CYBERSECURITY EDUCATION – THE NEW LITERACY

Alexandru TĂBUȘCĂ[1]

Gabriel GARAIS[2]

Alexandru ENĂCEANU[3]

Abstract

The present paper aims to underline the mandatory shift in higher education, especially, in order to include cybersecurity elements at all levels and domains of study. The nowadays almost complete reliance on electronic devices for sources of information, means of communications, utilities, research and even shopping, at some extent, bears a powerful emphasis on securing these electronic devices as best as possible. Besides the intrinsic security features and capabilities that are built into the hardware devices or programmed into different software applications, the human resources training and level of awareness towards the issue are critical. Even for students outside of the fields of study such as computer science, electronics, or informatics, at least a good level of general knowledge and awareness about cybersecurity issues like type of attacks, means of protection, basic rules of conduct regarding received files etc. becomes mandatory. The widespread knowledge about these issues, at higher education level within non-computer science related domains might exponentially increase the global level of security. The future highly skilled workforce of tomorrow would already be aware of the dangers and even able to avoid them, at least the most often encountered ones.

Keywords: cybersecurity education, electronic attacks awareness, cyber-education

JEL Classification: I21, L86

1. Introduction

For a couple of years now, the basic cybersecurity defence topic should have actually become almost a mandatory requirement, for almost all fields of education. Previously, the stage of the cybersecurity was almost reserved just for the computer science students/specialists or for self-taught "nerds". After the virtual explosion of all kinds of electronic devices that we, the final users, use either directly (smartphones, laptops, tablets) or indirectly (cloud services, online payments, online shopping, remote meetings, etc.) throughout the day, the need for security implies the use of so many dedicated professionals in the field of cybersecurity that it is not actually possible to cover the entire market need. The first, fastest and less expensive solution is to increase the general knowledge in the field for as many as possible, to cover at least the basic and most often happening cybersecurity incidents directly at the source, without the need of a specialized and highly

[1] PhD Associate Professor, Romanian-American University, tabusca.alexandru@profesor.rau.ro

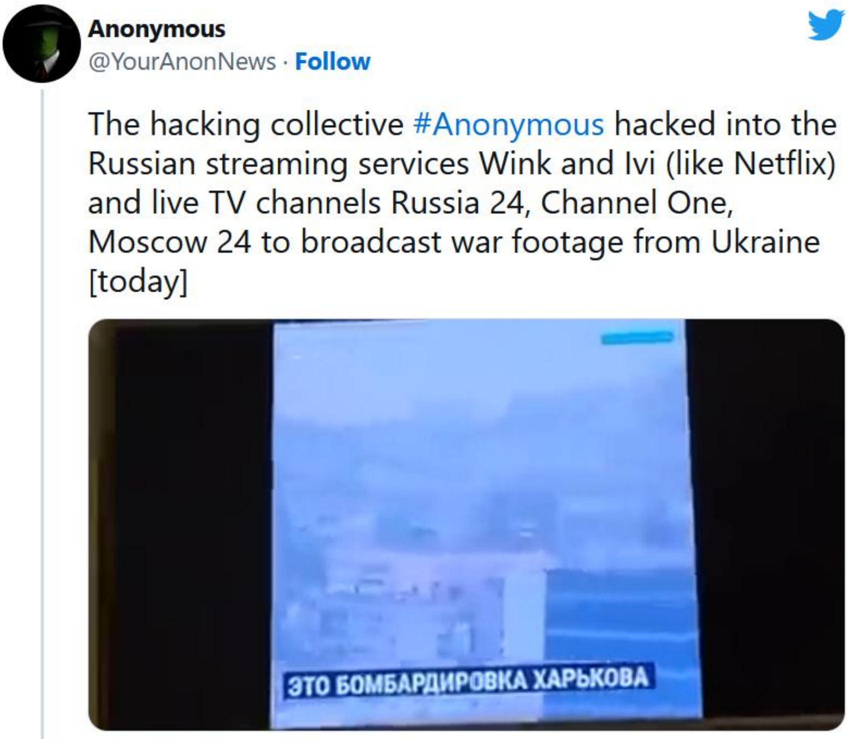
[2] PhD Lecturer, Romanian-American University, garais.gabriel.eugen@profesor.rau.ro

[3] PhD Lecturer, Romanian-American University, alexandru.enaceanu@profesor.rau.ro

skilled cybersecurity workforce.

