Grigore Lucian-Florin 324CD

Presentation Notes

Slide 1

Good afternoon! My name is Grigore Lucian and I want to give you an insight on what Cybersecurity is and why it should be a priority.

Let us consider this for a moment: there are around seven thousand languages spoken around the world. From the smallest nation to the largest continent, each language serves a different purpose. And of course there are languages more widespread that help people from different cultures communicate with each other.

But there is a language that does not come to mind when thinking about this. There is a language spoken by approximately 4 billion people all around the world. It is the language used by the communication protocols of the internet. The internet culture has become the biggest culture today.

Slide 2

Whether it is social media, YouTube or your favourite cooking website, Internet is the language that connects all its users in means that could have not been even imagined more than a century ago. It is similar to math or science in its universality. It does not matter if you are in Brazil, Japan or France. If you have one apple and someone else gives you another apple, you now have two apples and that can be understood by everyone without fail.

We are more connected than ever, but as any other innovation, Internet has its downsides or, more correct, its dangers. The more online we live our lives, the more exposed we will be to attacks. In the 21st century, online security will become just as important as physical security. And I know it sounds almost Sci-Fi-like, but I will try to convince you how important this change already is.

In the first part, I will give you an overview about what cyber warfare means and how it happens. Then, in the second part, I will try to give you an image of how can this completely change our lives, maybe without us even realising it and how can we protect ourselves from any external threat, even in the future.

Slide 3

To understand the threat completely, we need to start with the beginning. The first virus was written on a floppy-disk containing a video game and was physically inserted by someone in their computer. Funny enough, it was aimed to hack into a Macintosh, not a Windows machine. This is called a “sneakerware” virus, because you would effectively have to walk to manually insert it into a computer.

But the world has widely evolved and new types of viruses are developed every moment. Let me give you an example so you can better understand the magnitude of this type of threats.

Slide 4

We all know what happens in the Middle East. Through social media or news websites, we are given satellite images or even live recordings of the war waged there to give us a front seat view.

But there is also a hidden war, one that is not so popular, going on hidden from our sight. It is, of course, the cyber war. A war not fought with bullets and bombs, but with bits and bytes. A war where soldiers and spies become programs. A war where James Bond does not use technology, but he is technology. And much like James Bond who sneaks into an underground nuclear facility to save the world from an evil mind, programs and viruses designed to fulfil the same purposes sneak into the systems and computers controlling such facilities. In the 21st century, Agent 007 becomes Agent 001.

Slide 5

Although it may sound like a scenario for a Hollywood spy movie, something almost identical to what I have said actually happened not so long ago. A decade ago, the Israel and USA governments suspected Iran of creating more nuclear centrifuges than necessary in one of its nuclear facilities, located in Natanz, thus secretly developing mass destruction weapons. And they were right. But they could not send a person there to destroy the facility. It could become messy and would be incredibly dangerous. So they started in 2005 a joint program to stop Iran in the most clean way.

They wanted to attack the network of the facility. But how would they do it? One of the strategies revealed to the public was this one: they started by placing USB drives with the virus itself around the facility until some of them eventually got connected by the employees to the computers in 2009. And I know you ask yourselves how can that really happen, but let’s be honest: if you were to find a USB on the street, would you not insert it in your computer when you got home? The program would stay hidden from the moment it enters the network until it reaches one of SCADA (Supervisory Control and Data Acquisition) systems that control the rooms in which the centrifuges are stored. It would then mess up with the sensors and controllers to destabilise the centrifuges until these would eventually collapse and become useless. All of this has happened without any clue from the facility employees, as their systems would report nothing is wrong. They would even get fired because of it. A very clean approach prevented a possible disaster. It was called Operation Olympic Games. What a great name for such a clean approach! Vanity Fair magazine regarded this virus as “One of the great technical blockbusters in malware history”.

The problem was that the program, after infecting that particular facility, continued the search for similar systems, not stopping at all. Although being programmed to affect only the Natanz facility, it went on to spread to other countries, such as Indonesia, India or Azerbaijan. When it was finally discovered by KasperkyLab, it was named Stuxnet. A name that I’m sure some of you have heard of.

