Section 1.

Basically, one day I got a request on Instagram from a food supplements agency asking me if I can give them a shout out on my account. In return I would get forty percent off their products for a month. I thought it was a scam, but when I entered their account I found a lot of followers plus that the page looked very professional. Like a normal person who likes to save money I decided to enter the link and sign up for the forty percent and put my accounts name in it. Then I gave them the shout out and waited to get confirmation of my forty percent discount. Then everything went down hill, the next day I woke up and opened Instagram absolutely nothing appeared it was a blank white page with nothing on it. I tried to contact Instagram and sent them emails verifying that the account is mine but they said that they can't help. So I just knew that I got hacked and lost my account which had a lot of personal conversations that could hurt me in my private life. Since then I've learned to never ever press on any link or ad on the Internet even if I'm sure of the organisation behind it. After a short while I made a new account and decided to use the "two-factor authentication" on Instagram so if anyone anywhere tries to login to my account I'll know and block them. In the end I've lost my old account and all my personal massages got compromised.

Section 2

A website owned by the European Central Bank has been hacked, the bank has announced. ECB said that attackers had managed to hack into its Bank's Integrated Reporting Dictionary (BIRD) website, and that it is possible that the names, email addresses and position titles of the 481 subscribers to the BIRD enewsletter may have been stolen in a data breach. The cyber-attack occurred by injecting malware into the server of an external provider hosting the BIRD website. The BIRD website, which provides the banking industry with details on how to produce statistical and supervisory reports, has been taken offline until further notice. After I saw the news I was a bit scared because nowadays we only use credit cards and our banks have all our information. That means that one day we might wake up and find all our personal information compromised through our trusted banks. All I know is that the security levels should be raised a bit to try and eliminate any threat of losing such valuable information.

Section 1 - Describe one or several IT security incidents that you personally have experienced.
Write about what happened and what consequences there were. Think that an incident is anything that violates a security policy (or for a private person anything that you think is an undesired activity). It can be forgotten information, lost devices, direct attacks etc.

The first thing I think of when I think about security incidents are related to online accounts, mostly accounts that involves video games. Last year when I was on vacation I suddenly got a bunch of emails that contained PayPal receipts that claimed that I had bought “in-game currency”, which is used to buy cosmetic items in one of the most popular game there is. Someone had managed to retrieve my account credentials to the game which had my PayPal account connected to it which in turn is connected to my credit card. The hacker then tried to buy a bunch of this in-game currency in order to gift them to another account. Luckily for me I keep most of my money on a separate bank account than the one that is connected to my credit card. I just transfer small amounts of money to my credit card when I need them.

However, this incident was a great wake-up call for me and I’m now a lot more careful when it comes to linking my credit card or PayPal information to different services and games. After the incident I took some measurements to prevent it from happening again. I started using a password manager so I could use more complicated passwords and I also started to use Google Authenticator for two-factor authentication wherever it’s compatible.

Section 2 - Media report almost daily about different IT security incidents. Think back about what you have seen in media in the last few months. Reference these news and have a short discussion about the incident.

Last winter there was big news about the swedish healthcare service “1177” which is a free service that you can call if you wonder anything about a symptom you might have or just about anything related to health. All calls are recorded and logged so naturally you would think that they had taken measurements to preserve patient confidentiality. However, an online magazine revealed earlier this year that all of the recorded calls were stored on an unprotected server in Thailand that was being managed by a subcontractor to 1177 and that it was really easy to reach these audio files without any form of password protection or authentication.(https://computersweden.idg.se/2.2683/1.716432/1177-lackan-vardguiden)

I think the main problem is that people, especially people in charge, are generally uneducated, lazy and naive when it comes to internet security. It’s also seemingly hard to point out who is to blame when massive incidents like this leak happen. In my opinion the people who hire foreign subcontractors should also be held accountable if something like this would happen.

IT security incident.

Game of Thrones, a famous series that everyone talks about it. I kinda like it because it is one of the few series that can keep surprising me the whole time. Early this was its last season, I was so hype since it would be the end om the series (at least for tv-show version). Also, I HATE when I excedent sees a spoil on social media. To avoid this trouble, I tried to watch it as soon as I could.

At some point, I end up watching it on a website that I haven't visited before. The website looks decent, the quality of the series was really good. So I thought "Why not? I need to watch it before someone spoil me anyway". During the epic fight between human and the dead, my laptop started to make to much noise. That noise that you usually hear when your computer is working at high capacity. "What the... ?" I paused the series and try to find the cause of it. I remember that I was so pissed that I needed to pause the series in the middle of the great fight. I checked my task manager, my CPU was working at high capacity. "But how?" I asked myself. I don't have anything running more than Firefox.

"Never mind let's watch it first and find out what is going on later", said the voices in my head. Yes, I did listen to that stupid voice. It always gets me to do stupid stuff. So I watched the whole epic fight with the fan noise in the background, which tires to cool my CPU down.

I did some research after I finish that episode (GG Arya (h)). The website has been using my CPU to "mine" a cryptocurrency. But after the incident, I have been using "No coin" to block all mining script. (NoScript couldn't help me since I need to inactivate it when I want to watch the series).

Google uncovers how just visiting some sites were secretly hacking iPhones for years

Early this year, a Google researcher explained how some of the IOS users might have been hack by just visit a hacked site. Hacker uses the vulnerability in the Safari web-browser to gain root access to their devices.

The iPhone exploits were used to deploy and implant (spyware) which are design to steal files such as iMessages, photos, and live GPS location data of users, and upload them to an external server every 60 seconds. The implant also had access to the victim's device's keychain data containing credentials, authentication tokens, and certificates used on and by the device.

"The best part" is the implant will automatically wipe off from an infected iPhone upon rebooting and leaving no trace of itself. The implant will be reinstalled only if the user visiting the hacked site again

https://thehackernews.com/2019/08/hacking-iphone-ios-exploits.html

---

1. The backstory:

My girlfriend wanted me to download a specific software for her since this was beyond her capabilities. As a good boyfriend I agreed to this of course, without even imagining the tragedy that would follow.

The incident:
As a happy camper I set of on the web to find this software from a good and reliable source, or so I thought…After a while I found what I was looking for and I recognized everything about this software, the way the icon looked, the website for it seemed legit even the installation process was the same as I remembered it to be as the last time I got

this for myself.

Then after installing it and finally running the application (on my own PC) it wouldn't start… I became confused and tried to stop the actual process and restart the application, but nothing happened.

Then I started to notice a few odd things, my web browser started to change my "home page" every time I restarted the browser, it could be anything from betting sites to adult sites.

That's when the "oh crap!" moment came, I had downloaded a corrupt file…So after this I had to sit and uninstall some programs (One malware in particular was hard to remove since to uninstall it I had to enter a password in Korean) that got silently added by the installer and clean up the registry from bad entries and the whole package to get rid of this malware.
After some work and a lot of different tools I finally managed to get rid of all malwares, some bugs still remained though, I couldn't install Chrome again no matter what kind of installer I tried.

The conclusion:
Just because it's looks the same doesn't mean it still does the same thing.

2. Based on this article: https://www.theregister.co.uk/2019/09/04/corethree_baked_private_rsa_key_first_bus_ticket_app/
Discussion:
The incident brought up in this article is that a hacker has found a major security gap in a bus company's ticket application.
He cloned the application and found a private key included in the applications APK.
He then reverse engineered the application and was able to ride the bus for free for a whole year before making this public.
Of course this is not the right thing to do (that is my own opinion) but the hackers states that this was to enlighten everyone that there are a lot of software that are rushed out or poorly secured which could potentially lead to worse incidents than this.
If we keep getting these sort of unreliable applications with poor security, it could mean that people enter sensitive information that might be accessible to other people.

I think this is an important subject to bring up since we rely so much on our smartphones and believe that every application on the app stores are secure.

---

1. Personal experience that I have encountered as an IT Security incidents is that one app I had downloaded got hacked. The app that got hacked was MyFitnessPal that had given the hacker information about my email address, IP Address, Password, and Username.

A consequence that could have happened because of this was that a lot of users are using the same email and password on different websites, which could have been problematic because of the information that exist on this website and being able to get information about other users. In the documentary “The great hack” they are talking about data about people being more valuable than oil today and with this information they might be able to sell the information (including personal information) on the dark web. They might even be able to log in on different payment websites, such as PayPal or Klarna and be able to put you in debt or get money from your account.

I have also had friend that has been hacked into both their emails and on different websites, after they have gotten hacked the hacker then tries to pretend to be the user and sends link to be able to get into more peoples account to see their data which then they can use for selling the data or getting personal information that could hurt the users.

2. An IT security incident that was reported in August was about the new school platform for Stockholm having a breach in their system making anyone that was logged in finding the guardians personal information including Swedish personal number. This breach has now been closed, but there are no comments about the damage that could have been made. It is still a possibility that someone might have used the system and found personal information that they will use, that can give big consequence for the user that someone has taken the information from. Even if this was a short breach, it is hard to know how much the damage has been from this. It has been reported to the Swedish Datainspektionen that will look into this case and hopefully they will look through this problematic issue in detail, making sure that it hasn’t been a lot of users facing problem after this breach. With the new law since last year about GDPR, this is something that Stockholm Stad should have been looking through more before publishing the website, making sure that all this information was safe, with this incident they will probably be more careful with their system in the future.

---

1. For a while ago I accidentally clicked on a pop-up window. This happened without me being aware. I guess I clicked on the screen too quickly or I just had the mouse over a link on the screen that automatically initiated an unknown script. A click was recorded on a window linked to a European selling games website. One day I was notified that I had an invoice to pay. I found an e-mail address to write to and so I started the conversation to have the invoice canceled. The company was prepared to reduce the amount that I had to pay but absolutely not to cancel the entire amount. I started to look for more information on the internet about contesting the wrong invoice. I found a Swedish website where I could read about similar situations and how such a case as mine could be solved. I got advice on how to continue my case with that company. It didn't help all the way. When that Swedish actor became involved in my case, the invoice was quickly canceled. In the end that company wrote to me that they removed my invoice just to show their good will.

2. One event from February 2019 was the 1177 care guide leak. According to media, an unprotected NAS (Network Attached Storage) server was incorrectly connected to the Internet. The IT company's explanation in the media was that an employee incorrectly connected a cord. A large amount of audio files became accessible to the public. The company's VD announced that exactly a cloud-based system was missing its checklists that initiated the extensive leak. During an update, a device received an incorrect IP

address that caused the data leak. One explanation was that the Https protocol was used but the session was not encrypted.

You can think about how operating employee who works with such a system for some reason miss such an important link.

I think about how crucial it is for data security to be synchronized both at the hardware and software levels.

A high-performance file server belongs to a specific network located in a hierarchical environment. A specialized hardware ensures correct and competent data communication.

The software is used to guarantee the highest data security.

Data access is based on complex settings that affect the entire system's network and users.

An incorrect connection between 2 units should be stopped immediately due to correct unit settings. The boundary between LAN and WAN is secured in several ways. I wonder if a cord really can trigger such extensive damage.

1.

My main email has been distributed. This has happened several times. Sometimes the password has also been distributed, but most often only hashed passwords have been distributed. I'm not particularly worried about this, since the only password which has been gained from a known breach, is a password I used 15+ years ago. I got a spam-email saying that someone had videos of me watching porn, and that my email's password was 'blablabla'. These are spam-emails sent out en-masse, threatening to release such videos unless one pays a certain sum in crypto. This is the result of my email having been distributed in, for me, unintended ways. If this happens, it is for example more likely that the number of spam-emails received will increase.

I use the same password on all non-vital accounts which I have, and never save creditcards etc. Then if some random account is hacked, I can always restore it anyway. I only have unique passwords on my 2 emails(I don't use social media). They are both around 35 characters long, with numbers,symbols,upper/lower-case, and are easily remembered.

Check your email:
https://haveibeenpwned.com/

Check your password:
https://haveibeenpwned.com/Passwords

2.
In June 2017, a cyberattack was launched against the Danish shipping-company Maersk. The attack was part of the NotPetya-attack(which locked a system and demanded a ransom – which led to serious consequences for certain patients in hospitals which were affected), and caused disturbances at several of Maersk's terminals for shipping. In the end, the bill for dealing with everything related to the attack (they fixed it themselves) and the aftermath, landed at around 200-300m usd. Of course, Maersk controls around 20% of the world's cargo, but 200m is still a huge sum.

# https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#1ac8829b4f9a

# https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

In July 2019, the Croatian government was reported to have been the victim of a cyber-attack. It was a phishing-attack, urging people from the Croatian state or government to download a file, which when run would activate a script which downloaded malware to the computer. If this happens, and the malware is a, for example, Remote Access Trojan, and the script is run with root-privilieges, then the whole system is compromised and nothing on it can be trusted. If this happens to a government-related entity, that means that the political system has been compromised, which of course is very problematic and serious for the political system in question.

# https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

In 2010, the virus Stuxnet was identified. It is believed to have been manufactured by Israel's security services, in order to hinder Iran's proliferation of nuclear weapons. Iran had secured their nuclear site with an airblock – meaning that the site was cut off from the outside IT-world – but Stuxnet infected the site anyway. It did so by first infecting USB sticks, which later were used on-site.

# https://en.wikipedia.org/wiki/Stuxnet

I've used these three examples, since they highlight different aspects of cyber-attacks. These examples exemplify how cyberattacks can be used for achieving many various results. Stuxnet was seemingly a military operation, akin to physically attacking the nuclear site. The attack against the Croatian government was probably a political attack, perhaps launched in order to gain information about the internal political system or process of Croatian politics. The NotPetya attack was an economical attack, seeking to enrich the hackers. Cyber-attacks can target the whole of society, and therefore the whole of society has to be protected from them.

Personal IT security incident
In a previous course on server-based web programming one of the assignments was to serve a web application behind a reversed proxy on a production server to a public IP address. The web application was a simple javascript server that fetched data from a

third party API and presented the data to the end user. The reversed proxy was served by a NGINX server which main purpose was to redirect HTTP traffic to HTTPS. The server was hosted on OpenStack by the Linnaeus University and both services was running in Docker containers.

While I was my testing my setup, controlling that everything worked the NGINX server started getting malicious requests for various files. As far as I know it was the first time outside malicious activities directly targeted something I programed and configured. And it was interesting to be able to watch it happen in real time.

All the requests were from the same IP adress and was all requesting different variations of administrative php files for what seems like WordPress and Joomla hosted sites. For example it requested files and directives such as admin.php, wp-admin.php and administrator/index.php. The frequency of the requests were maybe 10-15 per second. To me it seems like I was the target of quite basic malicious web crawler specifically made to scour the web for easy targets, most likely self-hosted personal blogs by less tech-savvy people. On a 200 status for a request my guess is it would start to brute force an administrator login with the usual admin/admin, root/root credentials. A quick google reveals that these kinds of attacks are commonplace and frequent for most if not all websites.

Nothing of importance was on/in the server, containers and application and the attack was clearly targeted against something very different from my configuration. Plus the server would only be up for a couple of days. Though I did update my NGINX configuration to combat the web crawler. First of all I denied all requests for any kind of .php file and secondly put anyone who requested such in a very restricted limit_req zone, something like 1 request/day.

Media reported IT security incident

One media reported incident I remember is the 1177-leak which exposed 2.7 million recorded phone calls made to the 1177 service. Computer Sweden revealed that all phone calls since 2013 was stored completely open on a public IP address without any password protection on an unencrypted port 443. It seems like there has been zero thought of security and integrity on a fundamental level throughout the city councils and the number of companies and daughter companies involved in the process. The data stored is particularly sensitive in nature and falls under 'patientdatalagen' which you'd think warrant extra security measures to ensure its integrity. I think its clear that the people involved in the decisions on public procurement needs to be further educated on the importance of quality and competence when dealing with digital services and data storage.

IT security Incidents personally experienced

One security incident that comes to mind happened back in 2015. I used a website called haveibeenpwned (https://haveibeenpwned.com) to enter my email address and it would list all data breaches my email address had appeared in. At the time I was registered to a forum that had recently had a security incident and data was leaked. Information such as email addresses, passwords, IP addresses and personal information was leaked in the security incident.

One consequence following the security incident lead me to change my password, and make sure that same password wasn't used somewhere else, since it could lead to another personal security incident, following the leak. After this security incident I sort of realised the importance of having unique passwords for everything, and with these kinds of security incidents, other platforms can easily be attacked if the same passwords are used.

Another consequence and something I had in mind was to be wary of phishing links, related to the forum that had a security incident. Although I never received any phishing links about it, it was still something I had in mind. Since personal information was released along with email addresses, a phishing link could look legitimate.

Media reports of IT security incidents

Last month there was a security incident regarding a school platform used by pupils in Stockholm. Personal identity numbers and school results for 140,000 pupils were available to all users on the school platform [1].

