued his speech, saying: "We need to get the security and privacy of these devices before they enter the market, because what's the point of locking a house with a key if anyone can enter through a device?

logged in? You may be thinking, "This is not going to happen to me. I will stay away from these imperfect devices. " But that won't keep you safe, because simply by connecting to the internet, you're put in an impossible position, "take it or leave it."

His point of view is to be appreciated. "I don't think it's fair to put the burden of responsibility on the consumer," he said. This is also natural. Citizens of a country are confident that the state, and especially those involved in the field of personal data security, have thought about these issues in advance, but it seems that some events prove otherwise. With the multitude of applications that invade virtual stores, one would think that there is no time to read all the terms and conditions, especially their regulation. Gathering his team, Mr. Finn said that reading all the terms and conditions of popular applications on a regular phone took no less than 31 hours, 49 minutes and 11 seconds. them for reading the conditions, and, ultimately, because she wants to use them, she will have to accept them anyway. So where is the mistake? The specified terms and conditions give the application owners too much freedom over what they want to do. No stricter standards are imposed to protect users. For example, the Cayla doll, mentioned earlier, could function as a spy in the homes of all users. The doll's owner had access to all of Cayla's recordings and was free to distribute them to third parties. This makes us wonder if these types of applications do nothing but take advantage of the freedom that exists in the data laws for data security.

Mr. Finn's speech ends in an optimistic manner that gives people hope that in the future the security of user data will be stronger: “The stories I told you today are not accidental examples. They are everywhere, and they are a sign that things need to change. How can we make this change? Well, companies need to understand that by providing privacy and security, they can build trust and loyalty with their users. Governments need to create a safer internet by ensuring that up-to-date rules are enforced. And we, the citizens? We can use our voice to remind the world that technology can really benefit society if it respects basic rights. ” [YT01]

However, far from the future promises, concretely, have laws been taken to strengthen the security of users' data? To answer this question we will stop again on the scandal "Facebook - Cambridge Analytica" in 2018. Shortly after that, on May 25, 2018 data protection reforms were introduced in Europe, but they also have influences on other continents. The reforms are known as the GDPR (General Data Protection Regulation). The old rules of protecting citizens' data date back to the 1990s, almost 2 decades, when technology had advanced exponentially, and the way applications and various services understood user data security was unbelievable. Thus, these new rules limited the access of organizations to what could be achieved with personal data collected from customers. The final form of the GDPR came after almost 4 years of discussions and negotiations - it was also adopted by the European Parliament and the European Council in April 2016. However, the GDPR entered into force on 25 May 2018, to give time European countries to adapt and make small changes to these rules, in order to better fit in the context of their country. In the UK, this flexibility led to the creation of the Data Protection Act (2018), which replaced the previous 1998 Data Protection Act. Subsequently, the California Consumer Privacy Act was introduced for California residents. [Wired02]

The GDPR does not only apply to the businesses and countries of the European Union. If a company in the United States, for example, acts for customers in the European Union, then the GDPR can also apply if the company is an inspector of EU citizens.

How has GDPR helped people secure their data? Well, at the heart of the GDRP are 7 key principles - set out in Article 5 of the legislation - and they have been designed to guide how people's data can be controlled. Here are the 7 key principles, given that only the seventh principle is newly introduced for data protection: [Wired02]

1. Legality, fairness and transparency
2. Limiting the purpose
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Responsibility

Even though the GDPR imposes high taxes on inspectors and data processors, the legislation is intended to help protect the rights of individuals. As such, in the GDPR we find 8 rights exposed for this protection. They even range from allowing people to easily access a company's data on them and have the right to request its deletion. All 8 GDPR rights of individuals are as follows: [Wired02]

1. The right to information
2. The right of access
3. The right to correction
4. The right to delete
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights to automatic decision-making and profiling

Having said all that, we can see that GDPR really wanted to increase the security of users' data, it did this, and the biggest fines that can be given range from 20 million euros or 4% of the total profit obtained by the company, whichever is greater. [GDPR]

Conclusion

In the introduction we present that "Data security refers to the protection of digital data, such as those in databases, from destructive forces and unwanted actions by unauthorized users, such as cyber attacks or data security breaches (unwanted breaches)." [Wiki01]

Then, the investigation I did was the answer to the question: "Can there be a balance, a balance between protecting user data and disclosing and using it for various purposes?"

Researching some details in the history of this field, some more significant attacks and events, as well as the insignificant speech of a man named Finn Lützow-Holm Myrstad from the Norwegian Consumer Council and co-chair of the Transatlantic Consumer Dialogue (TACD, I found the answer, rather sad, that "balance may exist, but it does not exist", given that consumers do not place much emphasis on the security of their data, so that companies formulate the terms and conditions in the way that could benefit most of this indifference and of the data they hold.

However, if users do not realize how easy it is to sell their personal lives and what the consequences may be, various organizations are beginning to take action in this regard (such as that of Mr Finn), and then we have seen that GDPR was introduced in Europe on May 25, 2018, also in order to intensify the security of user data.

From all this, we can see how the field of data security is quite vulnerable to various cyber attacks, and data leaks are a serious threat to the integrity and security of a person's identity. But, like any godfather, his godfather, measures are taken for the protection of citizens, and the identified attackers or companies that do not comply with the imposed regulations are severely punished.

Bibliography

[Wiki01]: Data security, https://en.wikipedia.org/wiki/Data_security

[Wiki02]: Forcepoint, https://en.wikipedia.org/wiki/Forcepoint

[FrP]: What is Data Security, https://www.forcepoint.com/cyber-edu/data-security

[YT01]: How tech companies deceive you into giving up your data and privacy | Finn Lützow-Holm Myrstad, https://www.youtube.com/watch?v=4E_1AB1rsSw&list=PLwf5LtStpAI6d4dBQ9b5_5tLUlROecCm_&index=16&t=0s

[DataH01]: The History of Data Security, https://www.blackstratus.com/the-history-of-data-security/#Timeline%20of%20Cybersecurity%20History

[DataH03]: A Brief History of Data Security, https://www.dataversity.net/brief-history-data-security/

[IntU]: Global Internet usage, https://en.wikipedia.org/wiki/Global_Internet_usage

[Wired01]: Facebook Exposed 87 Million Users to Cambridge Analytica, https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

[Wired02]: What is GDPR? The summary guide to GDPR compliance in the UK, https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

[TG01]: Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint, https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint

[ST01]: Number of monthly active Facebook users worldwide as of 4th quarter 2019, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[GDPR]: What are the GDPR Fines?, https://gdpr.eu/fines/