Moreover, during the last years there were more and more incidents that showed the critical stages that might appear in case basic cyber security issues are overlooked. Just this year, after the savage, barbarian attack of the Russian red-army hordes over a sovereign and independent neighbor, Ukraine, the cybersecurity importance increased even further. Both the barbarian attackers and the resilient defenders (with a lot of help and support from all over the world) engaged in a first wide-scale cyberwar. Both parties employed mostly the DDoS attack method to stop the access and workflows of different electronic controlled systems, such as TV stations, power companies, communication networks, services of public/private utilities companies, etc.

Even though inherently a bad situation for the cybersecurity defense, the hack managed by the well-known group of online activists commonly addressed as Anonymous was one of the first successes of the civilized world in putting the Russian population in touch with the real war their demented leaders launched. In the end, the feat was not relevant because the vast majority of the aggressor's population actually supports the war, but the hack showed that even for a seemingly powerful country it is impossible to counter 100% of the cyberattacks launched against it.



Anonymous
@YourAnonNews · Follow

The hacking collective #Anonymous hacked into the Russian streaming services Wink and Ivi (like Netflix) and live TV channels Russia 24, Channel One, Moscow 24 to broadcast war footage from Ukraine [today]

Fig. 1 Capture of Russian TV station hack broadcast showing real war images from Ukraine [1][4]

[4] Source https://www.rferl.org/

In June 2022, another cyber-attack managed to paralyze the live transmission of the Russian war-criminal leader, from the St. Petersburg economic forum. The Kremlin authorities admitted that a DDoS attack stalled the forum, which was rebooted around 100 minutes later, with the Russian war-criminal delivering its lies bundled as a speech [2]. The attack itself seems to have been on a broader scale, with the livestream video delivery delay being only the visible tip of the iceberg. Sources from the participants to the forum, corroborated with official Russian administrative staff declarations, said that electronic systems problems started earlier, with the distribution of access materials such as badges (and their verification system) and with the confirmations to the main plenary not being delivered to participants. There might also have been a local element involved, as the same sources also mention a lack on onsite wireless internet connection after the problems started to appear [3].

2. Cybersecurity Basic Attacks

We will start by introducing the most common and often encountered types of cyber-attacks that took place in 2021. The same as for the previous years, most attacks are carried out from remote locations. Especially after the pandemic that brought an exponential increase in work-from-home users, at the same time and with the same rate increasing also the permanent/temporary online (mostly internet) connections between employees' locations and company headquarters, the remote-based attacks become something almost trivial in the online environment. Among the most often encountered attacks we can mention:

Malware. At this time, specialist discern several different types of malware attacks. Malware usually refers to a dedicated code written specifically to produce harm inside an IT infrastructure element (a device, a server, a certain type of file, the whole infrastructure, etc.). These attacks can be delivered to the final victim in a multitude of forms, such as worms, spyware, adware or the feared ransomware. Several cyber-security reports sustain that, in 2021 compared to 2020, there was an increase of 800% in the malware attacks at global level. Malware attacks, even though not the very sophisticated and complex of cyber-attacks, are not only a problem for private individuals or smaller companies.