Considering the fact that the school platform is created and used in the public sector, I think there are higher expectations of confidentiality versus a company operating in the private sector. But for the past few months and year, I have personally seen more security incidents coming from the public sector than from the private sector. The information that was made available was also mostly personal information about minors, which makes it more sensitive in my opinion.

There was also reports of a subsequent security incident in the same school platform where names, phone numbers, addresses and email addresses of guardians were made available to search for, by logged in users on the same school platform [2]. Luckily in both of these security incidents, you had to be authenticated on the platform in order to retrieve the data, therefore the consequences may have been less severe.

[1] SvD.se. (2019). Ygeman om dataläcka: Det är upprörande. [online] Available at: https://www.svd.se/personnummer-lag-tillgangliga-pa-skolplattform [Accessed 7 Sep. 2019].

[2] StockholmDirekt. (2019). Ny dataläcka i Stockholms skolplattform. [online]. Available at: https://www.stockholmdirekt.se/nyheter/ny-datalacka-i-stockholms-skolplattform/repshA!vGU0UDaYlLN8pTZ2oQGA1g/ [Accessed 7 Sep. 2019].

Computer security is one of the most , if not the most, important part of the current technological environment.

To keep confidentiality, integrity and availability of information at the highest standards companies have developed security policies.

These policies make sure that the data is not corrupted , keep it secure from wrong hands and it is available at all times.

Except from active attack from 3rd persons, individual mistakes may cause unwanted results.

In my case exactly that happened. When I was in the first year of high school, I shared a laptop with my small brother.

Using that laptop I did my homework and other errands. We submitted homework using the a student portal much like mymoodle.

One day I had forgotten to log out from that portal. At the time I didn't know that it was such a huge mistake.

Using my profile, my little brother had sent quite mean messages to some of my teachers. I had to learn this when one of them called me to his room to talk about it.

To make long story short I had to make a few uncomfortable conversations with some of my teachers.

In my case it was just a minor issue. The most harm caused was my embarrassment. But other security policy violations may cause drastic harms.

For example there was a security breach at Early Enterprise restaurants. The breach took place between may 23rd 2018 to march 18th 2019 so for 10 months.

2 million credit card numbers were stolen. On 21 Feb 2019 KrebsOnSecurity contacted them when they discovered that the credit card data was being sold in the cyber crime underground.

The data sold included credit card number, expiration data and in some cases credit card holders name. How ever company came clean about all this in 29 march 2019.

I think this incident summarize how important data security is. In this case lots of innocent peoples money might be stolen and the company will be in a lot of trouble.

I also believe that the company didn't handle the situation well by coming out really late either. Even though sometimes security breaches are unavoidable, companies should

come up with a solid security policy and train their staff accordingly.

1. Describe IT security incidents.

The most recent IT security incident I faced was on one of my relative's computer. It was a ransomware that had encrypted all the files stored on the hard drive of his computer. The data was still on the hard drive, but had an additional extension called ".5tpe4". For example, a file named "readme.txt" would have changed to "readme.txt.5tpe4". And of course, it was impossible in any way to read any of these files.

On the computer desktop, the ransomware had automatically created a .txt file with indications about how to restore all his data. The hackers that made this ransomware were asking for $1500 payed in bitcoins in order to have the data retrieved.

The first thing I did was to turn off the computer, in case every file wasn't encrypted yet. Then, I booted the computer on a USB drive where I had mounted Ubuntu. In that way, I could access to any of the hard drive files without launching the installed operating system (Windows 10). Unfortunately, I didn't find any file that weren't corrupted. I was advised to share 2 of the encrypted files to a website called "nomoreransom.org" that allows any company or individual to have a database of every existing ransomware.

Then, I tried to install Kaspersky Internet Security to run a scan on the computer so I could maybe detect from where the ransomware was coming from. But I couldn't install the software because of the ransomware. Then, I had to use a CD on which I mounted another version of Kaspersky. Then I booted the computer on this CD and succeeded to scan the computer, but it didn't work either.

We obviously didn't want to pay to retrieve the data, so I proceeded to wipe out all data from his hard drive and reinstalled Windows 10.

2. Security Incident in the medias.

As a Security Incident, I would like to talk about NoMoreRansom.org that is an indicator of how the Internet is not completely secure and people have to work to make it a better place. This website is three years old and yet it has helped over 200 000 victims according to "The New York Times". Saving for the victims around $108 million of ransom. This initiative was started by the National High Tech Crime Unit of the Dutch Police, the European Cybercrime Centre, Kaspersky Lab and McAfee and has two main purpose: finding a solution to these scams on the internet, and educate internet users on understanding and preventing these kinds of attack.

So far they succeeded to decrypt these ransomware : "Syrk", "JSWORM4.0", "IAMSooRRY", "Zerofucks", "Mira", "Gandcrab (V1, V4 and V5 up to V5.2 versions)", "Getcrypt", "JSWORM2.0", "MEGALOCKER", "ZQ", "PEWCRYPT", "HKCRYP" and some more. That means that if any user is infected by one of these ransomwares, it is possible for them to install a software on nomoreransom.org that will decrypt any corrupted file.

They are also collecting corrupted files from other user's infected computer in order to maybe find a way to counter new ransomwares.

1. Personal experienced IT security incident

One of the most severe security incident happened to me about three years ago. We have just finished project we were working on. Project team was released and returned to theirs departments. My team had to move to anther office. Unfortunately in the new location it was not possible for our IT department to setup public IP which was needed for some services (licence servers, web server and forum) we were still providing. Therefore to avoid this problem physical machine was left in unused utility room in previous location where it could obtain public IP. What is important others members of finished project was in that location.

One day someone noticed that the project web page is down. We could not reach also none of the VMs remotely, after trip to phisical location we found our server up and running all services and VMs available from localhost. But there was no Internet connection. Then our IT department answering our question about the issue confirmed that one of our server were used in DDoS attack and they put interface down to stop attack.

Cost of acident – in our organization, it did not cause data loose or other cost then system recovery and stopping services which were not critical, additionally it may by consider as an image failure.

Recovery after incident. Environment was set up from scratch on newest OS and software. Data were recovered from backups. Then the server was placed in our location and we were granted public IP (specially for this server). Also responsibilities for server adminstration was set up clearly.

Reason: lack of clearly shared server administration responsibilities.

2. Media incident.

In august press relies info about Suprema ("global Powerhouse in biometrics, security and identity solutions" - web page info) biometrical data breach. It affected 27.8 million records including fingerprints, facial recognition data, employees photos, passwords, logins, addressees total 23 gigabytes of data and that according to press relies could affect 5 700 organizations in 83 countries.

Description of incident: Group of Ethical Hackers discovered that databases containing highly sensitive and unsecured (no passwords nor cryptography) data where available under public IP. There are still no information if the data was stolen or misused.

Consequences: This accident affected personal (biometric data) of thousands of users. In case of password reveal to neutralize this situation is just to change passwords. In case of biometric data it is impossible to change fingerprints or iris (probably only after surgical intervention under condition of possession another Iris),
therefore all biometric security in case of people that were affected are compromised for the rest of theirs life. To prevent this situation it was enough to use cryptography or storebiometric data as hashes. As system stored data about access rights/rules to some facilities, IT systems and networks. It is reasonable to ask if someone could

gain unauthorized access to any information assets or facilities by adding own records to data set or hide tracks of hostile operation in facility, IT system or Infrastructure by deleting logs from data set?

Another interesting case is how global security player could allow such situation? Why sensitive data was not encrypted or hashed? Why passwords were stored as plain text? How internal security is being executed? Why right security mechanisms did not work?

Cost of accident is hard to calculate yet it could be considered that in European Citizens affected by breach could try to bring legal proceedings basing on GDPR.

References:
https://www.nytimes.com/2019/08/14/opinion/ransomware.html
https://www.nomoreransom.org/en/index.html

1.

The first thing that comes to my mind when I think about IT security incidents is the time when my account got hacken. This was like 10 years ago when I was a kid and one day when I logged in to my World Of Warcraft account so did I notice that all my gear and gold was gone from my account and that was when I notice that my account had been hacked.

And as a kid I freaked out because all my things was gone. I contacted blizzard to ask if they could help me to get back my gear and then I needed to wait for a day or so for them to reply to me, but then I was lucky because I got all my things back so nothing was really lost, but before that happened so was I worried. I can't really recall how my account got hacked, if it was something that happen to blizzard or if it was my fault. But after that day so have I been using Blizzard Authenticator for my account for extra protection so if someone have my password so can't they log in without the right code from the authenticator.

2.

The news that stand out for me is from early 2019 when it comes out that Facebook have been saving passwords in plaintext and that between 200-600 million accounts were exposed to facebook employees. And according to the news so did around 20 000 employees had access to the passwords.

The reason why this news sounds so bad for me was because I was taking a course in server based web programming and there we learned that you should always hash a password that will be saved and you can also salt the password to make i more secure. When you have hashed password so can't you translate that password to plain text it's a one way only, you only compare the user password to the saved hash. It's a bit of a chock to me that a big company like facebook is saving password in plaintext and I don't recall if they had a reason behind it or if it was a simple mistake by them, but 200-600 millions accounts isn't a small number.

1.
A few years ago, my friends Instagram-Account was hacked. From one moment to another she was not able to get into her own account because somebody had changed her password. She got an email from Instagram that somebody had logged in to her account from another computer. She recognized that it wasn't her who had logged in. But when she saw the E-Mail it was already too late and she wasn't able to use the reset link that came with the Mail anymore. As a consequence, she was not able to use her account for a few days and the hacker used it to follow people that she didn't know. After contacting Instagram about the incident, she was able to get her account back. For this she had to prove her identity by showing them her ID-card.

2.
A few weeks ago, I read about some security issues of iPhones in the guardian.

An external security team of Google found out that by using hacked websites hackers were able to transfer malware to iPhones. Just by visiting the hacked website the malware was able to get on to the iPhone. The hackers than had access to the user's location, their chat histories, their address book and all passwords that were saved on the iPhone. The access to the device is lost whenever the Phone is restarted.

But it can still do a lot of harm in the meantime. And at least access to accounts of the user are still available to the attacker. The attacks were going on for about two years. According to Google it took Apple about 6 days to fix the flaws after it was reported to them on the 1stof February. Apparently, this specific security issue is fixed by now but that doesn't mean that iPhones are save from other attacks.

The article in the guardian warns users from trusting their phones with every detail of their personal life and urges them to think about the possibility that one day this information could end up in the wrong hands.

For me the idea that somebody could gain access to my personal information without me knowing about it is shocking. And I think that for many people the possibility that somebody could steal their personal data seems to be a very unrealistic scenario and for this reason they don't think twice before saving their data on their phone or computer. So, the fact that the danger is very real should be made more known to users.

I'm referring to the following articles.

https://www.google.de/amp/s/amp.theguardian.com/technology/2019/aug/30/hackers-monitoring-implants-iphones-google-says
https://www.zeit.de/digital/datenschutz/2019-08/apple-iphones-hacking-chats-websites

---

Personal IT Security incidents

I have not experienced any big security incidents that have led to any consequences for me.

A couple of years ago I received a call from "Microsoft" that told me that they had discovered a problem with my computer. But this didn't lead to anything because I realized that this call was not from Microsoft, so I hung up.

I have also received possible vulnerability scam (phishing) emails from unknown senders, but I never open an email from an untrusty source.

Since you always see a preview of the beginning of the mail it makes it possible to get an impression if it's a serious sender or not.

I'm also very careful about buying things from different websites. If it's a company that I don't already know about then I will always google the company before I buy something from it. If there are any other sites that I already know about that has the same product, I choose that one instead of the unknown site.

I think it's important to be careful and a little bit source critical in order to avoid possible attacks.

IT Security Issues in Media

I have read the article: https://www.aftonbladet.se/nyheter/a/LA481p/telefonbluff-mot-aldre--tomde-konton that is about fraudsters calling older people and says that they calling from their phone operator fooling elders to create a new bank-id that gives the fraudster access to their bank account.

The security for creating a new bank-id has been changed since the article was published. Today you need to scan a QR-code to be able to create a new bank-id if the two units do not share the same network.

But it's still possible for the fraudster to transfer money between different accounts if they can fool the person to use bank-id three times. Once for logging the fraudster in to the bank site and once for adding a new bank account to transfer the money to and the last one for confirming the transaction.

Maybe a QR-code could be used every time a customer wants to log into his/her account. Just to make it harder for the fraudster to get into the victim's bank account.

I sometimes think about the security on Facebook compared to bank-id. On Facebook you get an email if someone logs into your account from an unknown unit. The units from where someone has logged into your account and where this unit is graphical located is also possible to see.

It is also possible to change the settings, so you must use two-factor authentication (2FA).

On the other hand, we want bank systems that are easy and fast to log into. We want to be able to have access every time of the hour to our bank account. And nowadays when the bank offices disappear, you as a customer must have "internetbanken" to be able to pay your bills and live your life. This means that the age span of the customers are quite broad and the experience of working with systems differ a lot from customer to customer.

If we want to make it more difficult for the fraudster to log into our accounts by using two-factor authentication. We also make it more difficult and time consuming for the users to log into his/hers accounts. People with bad skills in software and computers might not be able to log into their account without help. So, we want it easy for the customer but hard for the fraudster. Fulfilling both those requirements might be hard.

Section one

During my last job I found a security vulnerability in the computer systems of that company. During that time I was using an USB-Stick, which contained some space for storing data and a Linux distribution.
One morning I inserted that USB Stick into my working laptop and started the computer. It booted Linux. I wondered why (normally it should only boot the main system and not the stuff on my USB-Stick) and found out, that the bios was configured to do so.
The company used that mechanism while preparing the computers for work, and never changed it.

Anyone with a malicious USB-Stick could access that computer. If the attackers stick wasn't used first, he could just access the bios and use it from there. There was no protection for the bios ether. Not even a password.

Together with another student, we did some research and found out that there was no protection of the main disc either. Anyone who had a boot stick got access to the device and all the files on the computer. We could even install a small script which was started during the next start of Windows.

After we doublechecked everything we contacted our It-supervisor. He thanked us for our work and said that he would look into it. He also said us that our flaw would not be a problem, because no one could access the computers (which were also used for home office)

Section Two

A few weeks ago, the research team "Project Zero" found a big malware campaign against iPhone users.

The attackers managed to infiltrate multiple websites and used them to deliver their exploit. Using a bug-chain in the Safari browser and the kernel, the hackers managed to get access to all functions of the IOS-system.

To be exploited it was enough to visit an infected website, but they were not permanent. After a reboot, your iPhone is “save” again.

Even if we don’t know who the attackers where, they must have a lot of resources. They used a few 0-Day exploits, which are worth a lot. Normally attacks like this are very specific with their targets. In this case the attack was very widespread.

(source: Heise.de)

Personal experiences of IT security incidents

I am quite lucky because I have never been exposed to any major IT security incident. About five years ago, I was exposed to spam emails. There were about 1000 new unread emails a week if I did not delete them daily. The worst consequence of this was that I missed many important emails that ended up in the middle of all spam. I had only one email account at that time. All invoices, work-related stuff and non-important subscriptions were linked to that particular email address. Today I have three different email addresses to minimize the risk of this happening again. I have my main email account that I use for the most important things such as invoices and work-related stuff. My second email is for subscriptions and auto payment receipts. The third one is my garbage email that is used for memberships on questionable and unserious web sites. If I get spam emails on that address I really would not mind.

Today I have an ongoing IT security incident. There are several Instagram accounts with similar names to my account using my profile picture. These accounts are spamming other users' images and I have been trying to get rid of them for the past two years. My friends and I report these all the time but there are still several accounts left today. There is no major consequence for me over this incident except that it is embarrassing for me to be associated with those accounts.

IT security incidents in media

For about two weeks ago, there was a quite serious IT security incident. Security vulnerabilities were discovered in the online school platform of the City of Stockholm (https://www.nyteknik.se/sakerhet/stockholm-panikstanger-skolplattform-chockerande-att-sakerheten-ar-sa-dalig-6968823). It was a dad to one of the students that discovered the security issues. He was wondering why the platform was so slow and wrote a simple script, which sent a sequence of calls to the backend system. He quickly saw that the calls contained far too much data and also information that should not be there. He could get the names and social security numbers of all the teachers in the City of Stockholm, as well as the teachers' reviews of the students. In my opinion, this incident is serious as the dad explains that he is not an elite hacker but just a regular web developer who managed to come across all this information. A project that has cost over 900 million SEK and with more than 360,000 users should not have such a low level of security.

