PLISMUN19

GA1: STUDY GUIDE

Taking Measures to Strengthen Cybersecurity

Presented by Sebastián Dulava, co-chair of the GA1

Introduction

We live in a world, where every day we spend 90 minutes on average just looking at our handheld mobile devices, that is 23 days of each year and 3.9 years of our entire lives. That is quite a lot of time considering the World Wide Web has only been active since 1991 and the first smartphone, as we know it, being released in 2007. So, there are a lot of yet unsolved, foreseeable problems with this whole new online ecosystem. The main problem, as seen by many experts and users, is the overall cybersecurity.

The level of cybersecurity, though improved dramatically over the past few years, is still an issue worth mentioning and worth solving, because not only is it a threat to people as single users, but also to large multi-million dollar corporations and even governments themselves. The most skilled online criminals and hackers have been recognized as a worldwide threat, especially considering the now more occurring cyberterrorism. The issue of cybersecurity requires much more attention and awareness in today's digital era and needs the cooperation of countries, companies and skilled individuals to help solve it, even temporarily.

Definition of Key Terms

Cybersecurity: The protection of internet-connected systems, including hardware, software and data, from cyberattacks.

White hat hacker: A hacker who works for companies to reveal to weaknesses in their system and tries to improve security on their behalf. They are often referred to as "ethical hackers" because of the morals they follow to find these security breaches without exploiting them.

Black hat hacker: A hacker who illegal attempts to gain access to files which are not disclosed to the public, usually with malicious intent but not for personal gain. They search for exploits to further their own purposes.

Cyberspace: An electronic medium used to connect devices across the globe. In essence, it is the virtual connection between all global servers.

Digital footprint: The information about a particular person that exists on the Internet as a result of their online activity.

General Overview

Basic Background

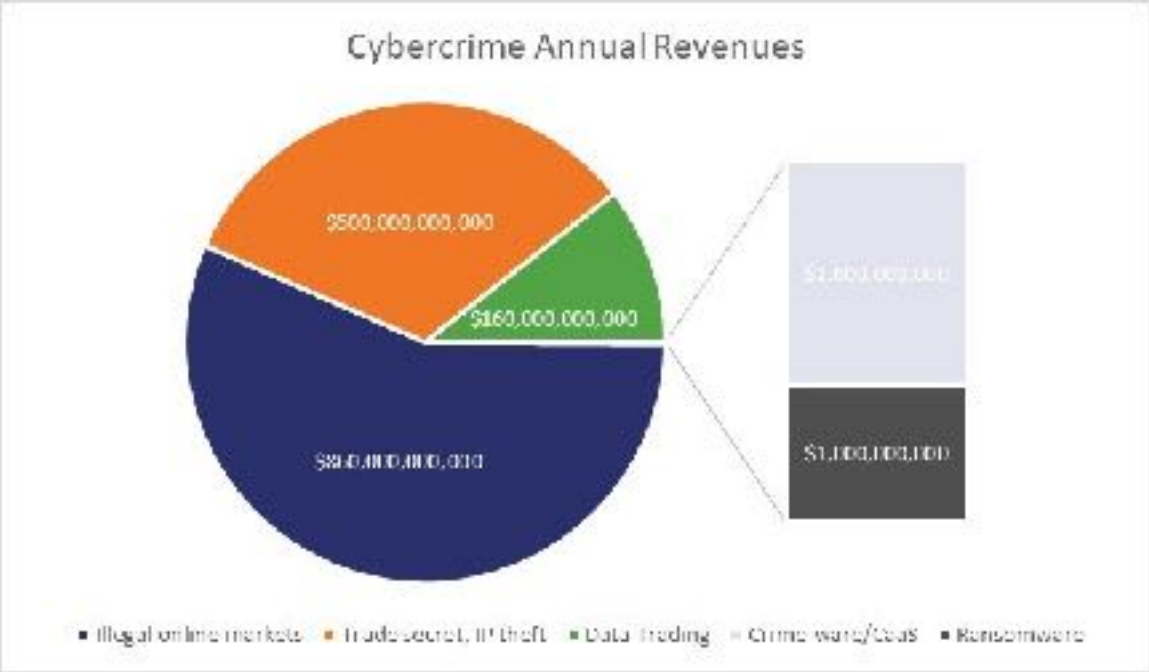
The measures, which are being taken to strengthen the cybersecurity, have been improving massively over the past few years, mostly because international corporations and governments are starting to get more aware of this pressing issue.