Ransomware. Ransomware is considered by the specialists as a subtype of malicious software with a particular type of attack/result. If successful, a ransomware attack effectively blocks the users within a certain IT infrastructure paradigm and does not allow them to access their systems. Unfortunately, it is a very effective cyber-attack for rendering an entire IT infrastructure useless very fast. These attacks usually encrypt the victim's data/information and demand a ransom for allowing access again. Besides the fact that, in most cases actually, even after the ransom would have been paid the attackers do not release their hold on the captured data, such an attack brings also a heavy tall in company image price. In an (in)famous attack in 2017, the WannaCry malware paralyzed more than 200000 computers with Microsoft Windows operating systems, disrupting critical services from the fields of healthcare, finance, or communications. The National Health Service (NHS) in Great Britain was disrupted, Telefonica communications giant from Spain also paid its tall, and different banks, especially from Russia, were also disrupted. The malware seemed to have appeared at the same time in all locations and, even though not 100% sure even now, it is widely blamed on a North Korean hacking organization called Lazarus Group [4].

Phishing Attacks. Phishing is, by far, one of the most widely encountered attacks and one of the easiest to avoid by (very) basic awareness and cyber-security training. It is a type of social engineering attack, which actually convince a victim to share different critical data (usually credentials like passwords, credit cards info, user accounts, etc.). During such a cyber-attack a victim might also be convinced that it is needed to download a certain file, from a certain internet link within an email message. Besides the classic email carrier vector for phishing, we might also encounter different carriers such as SMS, other phone messages or social-media posts/messages.

DDoS. This type of attack is an evolution of the classic DoS (denial of service), which stops a victim IT infrastructure by oversaturated requests (usually meant to attack websites/web services). The need of the IT infrastructure to solve each request brings the impossibility to do it because of the huge number of fake requests, thus in fact bringing all the responses to a halt. The updated version of this cyber-attack, the DDoS (distributed denial of service) aims for the same purpose of disrupting the normal workflow of victim's IT infrastructure, but instead of sending all the flooding fake requests from one location (which actually might be very easy to overcome by just barring that one source location), it uses multiple sources for sending the fake requests. This variation, the DDoS, is much more difficult to counter, in reality being almost impossible to 100% protect against it. The infrastructure might become unusable for a while, but a professional contingency plan would render the infrastructure active again quite soon.

Credential stuffing attack. This type of attack is in fact one of the most important causes of data breaches. According to a series of research studies made by Google [5], no less than 65% of IT infrastructure users were using the same password for more than one account. The usage of the same set of credentials for multiple accounts brings an increased level or risk, as it becomes easier for an attacker to get hold of one's password and use it for multiple accounts of the same victim. In credential stuffing attacks, the credentials obtained by the cyber-attacker (usually usernames and passwords), in most cases from a data breach, are later used to obtain critical data from one of the victim's "partners" of electronic conversations (employer, bank, e-commerce websites, etc.).

Password attacks. The very often encountered password attack is the one of the oldest and easiest to carry out type of cyber-attack. It represents a common causes of data breaches, based on the users' lack of cybersecurity awareness, especially in the case of very weak passwords that become very easily exploitable. One of the US giants of telecommunications, Verizon, published a report [6] mentioning that 61% of data breaches are due to weak passwords.

IoT weaknesses. By deploying this type of attack, the wrongdoers target a network of IoT (internet of things) devices or a single device or a specific type of devices. Due to different exploits and security breaches that are not covered by the producers/users the hackers can take control of a device and, usually, they can use it for two different types of attacks. They can either infiltrate the specific IT infrastructure the device is part of (and snoop for data, collect unauthorized information either in electronic format or even in audio/video mode) or they can take control and use it later to set up an entire army of dumb/bot devices that can further disseminate a cyber-attack in the category of DoS or DDoS. Due to the explosive expansion of IoT devices, it is most probable that the near future will bring an even greater number of attacks onto this vector.

Man-in-the-middle. This type of cyberattack is usually a much more insidious attack than the previously presented ones. The previous attacks are very visible, very soon/immediately, after the attack, as they are engineered to produce visible harm. The man-in-the-middle attack is usually used for infiltration and collecting data without authorization, within the transmission between two network points. The attacker tries to impersonate one of the two authorized parties of an electronic exchange of data (conversation) and thus can receive information such as passwords, personal data, other types of credentials, financial info etc. The results of this attack can be seen much, much later, as in a lot of cases the fake receiver of a transmission will also send the information forward, to the original destination. Such an attack can last for a long time, with an unauthorized party spying on electronic conversations and just extracting data without actually stopping the transmission process.