I think one of the biggest problems today in terms of IT security is the very low level of security, especially in Sweden. Maybe ten years ago, today's level of security could be considered very high, but the situation is different today. Today there are more and more people who know how to code and it is not a unique knowledge anymore. As technology evolves, so does people's knowledge of technology. Therefore, it is unreasonable if companies and organizations still use the same security thinking as they did ten years ago. If a simple dad working as a web developer could discover this problem, the question is really who else came across the database before it was shut down? In Sweden, I think the security strategy needs to be improved, especially concerning systems belonging to the Swedish government. Remember the 1177 leak that hit Sweden about a year ago?

IT security incidents that I personally have experienced

I have taken a phone Note 5 Samsung and some one took that phone. Luckily the phone was new I didn't have data inside it like media or phone numbers but I did two mistakes.

First the phone was not locked and I have added my credit card details in Samsung pay. As my Bank number is in that phone so all my purchase information is going to that number and

due to Contactless payment systems the person who took my phone spent nearly 5k SEK in 3 days. Then after 3 days I blocked my card but its too late.So there after I avoided to use Contactless Payment from Smart Phone and have enabled fingerprint lock system

Three years back I was working on Defense Project in India. The rules were very strict for code development or any kind of activity you cant open google, smart phones need to be submit at reception etc. Project time was very less and our company was hiring freshers as well. So one day suddenly one fresher was fired from our company and we were shocked to know the reason.

On last Sunday that employee call one of his experienced friend inside that project area and they both fixed the code which should not be disclosed to anyone. His friend was neither in that project nor in our company and when security asked he lied about his friend.

Media report almost daily about different IT security incidents

Classic case of Card Clone in India

Recently I heard about Cloning of card in India. Now what the hacker is doing they are going inside the ATM machine and put one device where you insert your ATM Card and some device to capture the Pin.

Each Debit card has magnetic chip which contain the data now hacker machine read the strip and capture vital information.

The data then copied to blank card and there are pin holes cameras to read the pin when user type it on ATM Keypad

Some victim loses 24k SEK in 15 min with 20 transaction

---

1. In a company that had several networks separated from each other by classification levels, an employee scanned a classified document on a device connected to a network not designed to process information having the classification level of the scanned document, which resulted in having higher classified information in a network that was not designed to process such information according to the information security policy. While it had legal consequences for the employee, who had signed and thus confirmed to have understood the security policy, the device, which had also a hard drive storing scanned information, was not allowed to be used in its intended network any longer, but in a network having at least the same classification level of the scanned document since it stored from this moment on a higher classified document in its hard drive. This incident had also an impact on availability.

In another case, it happened that a printer of a department was suddenly not accessible anymore, neither for the department's member nor for the system administrators. After a long time of troubleshooting, it turned out that the IP-address has changed for an unknown reason. Sometime later the same problem occurred again and it turned out that a department's member, unexperienced in IT, tried to change the configurations for a printout on the printer's console and by accident changed the IP-address without telling anyone what happened, either because this employee was totally unaware of the consequences or hoping no one would discover the cause of the issue.

2. https://www.wired.com/story/ios-attack-watering-hole-project-zero/

An attacker performed watering-hole-attacks over a long time, which has been discovered by google researchers. The surprising thing about that is that the targets were iPhones, which were considered to be very secure. However, there were a number of vulnerabilities exploited to get control over the iPhones. This incident, which affected many users, shows that you could never rely only on security mechanisms, the only thing you can be sure is that if you did not realize being hacked you did not notice being hacked. It is advisable to assume that someone might spy your actions and information, especially when you have no control over the security mechanisms and their implementation.

https://www.theverge.com/2019/6/13/18677282/telegram-ddos-attack-china-hong-kong-protest-pavel-durov-state-actor-sized-cyberattack

An DDoS attack was launched against the encryption service Telegram, which China was blamed for. The reason behind this attack was obviously to prevent users from Hong Kong from encrypting their messages, which should protect them and their actions against the local authorities. This is a typical scenario for corrupting IT availability for political reasons. While in this scenario it was obviously a state who was the actor, it could be any group or individual with political interests in general performing such actions. Anyone could be target of such attacks, since everyone belongs to some kind of group, which might be ethnical, religious political or anything else.

When downloading free software, another piece of software was bundled into the application installer and was therefore installed on the workstation that the free software was installed on. The bundled software can be considered spyware (collects data on the information system it is installed on and sends it to an undefined location). This particular security incident could be resolved by uninstalling the bundled software due to the spyware software was benign. The consequences for this security incident were very mild, in the worst case scenario some information regarding the information system was sent to the developers of the spyware and the best case scenario there was no consequences.

In 2012 the cloud services provider Dropbox underwent a data reach where essentially all of their customers email addresses and passwords (salted and hashed with SHA1/bcrypt) were disclosed. Dropbox forced a password reset in 2016 were users had to change their passwords. The consequences for this security incident was dire, the author's email was exposed which has resulted in spam and phishing being sent to the email and the salted and hashed password is disclosed. While the salted and hashed password may not have been broken yet, that particular password is no longer used for security purposes.

Recently there has been a wave of ransomware (cryptovirus that encrypts data on the information system that is infected and demands a ransom to decrypt the data) that has targeted American dentist offices. Ransomware attacks has been on the rise in the last couple of years with notorious attacks such as the Wannacry attack.

In the case of the ransomware hitting the American dentists, several victims have decided to pay the ransom to decrypt their data (patient personal records and so on), this is fairly common for the ransomware attacks and is most likely one of the prime factors in why these type of attacks are popular amongst hacker groups, it provides the hackers with a large quantity of financial income.

Source: https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/

The cyber security company Sophos recently found a vulnerability in the rendering engine Blink that is used in several web-browsers including Google Chrome versions older than 76.0.3809.132. This may prove to be a large attack vector due to the users of personal computers habit of not keeping the software up to date and the long application packaging process for medium to large companies.

Source: https://techworld.idg.se/2.2524/1.722871/sarbarhet-chrome-attack

The Android application CamScanner which can be used to produce PDF documents using the camera on cell phones has been found to contain malware which is used to gather log-in data from the device it is installed on. This malware was found by the Russian cyber security firm Kaspersky Lab. The application has been downloaded 100 million times which mean that a large quantity of devices have been infected.

Malware on cell phone applications (in particular on Google's Linux based Android operating system) is another global security trend. This most likely has to do with the increased usage of cell phones and the data stored on these devices in the last 10 years.

Source: https://thenextweb.com/security/2019/08/28/malware-found-in-document-scanning-android-app-with-100-million-downloads/

Personal IT Security incident

The incident described in this text is one of the reasons i started to care for internet and computer security. When i was young and unfamiliar with the dangers of the internet i experienced the devastating effect of a computer virus. It was around the time that MSN Messenger was a popular tool for teenagers to communicate and so me and my friends as well as the rest of the school used it. One day when i logged in i had a notification that my friend had sent me a link and the message said something like: Do you remember this picture?

Since it was a message from my friend i did not hesitate to press the link. Doom erupted. The malicious code had in a couple of minutes turned my beloved PC into a potato and the tragedy was a fact.

The result of my mistake was not only that our PC had to be sent for repairing but also the feeling of mistrust. The link that i had clicked which looked like it was sent from my friend was ofcourse a generated SPAM message used to spread the malicious code. That incident taught me to always think twice before clicking any suspicious links.

IT Security reported in the news

Here comes a daily reminder to always keep backup files locally and that the convenience of cloud storage isn't always complete total solution.

Two sites that report of the same incident:

Swedish: https://computersweden.idg.se/2.2683/1.723105/kunder-drabbade-stromavbrott-aws

English: https://www.bleepingcomputer.com/news/technology/amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe/

The site Bleeping Computer reports about a Amazon Server in North Virginia that as a result of power failure lost customer data. The incident happened August 31.

Incidents do happen and i am sure that Amazon is working hard for damage control but i personally find it remarkable that the company (and other similar like Dropbox) do not have any further responsibility to compensate the customers economically when their data is lost. The service they provide is storage and they sell it with words about the importance of backup and convenience of cloud storage.

Section 1: The supermarket's 'admin' panel.

To add a little context to the story, I should say that I happen to have a couple of friends that are somewhat experienced hackers. They are what you would normally call 'white hats'.

At some point during my second year of university, one of these friends and I were talking about supermarket exclusive promotions, that are sometimes advertised via internet, and about how some of them even have their own website. This was, of course, the moment when we started looking for the most suspiciously odd-looking promos we could find.

After a while, we casually ran into a not very good looking webpage by a renowned supermarket operating in the Canary Islands. Some links on the HTML were dead, the style and shapes on the interfaces were a bit off, etc. My friend then told me that it could be possible to break into the webpage's 'admin' panel, since chances were that the makers hadn't put much thought into it.

For the record, an admin panel is typically a tool for remotely controlling the views, resources, widgets, and many other things that the user can see and/or interact with on a website. Therefore, if you take control of the admin panel, you have full control of what is displayed on the webpage and, if you get lucky, of some resources stored client-side.

Turns out he was right. Not only the admin panel was easily accessible (www.name_of_the_company_prom.es/admin), but you could even skip the autentification required to have access to it by directly accessing (www.name_of_the_company_prom.es/admin/admin1), which should, of course, be explicitly avoided but wasn't.

Long story short, we could've won a couple of products for free and this is a clear example of how not to run a website.

Section 2: Massive user data leaks

It's become an actually quite common topic, the one related to security breachs and huge data leaks. This is because nearly everybody has a web account that includes personal information of some sort, and because said information is perhaps too often too vulnerable.

Of course it is both convenient and somewhat dangerous to store your personal information somewhere out of your control. You are basically lending your data to a third party, which from that point becomes responsible of keeping it out of undesired hands.

Nowadays, almost every decently big company has a database where client information is stored. From transactions, if any, to addresses and IDs. This would mean that breaking into one of this databases is a big deal.

Like in the case of Hostinger [2] and Luscious [3], when user information is exposed, they are the mainly affected party. Nobody wants his data collected by companies that they haven't personally allowed to, specially if it comes to bank accounts, addresses or even worse. In cases like the security breach at Yves Rocher [1], it could be as specific as to give the attackers information about the clients habits or amounts payed for a single product.

In this sense, information could also be utilized by other companies to do targeted marketing to their breached competitors, so it is definitely not an ideal situation to be in for the affected company, that can also earn the distrust of its users.

That is why, in this informatized world we live in, prioritizing security is always a wise choice.

Sources:

[1]https://www.infosecurity-magazine.com/news/data-leak-affects-25m-customers/
[2]https://www.infosecurity-magazine.com/news/hostinger-breach-prompts-mass/
[3]https://www.infosecurity-magazine.com/news/users-of-adult-website-exposed-by/s/

Introduction

IT Security is the protection of organisational assets such as computers, network devices and data from unauthorised access as well protecting them from disruption or misdirection of services that they provide [1]. IT Security is a common topic in the IT world since some of us have been victim to an IT Security incident or might have witnessed one. This report will be divided into two sections, the first describing security incident that i myself have personally experienced while the second part would be about security incidents that have been reported on the media

Section 1

Personally i myself have not really experienced any serious security incidents such as bank account or credit card details being stolen or a device being lost carrying important information or even an account of mine being compromised. But I have on many occasions forgotten a password to an account if that counts as a security incident. Well the consequences of that was that i had to try and come up with a new password that was not used on any other account, that was longer than 8 characters and that could be remembered without it being a too easy or that could be found in a dictionary or such. But apart from that nothing too special has happened

Section 2

A recent security incident was a ransomware attack that affected over 400 dentist offices across the US[2]. The incidents occurred due to vulnerability in the software used by dental offices. The Hackers used those vulnerabilities to deploy the REvil (Sodinokibi) ransomware on dentist computers across the US. The attack occurred apparently during the weekend but was only first noticed the following monday when Dentist offices tried to get patient information but where locked out and where presented with a ransom demand. The amount needed for the ransom was not presented to the public and it has not been directly confirmed form the clinics themselves if they paid the ransom but some sources say that some clinics might have paid in outright desperation [3] although it is usually not recommended to pay hackers since it only ignites more attacks. Its has not yet been confirmed though if patient data such as social security number and other personal information were stolen in the attack.

References

1. Cisco, "What is It security? ".[online]. Available:https://www.cisco.com/c/en/us/products/security/what-is-it-security.html

2. Catalin Cimpanu, "Ransomware hits hundreds of dentist offices in the us", ZDNET, 2019.[Online]. Available:https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/
3. Michel Kan, " Ransomware attack hits 400 dental offices across the us", PcMag, 2019. [Online]. Available:https://uk.pcmag.com/news-analysis/122382/ransomware-attack-hits-400-dental-offices-across-the-us

---

Internet Security Pre-Assignment

As i do not have any professional experience in IT, i find it difficult to remember IT security incidents that resulted in any real consequences. Sure, forgetting usernames and/or passwords does happen, but the only consequence to that is resetting said password or requesting that your username is mailed to you, and these consequences are mild inconveniences at best.

The one time i can remember having concerns about the security of my accounts was when i first found out about the website haveibeenpwned.com, a website that checks publicized security breach incidents and whether your email was a part of the breached data or not.

The first time i checked that website, i found that accounts tied to my email accounts had been breached 12 times (the number has now risen to 14) and that did cause me to worry a bit, since i'm one of those lazy people who uses a similar password for almost all accounts.

However, i have not noticed any real consequences to those breaches, no real suspicious activity on any of my accounts (that i frequently use at least). It did however make me realize how important two-factor authentication is. Since almost all of the services i use offer two-factor authentication, i'm not too worried about the accounts i have being compromised, since the attacker would also have to gain access to either my phone, which is very unlikely, or my email account, which i have set up with a secure password.

I am aware that this is far from the optimal setup for security, but i feel that it is good enough for a private person that has a very low chance of being directly targeted by hackers.

As somebody who doesn't keep themselves very up to date with IT security news, one of the few relevant articles i remember reading recently was about BlueKeep.

BlueKeep is a vulnerability in RDP in older Windows systems, namely XP, Vista, 7 and also Server 2008/Server 2008 R2. It was publicized and patched on the 14th of May this year, however, there are still a supposed 700 000 systems publicly exposed on the internet that are still vulnerable to the exploit.

BlueKeep has been compared to the EternalBlue exploit, which was used by the malware known as WannaCry, that infected more than 300 000 systems in just a few days in May 2017.

Last friday, September 6th, a framework was released using the BlueKeep vulnerability.

This is some fairly scary news considering that the EternalBlue framework was released a month before the famous WannaCry attack. While EternalBlue was a more polished framework compared to the BlueKeep one, it is still very potent.

This news also highlights the importance of keeping systems up to date, even if said systems stopped receiving regular updates years ago.

I worked as a network technician (in 2000) and the chief executive of the organization had arranged his own entrance, which was configured according to his recipe, which he used for several years. This entry was hacked and various things were written on our official web. He didn't listen to me so I brought in a security company to help me convince him.

After a rigorous review and demonstration, the manager said he understood it all, but we were not allowed to touch his entrance. He got what he wanted (he decides) until it happened again, only then did we have to rebuild the net to remove his entrance and stop more intrusions. This cost some goodwill for the organization.

NASA has had problems with an astronaut checking the ex's bank account through the ISS, space station.

It opens up new dimensions of security, are some categories so ignorant that they don't need to be checked or are we all just people? Can a higher degree of integrity be required in some cases? You probably expect people to be people and you do what you think you can get away with, "the moment makes the thief". You also need a motive, why do it? In this specific case, the person was probably driven by strong emotions that were difficult to resist. If the astronaut in question had known that what they were doing might have been logged, it might have been avoided, but there are those who ignore the aftermath. It may well depend on the purpose of the intrusion, here it was a one-time opportunity to quiet her personal curiosity. You have to create groups for different data there is probably no astronaut who needs that kind of access in her work. You can build access in different ways and that everyone to a certain degree has the same access throughout the system may not be so good, then the principle least privileged is better.

---

1. When I was in school, we could bring our phones but we had to leave them in a basket at the teacher's desk before class started. One fateful day, we came back from break to find that all our phones had disappeared. The entire class panicked and demanded that the school perform a spot check on everybody until the phones were found as they contained personal and possibly sensitive information on top of the fact that the devices themselves were of value. In the end, it turned out to be a prank from a student in the other class (who ended up getting detention) but this incident caused our class to be more aware of security be it physical (making sure the windows and doors to our class were locked during breaks), convincing the school to set aside a budget to install CCTVs, providing us with a more secure option to store our mobile devices as well as backing up the data on our phones to a separate secure location.