The International Telecommunications Union (ITU), as a United Nations specialized agency, has been researching the measures taken to improve cybersecurity amongst the UN member states and it has been producing the Global Cybersecurity Index (GCI) since 2014, now on its third iteration. In the GCI, ITU has been closely monitoring member state's commitment in five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation. This research done by the ITU has significantly helped the global cybersecurity as the participating states are coming up with new measures on how to improve their legislative stands upon this matter.

On the other end of the spectrum large international companies with their field of business in the cyberspace have been using white hat hackers to their advantage. Companies such as Google or Facebook are offering hefty sums to the white hat hackers to find security breaches in their systems, so they can seal these breaches and improve upon these mistakes so that the black hat hackers cannot infiltrate their inner workings.

Cybercrime

Cybercrime, as a whole, is composed of many different areas of focus. In 2018 cybercrime is estimated to create over 1.5 trillion dollars in profits, that is, for perspective, eight times the overall budget of the European Union for the year 2018. The three most profitable cybercrime areas include online black market, free video streaming sites and identity and IP address theft. The "cyber-criminals" can earn up to 500 thousand dollars annually and nowadays are not limited to using illegal sites and platforms, in fact a big number of reported cybercrime incidents happen on free access, legal platforms such as Facebook or the Google Play Store.



Cyberterrorism

Cyberterrorist attacks are attacks that cause violence and significant bodily harm as a tool for political intimidation using the internet, or attacks of large-scale computer network disruption usually aimed at larger companies. The definition of cyberterrorism is highly speculative and can overlap with cybercrime, cyberwar and ordinary terrorism. Some recent examples of cyberterrorism include:

a) Pakistani Cyber Army is the name taken by a group of hackers who are known for their defacement of websites, particularly Indian, Chinese, and Israeli companies and

governmental organizations, claiming to represent Pakistani nationalist and Islamic interests. The group is thought to have been active

b) since at least 2008, and maintains an active presence on social media, especially Facebook. Its members have claimed responsibility for the hijacking of websites belonging to Acer, BSNL, India's CBI, Central Bank and the State Government of Kerala.
c) British hacker Kane Gamble, sentenced to 2 years in youth detention, posed as CIA chief to access highly sensitive information. He also "cyber-terrorized" high-profile U.S. Intelligence officials such as then CIA chief John Brennan or Director of National Intelligence James Clapper. The judge said Gamble engaged in "politically motivated cyber terrorism."

Previous Attempts to Solve the Issue

As previously stated, a UN specialized agency, the ITU has been focusing on improving the cybersecurity on the governmental level and companies such as Google and Facebook have also taken matter into their own hands and are gradually improving their security systems by actually hiring hackers to find security breaches. The strengthening of cybersecurity has also been the topic of many UN-organized special events such as the “Cybersecurity and Development” event held in December of 2011 and co organized by the Department of Social Affairs (DESA) and the Economic and Social Council (ECOSOC).

Sources

https://searchsecurity.techtarget.com/definition/cybersecurity

https://www.itgovernance.co.uk/what-is-cybersecurity

https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

http://www.mobilestatistics.com/mobile-news/23-days-a-year-spent-on-your-phone.aspx

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

https://en.wikipedia.org/wiki/Cyberterrorism

http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

https://www.thesslstore.com/blog/2018-cybercrime-statistics/