Slide 6

This is just one example of what a cyber threat can do in the future. Do not get me wrong, there have been a number of scenarios like this one before, such as Operation Aurora or Operation Nightdragon.

In September 2001, the world changed. And I am not talking about September 11, I am talking about September 18, when internet world changed. A week after the terrorist attack on Twin Towers, a program named Code Red was the world's first complex blended threat. It went around the world in three days. Innovation happens even for the bad guys.

Slide 7

Now, why did I tell you all of this? Well, to efficiently build a firewall, you have to analyse the fire.

And I know we are not a nuclear facility and, hopefully, we are not being targeted by a country such as the USA. However, we can all be targets to this type of attacks. Personal data of regular people is the most rewarding prey for cyber predators.

The biggest attacks affect the most people. Cambridge Analytica used information about millions of people for political advertising without the consent of almost all of them. In the year 2000, Melissa was a virus sent as an email attachment along with the text "I LOVE YOU". Once the attachment was opened, the process would repeat itself. In a few months, the email network was clogged up, this being the first actual report of spam.

This list can go on and on. Actually, the number of attacks are increasing year by year. Kaspersky released a report recently that stated that the number of attacks on personal data increased from 220 million, which is already a big number, to a staggering 1.3 billion. We can already be one of the victims, without even realising it.

Slide 8

The next real question is: how can we prevent being attacked? Because it is too late to think about protection when already being attacked, prevention and precaution are crucial. There are 3 main cybersecurity laws that you have to remember:

- If there is a vulnerability, it will be exploited. No exceptions.
- Everything has a vulnerability of some sort.
- Humans trust even when they should not.

Slide 9

There always has been a form of human mistake when referring to cyber attacks on personal data. Someone opened a strange email attachment or a website, or filled an online survey with his data, or even inserted an unknown USB into their

computer. You never now where the threat can come from, so exposing personal data and devices such as your laptop or smartphone should only be done to trusted sources.

After all, the smartphone is slowly becoming the most used object in our lives. I dare to say we check our phone every hour. Think about this: what situation you picture yourselves in does not find you checking on your phone for at least one hour. A conference? Going to the gym? Probably the only such situation is when we sleep, quite frankly. However, I guess some people sleep with their phones under their pillow so that they wake up when they receive a message. We use it more often, we need to protect it better.

Slide 10

Now, what should we expect in the future?

The Sci-Fi movies about online attacks show smart devices around us getting infected and suddenly becoming evil. Although I'm pretty sure some killer cookies or my fridge will not plot to kill me while I'm asleep, the impulse of creating one more layer of personal protection should be brought to reality.

We should all be considering strengthening our online defences as soon as possible. Our times are shaped by the technological advances made in the last century. But what about the technological advances made right now? Of course, they will shape the future, in a good manner or not. Thus it is our responsibility to react to these changes now so that we won't suffer later.

Slide 11

Final thoughts:

We are more afraid of being robbed of our wallet on the street than we are being robbed online, yet we use our phone exponentially more often than we walk to school or to work.

We download a free antivirus because we don't want to pay 20 euros on a premium one, yet we connect our bank accounts with much more than 20 euros in them to our smartphone.

We click the "Connect with Facebook" button on a website sometimes without even realising it or questioning about that websites' integrity.

In the 21st century, we are more connected than ever. But we are also more exposed. This century barely started and it is already giving us a glimpse of what can happen in the future. It is in our powers to shift this future into good or bad.

Slide 12

Thank you for your attention.

\+ *references*

Final observations:

The PowerPoint Presentation does not have any animations because I think this way it is easier to follow the main guidelines from this document. If I were to present it in person, I would have added some eye candy to make listening to the presentation more enjoyable.

This document does not represent what I would have printed and held in hand during the presentation itself. If I were to print anything, there would have probably been some short ideas written on at most one page. I have tried my best to write down in this document what my actual words would sound like. However, these notes do not represent my entire speech. Although they strongly resemble what the final presentation would have been like, some of the words and ideas could have slightly been altered, depending on reasons such as the audience (its lack of attention maybe) or the atmosphere (relaxed or tensioned). Additional jokes, observations or facts could have been used to ensure the success of this presentation.

PS: I consider myself a spontaneous person, so that “could” in the last statement should be replaced with “would”. :)