2. After the Facebook-Cambridge Analytica scandal in 2018, Facebook is still making a regular appearance in security news. Recently there have been several security reports that prove that Facebook had database servers without any password protection that were publicly accessible and exposed the names, genders, countries and phone numbers of more than 400 million users worldwide [1]. Facebook claims that the information leaked is old, however, several test using the leaked Facebook IDs and phone numbers proved otherwise. Another security report involving the leak of more than two billion logs which included information such as usernames, passwords, emails and even exact geo-locations of the users was published involving Orvido Smart Home Technology. Moreover, the MD5 hash function which is no longer considered secure enough for password storage was found to be used on these passwords. The passwords were also hashed without salting and therefore made them considerably easier to crack [2].

[1] "Unsecured server exposes 419 million records of phone numbers linked to Facebook accounts | Cyware Hacker News", Cyware, 2019. [Online]. Available: https://cyware.com/news/unsecured-server-exposes-419-million-records-of-phone-numbers-linked-to-facebook-accounts-d3653a06.

[2] C. Cimpanu, "Smart home maker leaks customer data, device passwords", ZDNet, 2019. [Online]. Available: https://www.zdnet.com/article/smart-home-maker-leaks-customer-data-device-passwords/.

Almost on daily basis, there are security attacks that occur, where some are unnoticed by the victims due to probably their inexperience about cyber security or IT in general. These can include among others the theft of user laptops, installing viruses on the user's computer directly using the removable medias like flash disks, tricking users to reveal their passwords to the attackers.

Among the many IT security incidences I have witnessed, there is this one incident that, were one user's email account was taken over by hackers, this happened due the fact that he was always using a public internet café, where you pay and use public computers , and the payments are per hour, the place had attendants to assist those who had troubles, with for example logging in, and other related issues. However, majority who visited this place always used it to check their emails, and they were not very conversant with IT, more specifically with IT security, all they could imagine is that their accounts are safe with just a password, others used the assistance of the attendants to set up their emails, which means they had to set their passwords in their presence. And there was no certainty that you could trust them to that level.

The most risky part about this place is the fact, there was someone always monitoring the activities of the users , and allocating the time once your time expires, the computer is just locked and all your activities are left open, unless you have extra money to pay to regain access and close your activities, you risked leaving your account open and someone else who sits on that computer will have direct access to your email address, and that is what exactly happened to this user. His account was exposed and someone else manipulated the information and changed the password and took over the account. It was impossible to even tress whom to start from since in this place no identity was required, and payments in most cases where made with cash, and his private email account was not connected to his mobile. Therefore, his email was used to scam money from his contacts some of whom fell victims of this scam.

2) According to The Guardian newspaper of 30th /08/2019, researchers at Google's external security team found out that iPhone hacking operations had been going on for almost two and half years, it is claimed that the hackers used a smaller collection of hacked websites to deliver malware to users to user's iPhone of those who visited the site, no interaction was required, the methods used by the hackers could even affect the fully updated devices. Once the hackers were successful, the user's deepest information

would be obtained by the hackers, such as the location was updated every minute, the device's keychain containing all the user passwords, chat histories for the popular apps like WhatsApp and Gmail, iMessage. The researchers claim that the implant was not persistent, once the user rebooted the iPhone the activities were terminated until unless when the user revisits the website.

In my opinion this must not have been an individual project, it targeted the entire users of iPhone in the whole world, which means it required intensive research and skill a lot of skills. And one would wonder what the motive in all this was, and as well how come apple never reported any incidence related to this. Should a conclusion be drawn that iPhone are no longer as secure as they used to be

https://www.theguardian.com/technology/2019/aug/30/hackers-monitoring-implants-iphones-google-says

---

It was a normal day, I was checking my facebook and I saw that there is a message from an old friend. I usually don't open any untrusted URL's but this one was from a friend. it was a strange message with a URL embedded in it. I was about to click and open the link but then for some reason I said what if it's not him; what if his account got hacked. It was a lot of questions on my mind but then I decided to check the URL before opening it. There is a plenty of internet tools to check if a URL is contaminated or not. When I checked the URL, it turned out it was a virus and later on I knew that his facebook account had been hacked, this was one of the incidents I encountered.

Another bad experience was at an internet café. I was working on one of the computers there and was logged into my email and some social media accounts. When my session ended, I forgot to log out. The person who sat on the same computer after me did not save a chance to get into my personal messages and since my email account was open, he could change my passwords and I could not log into my accounts for some time.

When it comes to the media reporting IT security incidents, I was checking my twitter today and I accidentally saw an interesting piece of news about an incident that happened yesterday. Wikipedia, which is one of the biggest repository of information, has been hit by a malicious attack that made it unavailable in several countries including Germany. Up to the time I wrote this report the attack was ongoing and the Wikidpedia team was still working hard to solve the problem and get the site functional again.

Another incident that got on my mind is the 2018 Facebook incident when they announced that an attack had taken place on their computer network. Thus, exposing the personal data of over 50 million users around the world. However, Facebook later on announced that they had contained this security issue and reset the affected accounts, and announced that the other users don't have to make any change unless they get a notification. However, I changed my password anyway just to be on the safe side.

---

1. Several years ago, perhaps ten years by now, I booted up my computer and starting to surf the web. After a while I was going to check my email, so I surfed to the Hotmail homepage and proceeded to type in my login-information. however, I was denied since I had supposedly typed in the wrong email or password. I tried several times, being sure I was typing in the correct password, but nonetheless I was denied every single time. At last I gave up and unfortunately, I hadn't set up a good backup so that I could retrieve the account if lost. Some time passed and I had to come to the realization that I had to let that account go and start up a new one.

Some more time passed and after a while the news came that there had been a big hacking attack and a couple of thousands of emails had been hacked. The funny thing is that this list later came to be published on the Swedish forum site Flashback. After downloading the list and searching for my email-address, sure thing, there it was! Together with my easy-to-figure-out password, open for the world to see.

Lucky for me I was quite young at the time so losing my email wasn't that big of a deal, which I can't say to many other people. However, I learned the importance of having a good, long, safe password.

2. Facebook have been under the media's light several times and was the first thing that came to mind when reading this question.

What come to mind when thinking about this incident is the amount of trust we put in these companies to keep our information safe. A lot of people share big moments in their lives that they would like to keep private amongst their friends. These kinds of attacks are a huge infringement against that trust. You would think that these companies spend a lot of money on security, keeping your data safe, but it just comes to show that anything can happen. We should really think twice about what type of information we put in the hands of these companies, since we can't be sure we are the only ones that will have access to it!

https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

---

Leaked credentials

At some point in life, we have all been a target of a person somewhere in the world with malicious intent, such as wanting access to your email credentials. Many times, hackers are not targeting you specifically but instead obtains your credentials from a data breach. One frightening aspect of this is that many people are not even aware of the fact that their credentials could have been leaked in some way, as data breaches unfortunately are relatively common but not always announced properly to the victim. If you are curious about potential leaks, consider visiting a website such as [1]. I have been a victim of these breaches myself and it was troublesome as I had been lazy with password management by opting for identical passwords across many different accounts to make my life easier. To counteract this, I had to go back in memory lane to figure out all these different accounts where I could have used this password and then proceed to change it as soon as possible. This was a troublesome process and I have since then learned from my mistakes. Luckily, I managed to resolve the issue fast enough to avoid more problems. Today, I use password generator programs to apply difficult to crack passwords that differ between accounts along with implementing two-factor authentication to make future hacking attempts a lot more difficult.

The 1177 scandal

In February 2019 there was a data breach affecting the Swedish healthcare phone service "1177" [2]. During this incident 2.7 million phone calls recorded since 2013 that had been received by the care contractor Medicall got leaked. The 170 000 hours of leaked phone calls contained sensitive medical data about the people called 1177 such as their symptoms, their medicines and in some cases even personal numbers. All this data was available on a NAS-server that for some reason was exposed to the Internet, all you needed to access the data was the IP-address of the server and you didn't even need credentials to authenticate. This goes to show how simple human errors can result in devastating consequences to a IT-system because apparently the only reason why the server was available to the Internet was because of someone accidentally plugging in an Ethernet cable into the device.

References

[1] Haveibeenpwnd. *Have I Been Pwnd: Check if your email has been compromised in a data breach.* Available: https://haveibeenpwned.com/ [Accessed: 2019-09-10].

[2] Ottsjö, Peter. 2019. *Här är allt vi vet om 1177-skandalen*. Nyteknik. 20 Juni. Available: https://www.nyteknik.se/sakerhet/har-ar-allt-vi-vet-om-1177-skandalen-6948869 [Accessed: 2019-09-10].

---

1. Jag arbetade inom en organisation inom hälso- och sjukvård där följande incidenter inträffade.

- Botnet på datorer

Vi fann att ett antal datorer hade blivit infekterade av skadlig kod som hade tagit över datorerna. Den skadliga koden hade gjort att datorerna var uppkopplade i ett bot-net och var styrda ifrån en kontroll dator på internet. Då datorerna hos oss användes för patientinformation så var det akut att åtgärda de infekterade datorerna då de kunde sända ut journalinformation om patienter.

- Förlorade datorer utan backup

Ett journalsystem fick en korrupt databas där inte backup eller transaktionslogg hade fungerat gjorde att ett antal journalanteckningar förstördes och inte gick att återskapa. Detta innebar att journalanteckningar under ett par dagar gick helt förlorade och man fick kontakta patienterna för att fråga dom om vad som hände vid besöken.

- Uppdatering av routrar utan godkännande.

Enligt rutiner skulle inga ändringar i nätverken göras utan att de hade kontrollerats och godkänts i förväg. En nätverkstekniker skulle bara göra en snabb ändring som han ansåg vara nödvändig men tyckte att ändringen var så liten att det inte var värt arbetet att få den godkänd. Han genomförde ändringen som visade sig vara felaktig och det slog ut hela nätverket i upp mot 1 timma. Felet uppmärksammades snabbt men routinginformationen var påverkad så den fick raderas och återskapas vilket tog en bra stund innan det hade genomförts automatiskt.

2.
- “Sjukhuset skickade journaler okrypterat utomlands”

Sveriges Radio
https://sverigesradio.se/artikel/7292338
Publicerat tisdag 3 september kl 12.24
Uppdaterat tisdag 3 september kl 19.50

"Akademiska sjukhuset i Uppsala har skickat sekretessbelagda patientjournaler till Sverige andra länder okrypterat, trots att det strider mot lagen."

Akademiska sjukhuset har brutit mot både dataskyddsförordningen såväl som offentlighets- och sekretesslagen genom att sända journalinformation till mottagare i andra länder via Internet helt okrypterat. Detta ger personer eller organisationer som avlyssnar kommunikationen tillgång till känsliga data som inte ska hanteras på ett så oskyddat sätt. Det har alltså inte ens används ett svagt krypteringsskydd som hade gett ett visst skydd utan journaler har skickats via email helt oskyddade. Detta har skett då det inte finns någon standard att överföra data skyddat mellan vårdgivare såväl inom som utom landets gränser.

Det finns lagar och policier som säger att det inte är tillåtet att sända journaler över Internet oskyddat men eftersom det är enskilda läkare som gör det så anser de inte att reglerna behöver följas. Dessutom har man inte i vårdgivarnas ledningar sett ett behov att kunna kommunicera journaler och andra känsliga uppgifter på ett kryptologiskt skyddat sätt.

EXPERIENCES IN IT SECURITY

If I think about my personal experiences about IT security probably I would sum it up in two events that happened to me.

The first happened when I was about 11 years old. I was playing a game in my laptop with a friend and we wanted to play in a local world only both of us. So I searched how in internet and I found a tutorial that said that I had to turn off my firewall. So I thought “ok, who cares about firewall? I don’t even know what is “and I turned it off. So, what happened when I finished playing? Well, like 30 notifications from my antivirus of security holes and infected archives. I was so scared that I reset my computer to 0, and I never did it again.

The second was not too long ago, in 2018 maybe. I was trying to get a program from the internet (don’t remember what specific program) and I don’t know how I ended up downloading a malicious software. Basically it infected all my PC files and in each folder there was a text file saying that I needed to pay 100 euros to get my files back… Probably it wouldn't have been that hard to get back the files, but it was my gaming pc and I really didn't care about the files. Additionally, only one of my 3 hard drives was infected. This somehow hurt me because at that time I already was studying computer science and I was thinking that I couldn't fall in those cheap viruses.

About what I heard in the last months in media I remember a new about 2 cities in EEUU that were attacked by a ransomware. The two cities decided to pay the hackers, the quantity of around 500.000 bitcoins if I remember well. They used bitcoins so they could not track them.

For me is very sad that like in this occasion the criminals could get the money and leave unharmed. It is a very serious threat in today's world, and we must try to finish it. Of course, this is practically impossible. But as more people try to get into cybersecurity maybe one day we will be capable of going one step ahead them.

I was working as an alarm and surveillance systems technician in my homeland, and the process to install an alarm system is getting a building scheme and determining where it should the equipment be fixed. The next step is to configure the basic panel that is connected to all motion and sound sensors, alarm devices and keypads in the building zones. The panel is also connected to a phone line and could configured to call the business owner and police office, not just releasing an alarm. Moreover the alarm system can be accessed remotely from Internet to make a configuration. Finally the testing stage is taking place. One day we installed an alarm system to a gold company, but something went wrong and the team had to reset the system and all configuration and they called me to do just a little part had been remained of configuration related to a voice card. I did it and turned the system on, then we tested the work ability, it was working perfectly. After about three months, the employer called us and told that the alarm was released last night and the police was in place and there was no theft at all. Our company made an investigation about the security incident, and detected that someone penetrated the system and he was unlucky because he released the alarm unintentionally. But how?? The system still had the default password !!!! When the team reset the system, they did not setup the new password because the role in our security policy is the last one who make the configuration, must setup a new system password and keep it on company's database. I was not aware of , I thought that everything was done by the team except the part related to a voice card. It was a big mistake, the company could have been stolen, and of course, my fault.

On the media, Avast labs researcher founded that 29 models of GPS devices that use to track the whereabouts of children and seniors, have vulnerabilities. Hackers and third parties can expose data when sent to the cloud and lock on to the real time position of the wearer, and change the GPS coordinates. Moreover, these security flaws also enabling hackers to spy or eavesdrop the GPS wearer in case of built-in cameras and microphone devices. About 600,000 faulty GPS devices founded by Chinese manufacturer Shenzhen i365 Tech and available online for 25$ to 50$ and resold with different names. And the model called T8 Mini GPS Tracker Locater redirects a user to an unsecured website to download a companion app which expose the user data. This finding is known by Shenzhen i365 Tech and met with radio silence. The argument about the suspiciously cheap smart devices. However even some children GPS tracking devices consider free from security flaws , they may give adults a false sense of safety and affect kids' ability to learn how to be independent in the future.

Reference:

https://www.infosecurity-magazine.com/news/security-flaws-found-in-600000-gps/

IT security incident: Personal experiences

I have a number of personal experiences in IT security. One of the more interesting memories that I have is a security vulnerability that I discovered a few years ago in the official implementation of the PHP programming language.

PHP is implemented in C, and it includes a lot of functionality to aid in the processing of text, images, compressed archives, and so on. The vulnerability that I am writing about in this report was found in the **ZipArchive** class (**ZipArchive** is used to compress and decompress zip archives).

One interesting feature of zip archives is that they contain size fields that may or may not be accurate. With the case of the **ZipArchive** class in PHP, one of those size fields were read as an unsigned 64-bit integer. Later on, that field was (depending on the architecture) typecasted to a **size_t** and then used to allocate memory for an uncompressed file in the zip archive. During the memory allocation, the size field in question was aligned in order to accomodate the custom-made memory manager in PHP (called *Zend MM*).

Whilst the aligned value was used as the size for the memory allocation, the original (unaligned) size was stored as the actual size of the buffer. The unaligned size was then used to read data from the zip-archive.

The way that I abused this particularity in my proof-of-concept exploit was by creating a zip-archive with a size field that was carefully crafted such that the original value was large enough that the aligned size would wrap the integer and cause a very small chunk of memory to be allocated.

Due to the fact that the original (unaligned) size was used to read data into the allocated chunk of memory, the aforementioned integer wrap could then be abused to cause a heap overflow and gain arbitrary code execution against applications that used the vulnerable **ZipArchive** methods.

This vulnerability was reported and fixed by the PHP maintainers.

IT security incident: Seen in media

In my opinion, one of the more memorable security incidents published by media this year is the 1177.se mishap [1].

1177.se is a Swedish service that offers health-related guidance and advice. Part of their operations are outsourced -- in particular, their phone-related services are (partly) outsourced to Medicall in Thailand.

In February this year, it was revealed that phone calls recorded by Medicall was openly available on the Internet. What's worse, when contacted by media the explanation given proved that the people involved in the incident have very little knowledge on IT (it was said that "somebody probably put a network cable into the NAS drive by accident" [2]).

I think this is an interesting issue for two reasons:

The first reason is that it shows that private health care data may be recorded by operators in countries that are not governed by Swedish privacy and data protection laws. Presumably, these services are outsourced to save on costs -- but how will Swedish laws be applied to a Swedish service offered from a country on another continent?

Secondly, it raises the question of who should be held responsible for an incident of this sort. Should the (technically incompetent) higher-ups be held responsible? Or the IT people? Or the politicians for allowing a state-owned company to operate with these shoddy practices?

[1] https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet
[2] https://www.nyteknik.se/sakerhet/har-ar-allt-vi-vet-om-1177-skandalen-6948869

Own experience:

One time when I looked in my mail inbox I noticed a commercial mail sent from my inbox to all my contacts. It really scared me since I realized someone must have hacked my email. I did not know how this could have happened. A friend told me that I might have registered my email on a site and that I used the same password as my email.

Lesson learned: keep seperate passwords and don't trust that sites will not use your personal info.

Another experience I had is that I received fake sms from postal service telling me that there is a package waiting to be delivered but the cost for delivery has not been covered completely. I clicked on the sms link and I got to a site where i had to pay with my credit card. It would have cost 20kr. The site looked real but the url looked a bit suspicious. I was also not expecting a package. Then as I started to click around the site I noticed that no other link was working. It confirmed for me that this was just a bogus site. If I would have put my card details there they might have taken all the money from my account.

The 1177 incident: https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet. 1177 is a phone number people call to get medical advice. This means that information can be very sensitive for an individual. All the phone calls are recorded and stored. Apparently, as computer sweden proved was that the information could be accessed by anyone. You could listen to other people's phone calls about their medical condition. This was revealed in the beginning of 2019. The phone calls that were recorded went back to 2013. Anyone could download this information from the server that require no password to access. If someone did download this before it was revealed to the public is not known. It was an under entrepreneur that was located in Thailand to handle phone calls during late hours that exposed the information. It is very irresponsible of authorities to let these entrepreneurs handle these kind of information. There was a case where an under entrepreneur in czech Republic got to handle transportstyrelsen data. This included data that covered military vehicles which could be considered sensitive data https://www.svt.se/nyheter/inrikes/alla-svenska-korkortsfoton-lackte-till-tjeckien. The thing is that when this data get outsourced to other countries there is no guarantee that the data will be protected.

---

1. At my previous job we had a company intranet where all the information we needed was accessible. Most of the services were only accessible from the company network but some items like the schedules and helpdesk was accessible from anywhere. We discovered a bit of a bug in the system where you could access your schedule directly without first signing on to the system simply by using the URL to the schedule and your staff number as an endpoint. This was great because it made syncing your schedule with for example google calendar very simple and automatic. The problem, however, was that anyone could see your schedule and by simply switching the staff number you could see the schedule of all 3000 people in the company. The company eventually found out and restricted access to the schedules this way, the question was however, if it was this simple to bypass authentication what else was wrong with the system? Shortly after the company found out about this vulnerability the system overwent a major overhaul.

2. The highest profile and most recent security breach I can think of was last year when millions of sensitive phone recordings from 1177 Vårdguiden in Sweden were leaked to the internet because basically someone had the whole database on an unprotected webserver which was connected to the internet and accessible to anyone. Basically, anyone cold access this without authentication and download whatever they wanted. The thing that really struck me with this incident was the complete lack of procedures or understanding of security. It seems like it should have been very obvious to

anyone who set up this system that when confidential phone calls are recorded, they need to be stored and handled with outmost care.
https://www.svt.se/nyheter/inrikes/2-7-miljoner-inspelade-samtal-till-1177-vardguiden-helt-oskyddade-pa-internet

Another scandal which might not have involved security breaches but which definitely brings up some ethical questions regarding how data is accessible and distributed is the Facebook and Cambridge Analytica scandal. Cambridge Analytica basically harvested tons of personal data from Facebook users and used this data in targeted advertising, most notably in the 2018 US presidential election for Ted Cruz's and Donald Trump's campaigns. User in the so-called swing states who were being profiled as undecided by Cambridge Analytica were being especially targeted. They were being targeted with advertisements and fake news stories etc. which were designed to convince the person in question to vote republican. It is not clear whether or not there was foul play involved but it ultimately led to Cambridge Analytica filing for bankruptcy.
https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

---

Just a few months ago I got a spam mail on my student mail account from my home university. The interesting thing about this mail was, that the account who send this mail to me was my own email address. In the mail, they said, that they hacked all my accounts and that they have access to all the data on my Laptop and that they are watching me, what I am doing. To proof that they send the mail from my own email account so I could see that they have access to my account. They wanted me to pay them some money on a bitcoin address in 24 hours and if I would not do that, they will send private documents to all my accounts. I contacted the university and they told me that a lot of accounts received that mail and that I should ignore it and that I can do a report at the police station.

My aunt received one time another spam mail and the mail looked like as it was sent by her friend from Australia. Because she was so excited about it and not thinking about safety, she opened a link, which had been included in that mail and she got a virus on her laptop. You could see, that something wasn't right because the light of her camera was on, but her camera was turned off. She had no other chance than to delete and deinstall everything and to get a new software on it.

Just a few days ago I heard in the news, that Google found out, that iPhones, of thousands of users per week, have been hacked over the last two and a half years. Just a few hacked websites added malware on the iPhone of the people, who visited their site. After that, it became possible to read the WhatsApp messages, get their locations and they also had access to their pictures. (CBS News: "Hackers breached Iphones for years, Google says" , online source https://www.cbsnews.com/news/google-iphone-hack-discovered-mass-ios-hacking-attack-sustained-over-at-least-two-years-2019-08-30/ , accessed at 03.09.2019)

I have been really surprised about that security problem because it existed for such a long time without being detected and it was so easy to gain so much information from the iPhone and the user. That is also a contradiction to the general assumption that iPhones are one of the safest mobile phones.

---

1. This question reminds me of the 90s and the beginning of the common use of the Internet. The times when you use a dial-up modem to connect to the Internet. There was a phenomenon called NetBus (not the Bus company, NetBuss) around the Internet. It was a small application simply explained as a remote controller. The attacker provided the user with a small .exe file around 480 kb, sometimes named patch.exe or something else to trick the user to run the file.

Once when the user executed the file in a Windows environment, the file opened one port for incoming traffic. It was basically setting up and client-server architecture. With the help of the user's IP-address, the attacker now gained access to the targets computer through a, for the purpose, designed user interface. The attacker could for example; keylog, access file system, take screen captures or just open and close the CD-Tray.

This type of attack was popular among teenagers. Most of the attacks were pretty harmless, like shutting down someone's computer or change desktop background, etc. But it could be worse like keylog passwords or deleting important files.

The knowledge about IT and computer in common was low and it´s was sometimes easy to get someone to open the above mentioned .exe file. There was also hard to close this backdoor for a common user since the .exe affected Windows own register. If you thought that you were safe if the file was only removed you were wrong.

How could it be so easy to hijack someone's computer? As mentioned there was low knowledge about IT for the common user and there were not many products for firewalls and virus like it is today. This was a phenomenon for a couple of years and then faded out when people upgrade their security and become more aware.

2. I think there are a lot of different incidents where the human factor is behind the issue. We have the exciting incident where Swedish organization 1177 leaked information from patients recorded as sound files. https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet. Later the responsible people for the organization showed their lacking skills in IT security and it became a parody in media. Where someone put an “Internet Cable to a hard drive” etc.

Also, we can read about Russian where data could have been leaked because the servers did not have passwords. https://techworld.idg.se/2.2524/1.722811/data-fran-ryska-overvakningssystem-har-lackt-ut

---

I once lost the password to my online-banking account. My bank has a policy that forces you to update your password once every year, and I had forgotten to make a backup of my password. The consequences weren't very severe: I couldn't transfer money to other people for the span of about 5 days. I requested a password reset, which was granted. The process consisted of the following steps: I had to make a password-reset request, which I did by providing some personal information and confirmed through an SMS code. Then, the bank sent me a letter which I had to take to one of their offices. In the office they verified that I owned the bank account by means of a personal identification document, and allowed me to set a new password for my account.

A recent IT security incident is the discovery of a zero-day vulnerability in the remote management software webmin, versions 1.920 and below [1]. It allows any user to execute arbitrary shell commands on a server that is running webmin, if the webmin installation has changing of expired passwords enabled. It is achieved by appending a pipe symbol to the 'old' value in a POST request to password_change.cgi.
The vulnerability is exposed through a bug in the &unix_crypt function in Webmin, which verifies that the given password matches that in the /etc/passwd file. Since unix_crypt does not escape special shell characters, the pipe symbol is interpreted by the shell as an actual pipe which allows the attacker to execute any command. It took a while for Webmin to release a fix for the vulnerability, but starting from version 1.930 the issue has been resolved.
The vulnerability seems to actually have been implemented by an attacker that modified the source code for Webmin on the developer's server. Because the attacker made use of some smart tactics in order to prevent the changes from being detected, the code was able to make it into release builds of webmin.

1.One day I got a USB drive from my friend to exchange some information, the folders inside the drive seemed normal so I clicked on one of the folders to open it, the mouse pointer glimpsed for a while, but nothing happened and I was not able to enter the folder. I tried several times to enter the folder, but again nothing will happen. I noticed that the color of the folder was slightly lighter than the normal yellow color of the default Windows folder icon. At that moment, I felt that this situation is very suspicious and I should be distrustful against the folder and its content. I right-clicked on the folder then on its properties and what I found shocked me, this was not a folder it was a program with a .exe extension. It hit me what I have done, I just activated a malicious software. The computer restarted and the Widows OS has been damaged, so I was not able to log in and I lost some important information. The only thing I regret that why on the hell I did not have an antivirus?!

2.I remember the big attack on Sony in 2014. USA media said that the investigations concluded that North Korea was behind the attack since Sony pictures was planning to release a comedy movie called "The Interview" that criticizes the North Korean leader. The attack was carried by a group of hackers called GOP or guardians of peace and the attack cost Sony over 100 million dollars. The attack revealed sensitive information about Sony company and about its employees. In the attack an SMB worm that exploits the Server Message Block protocol was used, and the worm opened a back door into Sony's servers and was used to copy about 100 terabytes of data from Sony servers.

Fortunately, I have not personally been the victim of more severe IT security incidents, but I often experience some minor ones. For example, I often notice that when I give out my phone number when, for example, ordering a product online, I begin to get numerous calls from telemarketers without having given the approval that my number can be shared with other companies than the one I gave it to. Another experience I've had is when I bought a used iPhone which turned out to contain some pictures from the old owner and was also still locked to the old owner's apple-id. To solve it I had to ask for the old owner's password to be able to delete the phone from their account because they couldn't do it their self. This meant I could have exploited the situation in some way when I had access to their account (but I did not, of course).

For the second part of this task, I remembered that I had read some news of denial-of-service (DoS) attacks, where hackers overload a system and hence making it impossible for real users to use it. This has happened in many kinds of systems and websites and the severity of the consequences of this varies depending on what kind of system it is. For example, SL was exposed to such an attack [1] which resulted in much inconvenience for the customers that couldn't use the website or the app to plan their trips. Another example is an article [2] from February this year which is about how Valmyndigheten was exposed to a DoS attack during the night of the election that resulted in severe disruptions to its website and was for several hours not able to show the preliminary results.

Although these two incidents may not have caused more than some inconvenience for the users (though some believe that the attack on Valmyndigheten may be an attack on our democracy), I believe that this kind of IT security problem may be greater in the future. More and more services are being moved to the internet to offer better accessibility but will then also be more vulnerable to DoS attacks. The big challenge I see with this type of IT security issue is to see the difference between normal traffic and "bad" traffic and I believe this might be why these kinds of attacks still occur. Because as mentioned in the article about Valmyndigheten [2] there are ways of protecting yourself from these types of attacks.

References:
[1] Michael Sundberg (Expressen)(2019). *SL utsatt för överbelastningsattack.* https://www.expressen.se/nyheter/sl-utsatt-for-overbelastningsattack-/ [2019-09-02]
[2] Per Kudo (Svenska Dagbladet)(2019). *Valmyndigheten kritiseras efter it-attack: ”Anmärkningsvärt”.* https://www.svd.se/valmyndigheten-sagas-av-experter-efter-it-attack [2019-09-02]

Ans 1:
I installed a lot of applications for my personal device, even from the unknown providers. After few months, I found that the device cannot work properly, such as it needs a long time to run an application, pop-up some advertisement which I didn’t click it and always redirected me to some unknown webpage. After I found that those issues always happened in my device, I had tried to delete the application which I had downloaded. But the situation didn’t change, it still works unnormal and always automatically download a lot of different applications and run as a background application. I had tried a different method and still could not solve the problem. Finally, I try to reset my device and it became normal. But I lost some of the data of my device because I didn’t which part of the data was not been affected.

Ans 2:
The news from https://securityboulevard.com/2019/08/hostinger-resets-client-passwords-following-security-incident/.

The news is about that there had a company which is a web hosting provider and internet domain register had an unauthorized to their server. After they found that issue, they reset all the password of their client to protect their information.

I think the company had handled this issue well. After that issue happened, they immediately reset all the password of their client. I think this is a good method to prevent more information loss because hackers had been accessed to a server which store the client username, hashed password and their webpage IP addresses. Also, they assembled a team of internal and external experts improved their security system, which can prevent the same attack and find out the potential risks of the current security system. Those methods are effective ways to decrease the effectiveness of their customer and fundamentally improve their security system. But I think the company should always update its security system because there is a quick change of information technology, hackers usually using innovative methods to hack the information they need. It is no use after spill mike, if they usually update the security system, this issue could be avoided.

Experiences of IT Security

My worst experience on the internet was someone hacking the Facebook account of one of my friends. The hacker used the account to get money from all Facebook contacts. In order to get it, they wrote personal messages to all contacts but using different content. For example, they asked for a donation for a zoo or something like that. But they also used much more filed ideas. For instance, they asked the persons to fill out a survey. To do that you had to send your mobile number via the messenger and then got an SMS containing a code. This code should be sent back via the messenger after the person received it. On the internet, there is a service, which makes it possible to pay with the mobile number. To do so you only need to specify your mobile number. This code, the people were asked to send back, was to accept such a shopping made by using this service. So many of the contacted people did this because they trusted the person behind the account and thus got stolen a lot of money.

The time reported last year about the theft of personal data, where the personal data of many politicians were published. A teenager used two different Twitter-Accounts in order to post Links to Websites, each of them including private data of politicians that could be seen by the public. The article says, that the student used scripts and software to hack into external systems and thus got access to the data. [1]
This incident was shocking for many people because no one expected a student to get access to private data so easy. By publishing all this data, he did not only expose the politicians but also made obvious how unsecure it can be to have data on the internet. It seems like a warning for the people, that you should be aware of the risk you take by publishing data online, even if they are secured with a password or only saved on the own computer.

reference list

[1]Die Zeit: Ein Schüler hackt das politische System. online source https://www.zeit.de/digital/datenschutz/2019-01/datenklau-hacker-schueler-angriff-daten-politiker-datendiebstahl-datenleak.

Experiences of IT Security

Nowadays we are living in a digital world, where information is considered to be the most important asset and due to its importance, it must be protected in different ways from the intruders. In the first section, I will describe personal IT Security breaches and in the last one, there are different IT security incidents the media has reported lately.

First of all, I try to secure all my devices, software or web services using different passwords that reach a high strength. By doing this, I intend to prevent any intruder from physically accessing my device. One day as I opened the File Explorer on my laptop, I noticed in the This PC section another removable disk named after my neighbor. The disk was more than half spaced filled with documents and files that certainly did not belong to me. In my opinion, I think my computer was being used a memory place for photos, videos, documents and other different files. I was shocked at first as I thought my files might have been under threat and the intruders probably might have had access to them, so I quickly decided to remove the disk from my device. Then I ran a full antivirus scan, but I did not believe it would make a difference on the protection of my computer, so I took my computer to an IT specialist. He assured me after checking the computer that the intruder had no longer access to the computer and I installed a different antivirus product to protect my system from any other security breaches.

Secondly, losing devices is a common experience for me and that is the reason I provide high strength passwords for them. Once my lost device was found by another person and the intruder tried to get access to my Facebook and Instagram account. I received emails stating that I was trying to change the passwords of the accounts by using my mail address and then my phone number, which unfortunately was still activated. By entering from my laptop in both accounts, I managed to change the email address I had provided before and the phone number. As a result , I succeeded in securing the accounts and then I reached the police and shared with them the exact location of the intruder to get my phone back.

Furthermore, media is reporting daily IT security breaches that are very concerning for most of the people aware of the information importance. Recently, CNN published a report of Google cyber security experts having found evidence of an attempted mass iPhone hack over the last two years. They managed to discover a small collection of hacked websites that exploited vulnerabilities in Apple's smartphone software. By simply visiting the hacked site, the device you were using would be attacked from the exploit server. In case that the attack was successful, a monitoring implant would get installed. Ian Beer,a researcher with Google's Project Zero, said that they estimate that those sites receive thousand of visitors per week.

Additionally, back in my home town a hacker , aged 25 years old, managed to steal Bitcoins with a value of millions of dollars, credit cards and bank accounts. The policy reached him as they actually attacked the Albania Hackers Group who had been working for days in keeping governmental institutions' servers blocked from authorized access. This hacker stole approximately 530 million dollars, which were gained through the theft of users' credit cards' data.

In conclusion, providing secured networks is not a luxury, but a necessity in the digital area we are living.

---

1. Back in the day, I used to play league of legends when I was younger, and I got phished for my account. I clicked a link that a person was spamming in-game and he advertised that you could claim a free cosmetic item for one of the playable characters. I didn't think there was anything wrong with that since there were 2 other cosmetic items you could get for free from the official game website if you logged in a answered some questions, and I thought this was just another new free cosmetic item they released. I clicked the linked and got routed to a website which looked like the official game website and tried to log in. Nothing happened and 5 min later I was logged off my account and the hacker changed my password and email address linked to the account. I got then approached by the hacker through a friend which he messaged with my account. He demanded x amount of money for giving the account back. The most dangerous part was not him getting my game account since I had no really sensitive

information on it, it was that I used to have almost the same password for every service I used back in the day. So the hacker had my password for my mail and such. Luckily I manage to change my password on all services I used before he could cause any damage. After this incident, I have become way more careful with what links I click and what information I am submitting, I always check that the URL is correct and it has a certificate and such. Since then I have also started to use several different passwords for all of my different accounts so I wouldn't need to change all of my passwords again if I got hacked.

2. One incident that happened this year is the incident with 1177 and recorded phone calls being publicly available. 1177.se is a Swedish website where you can read about medical conditions or call for medical consulting. This year 2019 it was revealed that 2.7 million recorded phone calls was saved on an open web server with no password or any sort of security measures to stop anyone from accessing them. These phone calls can be traced back to 2013 and its estimated there is phone calls that span over 170 000 hours.

The recording of the phone calls is standard practice but they should be handled according to the swedish patient data law.These phone calls contain sensitive information about personal diseases and such and I feel like this is a huge blunder made by 1177 IT team. This big of a mistake should not happen, forgetting to put a simple password is something that should never happen when handling this sort of sensitive information. I would maybe be more understanding if there was an attack by a hacker but to save them on a public unprotected server is a massive failure. And this was an incident in the public sector compared to the private sector, which I feel is becoming more common these days.[1] [2]

References

[1]P. Rudolfson, L. Borgert and A. Sartori, "2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet", SVT Nyheter, 2019. [Online]. Available: https://www.svt.se/nyheter/inrikes/2-7-miljoner-inspelade-samtal-till-1177-vardguiden-helt-oskyddade-pa-internet. [Accessed: 07- Sep- 2019].
[2]L. Dobos, "2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet", Computer Sweden, 2019. [Online]. Available: https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet. [Accessed: 07- Sep- 2019].

Part 1. My own experience

A number of years ago, I cannot recall exactly when it was, I noticed that my email was hacked. I was not so old when I created this email, so the password was not particularly strong.

When I logged in to check my email, I saw that there were several report emails telling me that my sent emails could not be delivered due to that the address did not exist anymore. I remember thinking it was strange since I had not sent emails to those addresses, the thought of that someone had hacked my email was so surreal at that time

that it never crossed my mind.
A couple of weeks later my mother said she had received a very odd email from me and told me that my email might have been hacked. Next time when I tried to log in the service told me that my email account was blocked since a lot of spam emails had been sent from there.
I was in a small chock thinking "How could this have happened?!", I considered how it could have happended and realized that my password had not been secure enough when I chose it. Thanks to the email-service I could restore my account after following their security procedures, with a stronger password this time! I have learned my lesson, when I am supposed to pick a new password, I think it through properly!

Part 2. Media reports

In your mobile telephone you keep very private and vulnerable information bout yourself, you can handle your bank errands, sign different documents and all the contact information in the contact list. A lot of damage can be done if a malicious app gets a hold of this information.
This is what is happening in Japan now[1].

An infested app for android mobile telephones is being spread rapidly, it sends all the information about the phone to a server, IMEI, IMSI (International Mobile Subscriber Identity), for decisions about further behaviour. Then it takes control over the phone by turning of sound for notices, setting itself as a default handler of SMS and sends all the received SMS forward to a server.

A lot of services we use on the web, we access by our mobile telephones, since a lot of those services use verification by SMS, all these verification codes are sent to another server where someone can use these to access for example a bank account, email services and contact with different governments.

Having a mobile telephone in your hand you can almost reach the whole world with a few button clicks. But keeping all this sensitive information in one place makes it a very clear target.
The mobile phones are said being well protected against malware, but infested files can be transferred to a device in other ways then through an app store where the apps are reviewed. Apple reviews all apps before they are released but Google checks them first a while after they have been public in their store, making android devices more open to a security breach. There can also be other places where you can download apps, with other routines for how they review the apps.
We should be cautious with what we are downloading in our devices and act when something is out of the ordinary!

Refrences.

1. Seals, T. (2019). *FunkyBot Malware Intercepts Android Texts, 2FA Codes*. [online] Threatpost.com. Available at: https://threatpost.com/funkybot-malware-intercepts-android-texts-2fa-codes/148059/ [Accessed 9 Sep. 2019].

A long time ago I won a big prize in a well-known lottery organization. They have sent me an email and I was so happy that I will be a millionaire in just couple of days as soon as I receive the money. They contact me with the information that I need to submit in order to be able to receive the money. The number was huge and enticing and the information that they asked for was not very important compared to the prize that I have received. So without any hesitating I have filled in what they asked me to submit and I sent them an email with the needed information. But in the time when I was clicking the send button an Idea came to my mind whether this email is true or fake. But it was too late, I have clicked the button. I went ahead and cheeked the email I have received and double checked the email address and all of sudden the email address was fake. It was created in a smart way that it was very similar to the original one. I felt sad to give my information to someone I don't know. And I learned a lesson that don't rush giving important information before double check to whom you give it. Such security incident can cause to have more severe incidents because the information that the attacker receives in many cases give him/her authorization to more sensitive information. For example, he or she can use such information to log into the victim's email account and they might be able to transfer money from the victim's bank account and so on.

Researchers from the ICSI (the International Computer Science Institute) found that more than one thousand android apps are stealing data despite the user explicitly denying permissions.[1] In the old versions of Android users couldn't manage apps' permissions, therefore the user had only two options either install the app and accept all permissions or not to install it. But then Google added the ability for the users to allow or deny each permission individually which was good news for many android users. This has let the users use android apps confidently by relying on permissions management provided by android system. The researchers found that these apps have found a way around, in order to gather information from the users such as their precise locations and device IMEI. I think this new raise the question that to what extent google play apps and android system are reliable?

[1] https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/

#My Incidents

Long ago my brother had a house party and the family computer was on with my high school account logged in. So the next day i get a phone call from a raging teacher. Screaming how it's NOT OK and that he shall have me expelled from school. Totally clueless, I could not say much; other than that I had no idea what he was talking about. Later found out who had gotten on the computer and written the message. Lesson learned when it came to staying logged in and not having screen lock on computer. Unauthorized access can so easily happen, and cause so much damage. Having the browser save and type in passwords makes life so much easier though. The constant battle of easy access vs security.

Even longer ago, my CD-ROM started to open and close by itself all of a sudden. Some other strange things happened and I understood someone else was doing it. As far as I know, this breach didn't have any other consequence than scaring me. Not much later, I was most likely using the very same trojan to prank my friend.

Media Report

Scanning recent news I find yet another incident related to GPS. This time over half a million trackers have been found out to expose location data of its users[1]. 29 different models from the same company (country shall not be mentioned) contains a number of vulnerabilities. One of them being that they all were shipped with the default password "123456". Remote attackers could then track users in real-time, falsify location data and access microphone. This reminds me of similar GPS incidents, such as the Strava scandal[2]; exposing US army bases and sensitive information about them. Things move forward so fast, the majority of people do not take the time to fully understand the implications and possible usage of the devices they purchase.

Consumer awareness, trustworthy companies and open source software is becoming more and more important; as more of us integrate our lives with these types of technologies. Buying the cheapest thing on the market is probably not a smart thing to do. Neither blindly trusting companies that all to often breaks that trust, and prepares a budget that includes paying fines.

[1] https://thehackernews.com/2019/09/gps-tracking-device-for-kids.html
[2] https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

---

1. IT security incidents are a serious matter that can affect any individual. I have already had my own experience with IT security incidents in the form of a hacked e-mail account. A few years ago I received a lot of spam mails which I did not pay attention to at first. The big mistake I made was to click on a link in one of those spam e-mails which looked very real. Even if I recognized very quickly that this link was fake, the evil took its course. After that incident, I received dozens of spam e-mails a day which filled the storage of my inbox. A few days later, I received a lot of „recipient e-mail address not found" e-mails, even if I did not write any of them. That was the point when I recognized that my e-mail account was hacked and probably exploited as part of a botnet due to the high number of e-mails. As a result of this incident I first changed the password and reinstalled the PC. In addition, I have installed a new virus scanner and created a new e-mail address.

2. A recent IT security incident affects the data leak of nearly 90,000 German Mastercard customers. Due to a data leak of the Mastercard Bonus Program "Priceless Specials", personal data such as first name, surname, e-mail address, IP adresses and the date of birth of the customers were leaked (Gatlan, 2019). Moreover, the complete card number has been published. Mastercard pointed out that this data leak did not affect the payment network. The hackers are not able to use the Credit Card data for purchases on the Internet because the expiration date and the check number (CVC) of the card have not been leaked. At least the expiration date is required for any purchases on the Internet (Gatlan, 2019 + Teller Report, 2019). For affected customers, the risk of

receiving phishing e-mails to reveal their passwords or other payment information has increased. To protect customers from negative consequences, Mastercard offers a free exchange of the credit cards (Teller Report, 2019). As the importance of card payment increases, the protection of personal data, in particular payment data, is of crucial importance. Customers should be aware of the higher risk of phishing mails and should accept the exchange of their payment cards. On the other hand, Mastercard should identify the cause of the data leak and take appropriate measures to avoid its recurrence.

References:
Gatlan, Sergiu. „Data of 90K Mastercard Priceless Specials Members Shared Online", Bleeping Computer, 02 September 2019 [Online]. Available at: https://www.bleepingcomputer.com/news/security/data-of-90k-mastercard-priceless-specials-members-shared-online/ (accessed 03 September 2019)
„"Priceless" bonus program: Mastercard: Data leak also affected complete card numbers", Teller Report, 22 August 2019 [Online]. Available at: https://www.tellerreport.com/news/2019-08-22---%22priceless%22-bonus-program--mastercard--data-leak-also-affected-complete-card-numbers-.Hkgb-kyn4B.html (accessed 03 September 2019)

Personally, I have managed very well not get exposed to IT security incidents. I always try to be attentive and use a skeptical view to links sent to me. I have always wondered, who are these stupid people falling for this kind of scam. But I realize nowadays when even my grandparents are using the internet daily, that there is a lot of people being exposed to scams like this. Also, the scammers improve their skills and create more targeted and realistic scams, which brings more trust to the victims who might lose that skeptical view for a second while clicking on that link. A couple of years ago I was working at a logistics and warehouse company. Lots of packages were sent and received every day, and also a lot of emails about lost, late or wrong deliveries. Now that I think back to that situation, I realize, this must be the dream for scammers, and so it was. It was a fake mail with a shipment tracking link from Postnord, which in my opinion is a brilliant idea from the scammers even though I don't encourage it. It was sent to all mail addresses in the company and if I remember correctly it was three people clicking that link. I remember the IT guy sent out bulk mail to warn everyone not to click that and after that, he ran to every department screaming like a crazy man, he panicked. This was what is called ransomware, what the scammers do is to take over the computer's operating system and ask the user to pay a ransom to allow him or her to access a program that unlocks the computer. Unfortunately, I don't know how our IT guy solved this.
https://www.tidningenkonsulten.se/nyheter/varning-postnord-bluffen/
More about this ransomware attack.

About IT security incidents when it comes to the media report, the first thing that comes in mind is, of course, the 1177 leak. I'll guess most of you know about this leak but if that's not the case, I'll explain it briefly. 1177, the Swedish health care guide was was recording phone calls between them and people who were calling for help. This can, of course ,be very private conversations and it often starts with the person calling exposing their names or personal identity numbers. These recorded calls were stored on an unprotected server, giving access to everyone if you just knew how to reach it. I don't know much about internet security yet, but I know for sure this is one of the basics to keep private stuff protected, and for a state-owned company, this is a big scandal. I guess one of the problems is the growth rate of online services has been very fast and many developers lack knowledge of security part. Also as Ola mentioned in the introduction to this course, companies don't want to spend too much money on security, it's not a problem until it becomes a problem. I also think that in general, not only for the ones working in our branch, the knowledge of internet security is too low. It's hard for companies ordering this kind of services to know if it's secure enough considering they have no basic understanding of how anything of that works and because of that it's easier for companies delivering services to "cheat". To sum it up, since the internet is a big part of many peoples lives nowadays I think everyone would benefit from some basic teaching and understanding about internet security.

Personal

The biggest security incidents I've been involved with was back in the wilder days of the internet, specifically back when various services (like Microsoft's Hotmail/MSN accounts) did not enforce password policies, and everyone used the now defunct MSN Messenger to chat with classmates.

Hotmail:
First of all, I had a terrible short password that was 4 characters long and was based off one of the columns of the keyboard.

Short simple passwords are easy to hack so my account was hacked, the account was then used to spam people on my contacts list, presumably the ones of a similar age as myself at the time also had terrible passwords: because the way I discovered all of this was that I was spammed by other people in my contacts list with the exact same message that had been sent by my account.

Changing the password and following the "have you been hacked" informational pages solved this. I believe many of the people on my contacts list abandoned their accounts and created new ones.

MSN Messenger:
Secondly there were addons for MSN Messenger that you could very easily install (through a click in the chat-window), that of course became victim to a virus that contacted all of your friends with a message along the lines of "The message sent failed

to download, click here to try again" which of course installed the virus and spread it even further, also the MSN Messenger used your Hotmail/MSN account so this virus also had access to your emails, and possibly your password.

Possibly this is one of the reasons why the service was later shutdown by Microsoft.

Media

The Tesla Model S was some weeks ago found to have a security flaw in the keyless fob of the car. A similar flaw was discovered a year ago by the same researchers led by Lennert Wouters from the Belgian university KU Leuven.

Thanks to a configuration error the fobs used two 40-bit encryption keys to authentify the fob, unlike the flaw from last year (which required new fobs), this was fixable through software updates of the car and the fob so that the encryption instead is 80-bit.

Two 40-bit keys are just twice as hard to hack instead of the massively harder 80-bits.

Consequences for this is of course hard to quantify but presumably people have a lower opinion of Tesla, and may have lead to people choosing another car manufacturer, or one of their other models that never had this security flaw.

In this assignment we need to describe one or several IT security incidents that I personally have experienced. Moreover, I write about an IT security incident which I have read on media in the last few months.

One an incident that I have experienced that one day while I was trying learning by practicing a few hacking experiences and downloading malicious software such as trojans and couple of viruses my pc started not responding and then turned off by itself and after that when I turned it on I noticed that the OS got damaged so I had to reinstall OS again but I lost all my data.

A second experience which was very bad for me that I took my laptop to me to work on it while my traveling but unfortunately someone stole it at the airport while I was busy in showing my documents at the airport. I lost all my information assets on laptop including assignments, projects and study materials and all software with their own licenses and many more information assets such as my personal photos. The problem was that I did not do any back up since I was lazy and every time I say I do it later. As a tip do not make same mistake and do not be lazy and do back up.

One of IT security incidents which I read was on May 2019. Binance which is one of most famous exchange and trading cryptocurrency platform in world faced a very complicated cyberattack. As a result 7000 BTC has been stolen (one BTC 10622 $ today 4.9.2019) in one single transaction. Moreover, Binance said that the investigation which related to the leak of the customers verification information could affect up to 60,000 customers who sent KYC information during 2018 and 2019. Binance thinks that there is a relationship between leak of customer's information and the hack which happened recently.

The hacker or hackers made a group in Telegram under the pseudonym "Guardian M" and started post hundreds of images of individuals holding their IDs and pieces of paper written with "Binance, 02/24/18,"

Another incident related to social media specifically Twitter. On Friday 30.8.2019 the account of CEO of Twitter was hacked by a group called "The Chuckle Squad". The group tweeted racial slurs, antisemitic and Holocaust denial messages which stayed about 10 minutes on his account before getting deleted.

The incident made the customers of Twitter reduce their trust in Twitter and its security specially that the account which was hacked is not a normal account since it's the CEO of Twitter account which is supposed to be secure.

Moreover, the customers start thinking if CEO could not keep his account secure which it should be secure since it is very important for reputation of Twitter but he could not then how we can make sure that our accounts can be kept secure. The only one who did not feel less secure in using Twitter is the president Donald Trump

---

1. Personal Security Incident

Around July 2017 I started getting e-mails from Facebook telling me that a login to my account was unsuccessful. There was an option to report that this was not done by me, which I did every time this e-mail appeared in my inbox, but it did nothing. The were over 20 such e-mails over a period of three months. The whole thing was also suspicious since I deleted my Facebook account in 2008 and thought that it did not exist anymore. Finally, an e-mail telling my that my account was now back after a successful login was sent to me. I had to inform them once again that someone else was doing this and quickly guess my password from 2008 and login to Facebook myself. There had been no activity on the account except for one login. Once again, I deleted the account, hopefully permanently, but I have no way of knowing if it is actually deleted.

Since my account was in disabled mode, not actually deleted, I would have first needed to reactivate my account just so I could change the password in order to prevent this. It felt like the worst possible design was used every step of the way since I did not even think that my account was somehow still accessible, so the thought of reactivating it just to change password and re-deleting it never even crossed my mind.

2. Security Incident Reported in Media

The Swedish scooter rental company Voi was found to have stored their customers' usernames, phone numbers, and e-mail addresses on an unsecured server. This information was accessible by anyone using what Voi claimed were "inactive parts" of their software and was found by the German media company Bayerischer Rundfunk [1].

Bayerischer Rundfunk claimed to have gained access to around 460,000 users' information while Voi claims that around 100,000 users would be affected. No credit card or other payment method information is supposed to have been leaked. Voi fixed the security hole swiftly.

These types of stories are quite common where a company or some organization store users' data on unsecured servers, sometimes even in plain text, making the sensitive data accessible to outside actors. Whether it is laziness, inexperience, or too small budgets for proper security measures, it should not happen as often as it does. The affected companies are often time also blaming whoever published information about the security hole, as Voi did in this case. Users have a right to know when their data might have leaked and should be informed about each possible leak.

It is not impossible that the financial damage that this did to Voi could have been less than what it would cost an IT security firm to properly test their software in the first place. However, these types of leaks could be inevitable, as even the largest tech companies, e.g. Google with Google Plus, have had similar leaks of users' information. At some point, someone could make a mistake, something could fail, a new security hole might be found or a vulnerability will appear when altering software. Perhaps the only solution is to have constant security tests in place that always try known and new attack vectors on software, even though it would most likely be impossible to achieve in a large enough scale because of the monetary cost.

[1]. Granroth, A. (2019). Svenska elsparkcykelföretaget Voi läcker kunduppgifter. [online] SweClockers.com. Available at: https://www.sweclockers.com/nyhet/27219-svenska-elsparkcykelforetaget-voi-lacker-kunduppgifter [Accessed 2 Sep. 2019].

Back at my home university, a master student got their student account compromised, and a phishing e-mail was sent via their official university email. The e-mail said that you had requested to change your personal details, and you should let the university know if it wasn't you that did that. The 'notify us' button would take you to a lookalike login page of the university, where nothing would happen after you had filled in the details. As the attack, as mentioned, came from an official university e-mail address, it could reach all of the university's students and employees. The e-mail looked very real, so quite a few people fell for it. The university later came out with the obvious statement that everyone who did fill in details should change them as soon as possible. I am not sure if any additional measures were put in place to prevent such an event in the future. I also am personally not sure what the point of this attack was, as university accounts usually do not contain the most interesting information for such an attack (which is why I normally see phishing e-mails from people claiming to be a bank). No further e-mails were sent after the first one, so it was not the case that users that filled in their details instantly also were sending the phasing e-mails.

Some time ago I read a news article about hacking conference Def Con. The participants of this event were hacking voting computers. It turned out, many of these vital machines for a fair and democratic election were running outdated software containing critical security flaws (e.g., a 15 year old windows version). This is obviously not desirable, as this opens the door to individuals or even other countries to temper with the election results. In the end, all voting machines were hacked. This shows us that we still have a long way to go before we can fully rely on technology when it comes to crucial things.

Section 1

At work, I received an e-mail with a link that I clicked on. The email was very informative and looked like it was coming from the administration department of the company. It told me that I had to change my company account-password as soon as possible by clicking on a link that would take me to the corresponding company website. I clicked on the link and realized that I had been a target of a phishing attack. Fortunately, directly afterward, I received an email with a message telling me that I had failed a false phishing attack test that the company had ordered to execute on company employees to test the companies security. Since this was a false phishing attack there were no consequences else than that the false attack taught me to always check the sender's e-mail address moving forward, before clicking on any links in e-mails. I have realized that it is much easier to remember to check the sender's e-mail address on your private e-mail than on your work e-mail since you take for granted that all the e-mails that you receive come from a company employee, at least in my case.

Section 2

Twitter CEO Jack Dorsey had his Twitter account "briefly hacked" a few days ago. Highly offensive and racist remarks were spread. Fortunately, the situation was under control shortly after and now the Twitter account is back in the hands of the CEO. Since fake news is one of the biggest threats of our world, being spread much faster than actual news, the consequences of such a powerful person's Twitter account being hacked can be major. The consequences of this hack might not be so big, although it shows how you can never be safe online since not even the CEO of the biggest finance and politics communication channel is 100% protected from being hacked. Imagine, for a very extreme example, if Donald Trump's Twitter account would get hacked instead, imagine the consequences it could lead to (e.g. stock market collapse, war, etc). This scenario is just one of many showing how important it is with good security and how the hackers are finding new exploits that we must stay protected against.

Source: https://www.bbc.com/news/technology-49532244

1.
I am quite lucky because I have never had any serious IT security issues. I get regularly phishing scam mails, but I never do anything with them besides reporting and deleting them forever.

Once, there was a case when I have received an email from my hosting provider with some requirements to login to my account via provided link and to update some information asap. The requirement was weird, but the email address was legit – it came from their domain. After contacting customer support I was told that they haven't sent anything to me and if I clicked on any links in the email I should change ALL my passwords and scan computer for viruses. When I asked how did this happen that the email was sent from their mail servers, the support guy just mumbled some gibberish and repeated that I should change EVERYTHING :)

Another case I remember involved LNU. Somebody got hold of my program's mailing lists and was sending phishing scam mails to all the students. I don't think anybody got "hurt" though.

Many years ago I was able to break into my brother's computer by guessing his password, because it was only four digits long. And I did it twice. After that he started using password that were a bit longer.

2.
On August 23, one of the biggest web hosting providers on the internet Hostinger has discovered that one of their servers with internal system API has been compromised. The API was accessed by an unauthorised third party who gained entry to Hostinger's client's database that contained hashed passwords and postal addresses among other personal information about 14 million Hostinger users, but no financial data was compromised.

According to Hostinger they do not know how many clients might have been affected, but assured that immediate actions were taken to secure the API, so no unauthorised access was available hereafter. As a precaution, the Hostinger has force reset all customers passwords.

---

1. Security incidents I have experienced

One of the security incidents I have experienced was a data breach for the Unreal Engine Forums which happened during August 2016. The data breach was possible because the forums was using an old version of vBulletin which had a known security vulnerability. The attacker managed to get a hold of a copy of the forum database using a SQL injection vulnerability. The database was filled with usernames, email addresses and salted MD5 hashes of passwords for 530 thousand user accounts.

Another security incident which I also have experienced was when the CD Projekt Red Forums suffered from a security breach during March 2016. The attackers managed to gain access to an old forum database which contained usernames, email addresses and salted SHA1 passwords for 1.9 million accounts. Both of these breaches did not impact me as much as they could have since I always use unique passwords for each account I create which limits the damage during breaches such as these.

2. Recent security Incident in the media

One of the latest security incidents in the news which I have taken notice of was that a report was released recently on September 4th by Techcrunch which reported that multiple databases with over 419 million records in total which included phone numbers and facebook IDs was accessible on an unprotected server. A facebook ID can be used to easily identify the username of the account the phone number was associated with. Some of the records also included names, gender and country. The unprotected server was found by a security researcher. According to Facebook the breach only exposed 220 million phone numbers because of duplicate entries. This incident is only one of the many security incidents Facebook has been involved with in recent times.

https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/

Personal Experience

My experience with an IT security incident is probably as mundane as many others. I will be writing about an email I received this summer. Not really a phishing email but a bit more interesting. I don't remember the mail word for word but remember the gist of it. It was something akin to "Hi, I got your password 'PASSWORD' and now have access to your accounts, give me money else..." only unnecessarily longer. But the password that was sent in the email was actually one of mine a really old one but still one I've used before. Since I didn't use that password anymore for any I account I know of, I didn't pay much attention to the threat. What I was more interested in was how they got the password. My guess is that they got it from one of the many data leaks that have happened. Apparently my email address has been in 10 different data breaches according to the 'haveibeenpwned' website. So probably someone got a hold of one of these data breaches and it's unlikely the password was stored in cleartext. So they probably identified what hash it was and ran a dictionary-based brute force attack against it. That's my guess at least on how they got the password. The scary thing, however, is if I hadn't updated my password and just used the same password for years they actually could have gotten access to my accounts. Now if it were a recent password I received in that mail I would probably have handled it in a similar manner, dragging that mail to the trash bin and obviously recovering/updating the password where it's been used. I think 99% of these sort of 'threat' emails are just that a threat. The "hacker" probably better-called as a script kiddie is just hoping for someone to bite and following through with whatever vague threat they're posing is highly unlikely. The only time you're at a risk is when you engage these sort of people then they know you're a live target. At least this experience showed me the importance of regularly updating your password.

Media Report

The media report I decided to write about is regarding the Hong Kong protests and how the communication channels have been target by attacks. It's better to read about here "https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html" and here "https://www.ibtimes.sg/massive-cyber-attack-disrupts-popular-online-forum-lihkg-used-by-hong-kong-protesters-32293" but I will do my best to sum it up. The main messaging app used by Hong Kong protesters telegram was DDOS'd during their protest and their main forum LIHKG the protester use to organize were also attacked with DDOS attacks, these attacks IPs were mostly originating from China leading people to speculate if this was organized by the state. Now, these types of attacks that take down a website or disrupt an application are not that uncommon but these attacks are clearly trying to disrupt the protesters in Hong kong meaning it's done with a political agenda. These sort of attacks for political power is not only scary but something we've seen surface more and more of e.g the accusation that Russians hacked the 2016 American election for example. The online attackers are not only basement dwellers that are doing it for disruption or monetary gain but also (potentially) state actors that do it for political control and power.

During my internship in web development, I encountered a security issue. Indeed, I had to manage account of users. When developping it, I encountered issue with the access token expiration when using Federated Identity Management of AWS. Indeed, there were two different access token and both having different expiration delay. So the client could have encountered issue when someone stole the password of an user, he can have access for a moment to the account and do action even if the user changed his password which revoke one of the access token.

In France, a huge security flaw happened at the beginning of the month. Indeed, the Interior Ministry website let a security flaw that leaks private information of 130 000 policemen.

IT Security incidents

A couple of years ago a friend of mine had an online stalker that also turned on me by hacking my email and ordering items in my name. He also looked up my telephone number and called me to make threats about other things he would hack. The companies that the hacker ordered from were thankfully nice about it and cancelled the orders when i explained what had happened. After changing my telephone number and changing my passwords on everything i never heard from him again or noticed anything else he did altho my friend kept having troubles with him for another year after that.

In more recent time a gaming company i were registered with had a breach where passwords were leaked and my password was among them but i never noticed anything from that incident.

I try to protect myself by using hard passwords that i change from time to time and to use different passwords for everything.

IT Security incidents in media

In August of 2019 a german Mastercard partner had a breach that made personal information about mostly german customers leak. Information like name, date of birth, payment card numbers, emails, phonenumbers, genders and home addresses were published online. Around 90 000 customers were affected by the breach. Mastercard took actions to get the published information removed and the partner site were closed to prevent any further leaks [1].

Since the partner that the breach affected was one where the customers got points for shopping with their Mastercard, potentially losing these points could have been a big problem for the affected customer. And even though only the credit card number got leaked and not the expiry date or CVC code of the card, having all of that personal information leaked online could get the customer in a lot of trouble if it got in the wrong hands and just the feeling of having your personal information out there uncontrolled by yourself is bad enough for most people.

References

[1]T. Robinson, "Mastercard says German Priceless Specials loyalty program breached | SC Media", SC Media, 2019. [Online]. Available: https://www.scmagazine.com/home/security-news/mastercard-says-german-priceless-specials-loyalty-program-breached/. [Accessed: 02- Sep- 2019]

1.
It was one year ago, we had a guest lecturer at the university where he showed us a website that they (in their company) use to practice their hacking skills on that website.

He gave us the website link and suggest us to try to hack into that practice server during the lunch break.

The website was a simple single page application where everyone can fetch the data from the database but only registered users that can log in into the system and can alter, add and delete the information in the database.

First, we tried to find a UI bug that could lead to a way to hack the server but we couldn’t, after that we tried SQL injection to the database using the username & password field and it worked we were in!

After just 5 min we managed to delete everything in the database and make the website totally useless by just writing one query in the username/password field. Of course, the idea of the website was to practice and try to find security weak point but at the same time, this shows the importance of the security in any simple website and how vulnerable system can be and why it's important to build a security system.

2.

In June bunch of hackers managed to steal around two million dollars from saint ambrose catholic church.

The process was simple, first, the hackers managed to get some private information through hacking into the churches email account and reading all the email and gathering enough information to convince the church that they are the contractors that currently working on renovating the church.

After that, all they had to do is send some scam emails and make a phone call to church pretending to be the contractor and pretending not being received their last 2 months payment because they have changed their bank account!

And the father of the church believed in the scammer and transfer 1,750 million dollars, which is equivalent to two months payment of the contractor to the hackers.

Source: https://www.darkreading.com/network-and-perimeter-security/how-hackers-emptied-church-coffers-with-a-simple-phishing-scam/a/d-id/1334971

---

1) One IT incident that happen was a few years ago on my old laptop. I had realized that my antivirus software had been turned off and it was not possible to turn it back on. When I tried to launch it, the software would have no response. So I thought that I would try Windows Defender then. But that had the same behaviour, no response. So I decided to uninstall the antivirus and get a new one. This new antivirus seemed to work perfectly fine so I decided to run a virus scan to inspect this suspicious behaviour that my computer had. After a while the scan was done and it found several Trojan horses. These had even spread to my personal files, such as old programming projects.

I removed the viruses that was possible to find, but the problem was that for each scan that I ran, it seemed to find more viruses. After removing some more viruses I rebooted to computer for some reason but this time I was greeted by a blue screen instead of the login screen. The boot path seemed to have been corrupted. Instead of dealing with this whole mess, I just reinstalled Windows on the computer and wiped everything on my hard drive.

I suspect that I probably got this virus infection while downloading some seemingly safe software that had these Trojan horses, or I was infected by some friend that had some of their project files infected that they shared with me.

2) This August reports came out that Huawei employees have been helping the government in Zambia and Uganda to spy on their political opponents. According to the telegraph the Huawei employees help the Ugandan government to access WhatsApp messages of a politician. WhatsApp messages are encrypted, so if this is proven to be

true it's quite concerning that they can access them in my opinion, since it's a very big breach of privacy.

According to several reports the Huawei employees also helped the Zambian government to get access to private information like phone and Facebook of a blogger in in order to arrest him due to him having been critical of the Zambian president. Huawei has denied these allegations saying "Our internal investigation shows clearly that Huawei and its employees have not been engaged in any of the activities alleged. We have neither the contracts, nor the capabilities, to do so."

These indented are quite concerning since I believe that they should not abuse such power, this news would make consumers of their products feel unsafe about their privacy, since seemingly they can access a lot of information about them and even giving in away. The US government have showed concerns about this company many times but at the same many companies from the US are seemingly guilty of similar things that Huawei is accused of. I believe that companies should stay out of these kinds of political issues and to not breach users privacy like that. But when it comes to Huawei overall I'm not as concerned as the US government seem to be as mentioned before.

Sources:
https://www.telegraph.co.uk/news/2019/08/15/huawei-employees-helped-african-governments-spy-opponents/
https://www.cnbc.com/2019/08/14/huawei-employees-helped-african-governments-spy-on-opponents-wsj.html

---

About 90% of all internet users have been a victim some kind of security incident be it directly or indirectly. A security incident is any event that may indicate that there has been a breach of one the CIA (Confidentiality, Integrity, and Availability) triad for that organization or entity. I have had some many security incidents in the past years, both directly and indirectly, some were thoroughly thought through attacks and somewhere some were so sloppy even my grandma will not fall for. However the incident I am excited to share with you is one that took me by surprise since I am a paranoid tech user who is always skeptical of every little device, email, attachment, just say anything that is connected to some network. In July 2016, I and a couple of friends planned a backpacking trip around Europe and North America, before traveling I as a student with limited economy opened a credit with one of the banks in my country. To cut a long story short, this summer was one of the best, filled with great experiences and lots of fun. Then comes September, I came back home and I got a mail from the bank with a monthly bank summary of what I have inquired in the card and how my payment plan has been set up. At first glance, I immediately noticed so inconsistencies, they had transactions and purchases in countries which I never visited. The withdrawals and purchases were countries in the middle east. I immediately called the bank and told them. At first, they thought I was making up stories not to pay. I then sent to them my passport and flight ticket to prove I had not been to those countries which my twin credit card was being used. I was furious told the bank to check if they have been breached. But deep down in me I was retracing everywhere I used my card the entire time, I remember some sketchy ATM machine which I used in a train station to get a

train ticket while in a rush. So the bank automatically suspended the credit card and after several weeks passed by the bank contacted by the bank who told me, they haven't had any breach in their part and believed my credit card was compromised maybe at some ATM I used but could not pinpoint where exactly. However, I was reimbursed and advised to always double-check for any inconsistency with an ATM machine before using.
Recent reports from the Check Point Research Labs reveals that billions of mobile users around the world might be vulnerable to an advanced SMS phishing attack which exploits a security flaw in Samsung, Huawei, LG, Sony, and other Android phones. The researchers found out that Open Mobile Alliance Client Provisioning (OMA CP) which is the industry standard for over-the-air (OTA) provisioning, included limited authentication methods which a hacker could exploit and pose as a network operator and send deceptive OMA CP messages to users. You can read more at https://www.helpnetsecurity.com/2019/09/04/android-advanced-phishing-attacks/.

Note LNU hit by a phishing campaign
https://lnu.se/mot-linneuniversitetet/aktuellt/nyheter/driftinformation/it-phishing-190905

mobile users around the world might be vulnerable to an advanced SMS phishing attack which exploits a security flaw in Samsung, Huawei, LG, Sony and other Android phones. The researchers found out that Open Mobile Alliance Client Provisioning (OMA CP) which is the industry standard for over-the-air (OTA) provisioning, included limited authentication methods which a hacker could exploit and pose as a network operator and send deceptive OMA CP messages to users.You can read more a

Experienced IT security incidents

1. Forgotten passwords. I usually try to put difficult passwords and then I end up forgetting them, being unable to log in to my accounts. (Solution always 'forgot your password' feature)

2. Shoulder surfing. It happens when I'm on my phone texting or on my laptop and someone else looks at what I am writing. Sometimes it has led to release of private information, but not with visible, severe effects.

3. False advertisements. It happened when an advertisement appeared on my phone trying to convince me to download a particular antivirus because my phone was infected with a virus (it might or might not have had one) and that advertised antivirus was supposed to be the solution. I tried to download it the first time but after the first step noticed that something was wrong. It appeared a few times later and then stopped.

4. Lottery scams. It happened via email or phone where someone faking an institution declared that I had won a lottery or a price for something in which I had never been registered before and asked me for a fee and additional information in order to get it. This has happened quite often to me and my father, usually by email and phone

messages. The first time I might have send them some of my personal data like address or phone number.

5. Social engineering. Once, at our group email arrived an email from our English teacher saying she urgently and desperately needed some money (for a reason I don't remember) and below were listed a bank number where we could donate. She wasn't even our teacher, we have never had a teacher with that name and no one fell for that.

6. Malwares. By downloading files from unsafe websites I got a malware on my laptop. I noticed when it was allocating all of it's memory (that was just one visible consequence).

Famous media news about IT security incidents

1. Facebook and Cambridge Analytica scandal. In 2018 it was revealed that a data analysis company had gathered a lot of personal information from people's facebook profiles without their consent and used it for advertisement purposes during Trump's campaign.

2. Hilary Clinton's emails. In 2016, during her presidential campaign FBI discovered that she used a private server to send classified information, while she was a secretary of state. When she had to hand these emails to the FBI, her lawyers deleted an amount of them declaring them as personal, while from the part they delivered for investigation were discovered more than 100 emails that had delivered classified information.

3. Quora's data breach. In 2018, Quora declared that a third party had compromised her system and over 100 million people's personal data was revealed, including names, emails, encrypted passwords etc.

4. Bitcoin theft in 2019. An amount of bitcoins worth around $40 million were stolen from an exchange company called Binance. The theft was made by using different techniques like phishing, viruses etc.

1.
One of the IT security incidents that I experienced was when I was younger, 7 or 8 years ago. I had a laptop which was attacked by a Trojan horse. A Trojan horse is a malware which takes the appearance of a legitimate software but actually it is modified to include the parasite. The consequences of a Trojan are quite terrible. It attack directly the OS file which become corrupted and does not work well. Indeed if a single system file is erased the OS can be severely damaged. In the end the OS of my laptop was erased and I could not use it anymore. Consequently with my laptop which does not work anymore all the information and my personal data, pictures, videos, application saved on my hard disk was gone.

Several years later the same incident happened but this time knowing what is a Trojan and knowing the risks, I managed to restore my system on a previous save state from month ago and none of my data was lost. Thanks to the first incident I became able to react quickly in order to keep my laptop.

2.

On the 20th of August, Imperva, a leader in Internet firewall services that help to prevent malicious cyber attacks, alerted its customers that a recent breach was discovered. Indeed this breach exposes the email addresses, API keys and SSL certificates for certain of the firewall users.
Imperva sells technology and services that detect and block different types of malware. The data exposure affects only the customers of the Cloud Web Application Firewall (WAF) Incapsula.

With the data exposed, at the least attackers could reduce the security settings of the WAF, but they could also attack more easily by "whitelisting" themselves. In this case, the hackers can intercept view and/or modify the traffic destined to a client. This is a quite big incident because in this case all the informations of the client do not have confidientialy and authentification any more.

The company Imperva urged all of its customers to do several steps to mitigate the threat like changing password, enabling multi-factors authentication, resetting API keys and generating new SSL certificates. Theses steps are common and it's recommended to changes our differents password often. One good things to do is to never have the same password for differents accounts.

Source: *https://krebsonsecurity.com/2019/08/cybersecurity-firm-imperva-discloses-breach/*

In an online game that I've played for many years, there were phishing attempts when the game wasn't so popular back then. The Intruders were creating a copy of the original game login site and serving it from another domain. In-game chat they were giving the link for the copy site and telling people that the game company giving free in-game stuff. When somebody clicks the link they just see the login site of the game and they think the offers are real. Therefore they write their credentials to the site. (I've done it once) It doesn't matter whether you write your credentials correct or wrong. The site always says wrong id or password and sends given information to the intruder. After that, the intruder can easily use the account or sell it to someone else. The game's Terms of use says that your account is personal and can't be shared with anyone else. (see: [2]) Hence this is a security incident and violates confidentiality.

Almost in every IT security attack, the attacker has a goal. As I understand from the incident in [1] the goal is political, and it can be preliminary for a bigger attack.

Basically, in [1] there is an attempt to infiltrate the network of the US power grid. The attackers regularly checks for the vulnerabilities in network nodes in different locations. But they couldn't succeed as said in [1].

If they managed to infiltrate the network, their actions could have heavy consequences. Since people are using electricity almost in everywhere, a big scale power cut would affect so many things. For example machine-connected patients in hospitals, transportation(subway, tram, etc.), stock exchange centers(a prolonged power cut may affect the economy), city infrastructures, etc. Also, they can do other possible actions like force the hardware limits of the power grid. This may also cause explosion, fire.

Since there are severe consequences of the attack it is important to have security. If they had noticed the attack after it succeeded it would be a disaster. Hence the security also needs to contain some kind of attack attempt detection mechanism.

[1] https://www.wired.com/story/triton-hackers-scan-us-power-grid/

[2] https://support.riotgames.com/hc/en-us/articles/204214670-Shared-accounts

---

IT security incidents experience

I remember an incident a few years ago when I was in high school. The school platform we used for assessments etc, suddenly stop working. This happened because a minor student at another school chose to attack the server where the school platform was located.

The whole story is quite funny but of course serious. I think this minor student never realized that the consequences of this act would be so big.

This was a new school platform at the time, students could submit school assignments, teachers set schedules, etc. This school platform was common to all schools within the municipality.

What happened was that this student (who went to another school) did not do his assignment in time. To get the assignment done and buy more time, he thought if he could get the platform out of service, he had something to blame. So, he performed a d-dose attack on the server and the school platform became so overloaded that it stopped working. However, this not only affected his school and his assignment, it affected all other schools and in addition, parts of the municipality's system stopped functioning when these systems shared the same server. The consequences were incredibly big, and many users were affected. The school platform was down for several days and it cost the municipality over a million to repair the damage that occurred in conjunction with the incident. All because a 13-year-old student managed to d-dos attack the server.

Media report about different IT security incidents

A couple of weeks ago I read and looked at the news of an incident about a leak of sensitive information about school students. This was an expensive school platform in Stockholm. It should have been possible for users to access other students' data which could be sensitive.

https://www.aftonbladet.se/nyheter/a/OpeWm3/sakerhetshal-i-skolsajt--kansliga-uppgifter-lackta

Another incident from this year, is how the 1177 care guide leaked recorded calls.

https://www.expressen.se/nyheter/miljontals-samtal-till-1177-vardguiden-lag-oskyddade/

What is common to these two incidents is that there are large systems with many users.

The school platform for example have cost about 700 million and has been developed over a 5-year period. Didn't they think about the security?

One problem that I think will never really be solved is that the technology is constantly evolving, and it is difficult to maintain these systems in line with the technological development, which means that vulnerabilities will always exist from that point of view.

Another problem that I think is becoming more common is that more and more people are working with development. This means that people become more aware of different vulnerabilities and can discover them more efficiently than before.

Hopefully, every security incident that occurs, means that we might focus more on safety primarily in the future

---

Section 1:

This incident occured when I worked as an IT-Technician a few years ago. A customer had got a suspected email from a foreign source. The customer worked with tourism in our municipality and daily got request, bookings and questions that was related to tourism from various countries, enterprises and private persons, and had no suspicion that this particular email was a threat or a security risk. When the customer had opened the mail, every locally stored files and documents on the computer was encrypted. And to decrypt it the source (the sender of the mail) usually asked for a ransom to return all data to its origin. But this wasn't the most serious security incident, every customer has an individual user profile which is mapped to a network drive on a server and also to a backup server, and the easiest way to restore all the corrupted data was to connect to the backup server and retrieve the backup user profile. So the technician which handled this errand made a serious security violation when connecting an "infected"/corrupted computer that had got all data encrypted to the backup server. This could have made that not only the backup data of the customers user profile to be corrupted and encrypted, but also all other user profiles stored in the backup server would have been at risk of getting their data encrypted. These kinds of security threats is often called CryptoLocker or RansomWare, which encrypts all locally stored files or documents with a specific encryption key, and the data can only be restored if you have the decryption key or access to a backup storage.

Section 2:

Earlier this spring, during midnight between march 18th/19th, an attack was launched against one of the world's largest manufacturer of aluminum, Norway Hydro. Just past midnight they detected unusual server activity. Users had got their passwords changed, files and document was encrypted and network interfaces was deactivated. Few hours later in the morning they realised that the attack had moved through and up the network hierarchy and affected the organisation globally. And they decided to disconnect all computers, servers and systems that was connected to the organisations network. More than 22,000 devices was shut of the network. A large operation to neutralize the attack, recreate lost information and data, and retrieve data from backup servers throughout the whole organisation was initiated. The production stopped completely during a time, and some automation systems needed to be operated manually. It took more than two weeks before the production was restored to 60-70% capacity. Shortly after the attack the price of aluminum rose over 1%, the highest price for over three months. It took even months before reaching normal levels of production capacity. They still don't know exactly how and where the attack started and entered the system, but speculations assumed it started in the US organisation, and could have entered through scheduled commands, group policy management or via remote access tools. The attack was labeled as a ransomware attack, using a malware believed to be "LockerGoga", and was first detected during january this year. It has only been directed against industrial- and technology enterprises and has went undetected from antivirus and security programs. During the quarterly report from Norway Hydro, it was announced that the attack would have a negative impact to the organisations result by more than 400-450 millions SEK.

reference:
https://www.atea.se/it-specialisten/sakerhet/efter-cyberangreppet-mot-norskhydro/
https://www.holmsecurity.se/blogg/hydro-attacken
https://www.hydro.com/en/search/?q=attack

Hacking has become an old habit of people who love to blackmail others!

I have experienced two hacking incidents since ten years ago, where I had no idea about software engineering, IT security or hacking in general:

The first incident was about hacking my Facebook account by a hacker. Ten years ago I have tried to access my account but i couldn't due to changing my email as well as the password, the hacker has mailed me trying to blackmail me for money in order to getting back my account, the worst part is that I have my family and friends on Facebook, the hacker have got their information and kept blackmailing me with a new support of hacked information. The consequences of this experience is that I've lost my account and haven't heard from the hacker anymore.

The second incident was about hacking my personal computer and stealing important information regarding my studies and private data. One of the hackers has attacked my computer with a bug that could collect private information of my personal life; the hacker has blackmailed me using the stolen information as a pressure tool on me, the hacker has asked me to pay $1000 in order to get back my info. I personally ignored this incident since the hacker would blackmail me for good. the consequences of this incident is that I haven't heard from the hacker anymore.

Hacking up to 50 million Facebook accounts was one of the biggest IT security incident during the past few months; where Facebook has reported almost 50 million of its users were left exposed by a security flaw, and the users that had potentially been affected were prompted to re-login after they were logged out. According to Facebook, The company claimed that attackers were able to exploit a vulnerability in a feature known as “View As” to gain control of people's accounts [1], where the attackers could control a code of the attacked platform of Facebook system. It is known that Facebook is a powerful company which has good IT security system in order to protect important data of the users, but on the other hand, the hackers have found a gap to access to those data and put people in danger. Blackmailing has already started right after the incident of Facebook, which made people mad at the company, and the trust has obviously decreased. Facebook should work more in its security since the company holds private data of people which is important and private.

References:

[1] https://www.bbc.com/news/technology-45686890

---

1) IT Security Incident I Encountered

The incident i could think of was not a direct attack to me however, it violates my privacy. I was researching on a topic so I browsed a site known as daniweb.com. It requires that you have an account to be part of the community. It is a community for technology and programming discussion. According to Daniweb, it was confirmed that the Daniweb database was breached in December 2015 in which over one million user profiles, including email addresses and IP addresses were stolen. Although they claimed logins and password were protected using additional security layer, yet, perpetrators were able to cart away with the encrypted version of the password. It was a tool called (have I been pwned) that reveal to me that I was affected by this incident.

Quickly I changed my password. Security is indeed a great challenge because even if as an individual you beef up your security, the new trends of attack shows that private and government organization are targeted the most because millions of data can be stolen. Fortunately or unfortunately an individual data could be among the stolen data.

2) The Citrix Breach

According to thehackernews.com, it was reported that the Iranian-backed Iridium hacker group hit Citrix in December last year, stealing at least 6 terabytes of sensitive internal files, including emails, blueprints, and other documents. The hacker group's proprietary techniques include bypassing multi-factor authentications for critical applications and services for further unauthorized access to VPN channels and SSO (Single Sign-On).

How Do Hackers Get Past Multi-factor Authentication?

Brute force cyber-attack: An attack known as password spraying is used. It involves an unauthorized user attempting a single password against multiple accounts before moving on to attempt a second password. This process avoids the user's account becoming locked and alerting them about suspicious activity.

Social engineering: There are various social engineering techniques used recently one of which is to social engineer a cell phone carrier into allowing them to clone a victim`s SIM card also known as SIM swap. By doing this, they receive a copy of any SMS messages sent to it, and they can also receive SMS MFA tokens as well. Sometimes, they contacts the victim and request the need of their MFA code from a source that seems genuine to the victim. Once the code is given away, the hacker will change the recovery information on all the victim key accounts.

How to Protect Against These Attacks?

The best practice currently is to enable Multi-factor Authentication wherever possible plus using an authenticator app or service. However, no amount of technology will be sufficient if users still fall prey and give out their personal details to attackers. This implies that educating people is the most critical aspect of protecting an organization or an individual user.