Cross-Site Scripting (XSS). An XSS type of cyber-attack appears if a hacker manages to inject a malicious set of code into a victim website. The malicious lines of code are usually launched as a script file, inside the victim’s web browser and is responsible for acquiring unauthorized data send by the users through the web browser.

SQL Injection. This type of attack, dissimilar to the XSS one, usually targets a database client rather than one user directly. Nevertheless, especially with the multitude of web platforms/frameworks that rely on databases for maintaining a website, (such as the omnipresent Wordpress also), the cyberattack is in fact targeting websites in a lot of cases. The logic behind this type of attach is very similar to the XSS type.

Based on estimates for the COVID-19 pandemic times, the rate of cyberattacks (of all kinds) increased by 600% between pre-pandemic and end-of-pandemic times.

A very well-known and respected specialist in the field, the publisher of Cyber Defense Magazine[5], Gary Miliefsky, said "*Cybercrime has surpassed Drug Crime as the largest form of global thievery since 2018 and continues to grow. At Cyber Defense Magazine, we predict that Cybercrime will account for over $12 trillion in theft and damages by 2025*". He also concludes that "*The biggest form of cybercrime is spear phishing and remote access trojans (RATs), which are not that sophisticated at all*".

3. Basic Response Solutions

Besides the last three types of attacks mentioned in the previous section of our paper, which require specific and technical expertise to address, all other types of attacks, all others can be avoided, at a high rate of success, by implementing only cybersecurity awareness principals that can be taught to and mastered by people not working in the IT field as their main activity.

At this time, the labour market does not offer enough highly skilled cyber-security professionals, and the situation is not possible to be addressed very soon – as such a specialist does not become available overnight, besides the basic and traditional training (computer science schools, dedicated cybersecurity programs) that might be available the person itself must be capable of understanding and efficiently employing a lot of mathematical and logical tools. Nevertheless, we consider that at least a part of the problem might be addressed by teaching skilled workers from other fields to efficiently make use of a set of basic tools and principles related to cybersecurity. Thus, by hugely enlarging the "army" that knows how to counter (lots of) cybersecurity attacks, we will correspondingly diminish the risk of important breaches of security.

The main body of cybersecurity specialists today consider that a good cyber-security posture can be attained by a company if it pays specific attention to the following cyber-defense elements [7]:

- Asset management and inventory identification
- Management of risks
- Access rights management
- Management of threats
- Security controls
- Disaster recovery and business continuity
- Management of security incidents
- Cybersecurity education, training, and awareness

All the elements above, even though their titles are seemingly very IT technical oriented, can in fact be covered at proficient enough level, by cybersecurity education implemented at non-technical study programs, within the higher education systems (and even at high school level with dedicated modifications). Students from the fields of law, sports, economics, arts, etc. can be taught the most important basic elements of cybersecurity, they can be made aware of the huge risks that a weak password, the usage of the same username

[5] https://www.cyberdefensemagazine.com

and password for all websites or dismissing upgrade/updates for the security software might imply.

On the other hand, we should not forget that there are cyber-security services that only highly skilled and dedicated professionals can efficiently provide. There are services that only a professional IT engineer or dedicated cyber-forensics company can provide: pentesting, internal and external network audits, network intrusion analysis, vulnerability assessments and digital evidence preservation.

However, even in a SOHO[6] environment, without trained cyber-security professionals, there are several things very easy to implement, that can be used against intrusions by anyone with a minimum basic cyber-security education:

- *Use antivirus and antispyware* - To gain access to data, attackers install malicious software on attacked devices, such as viruses, trojans, worms, ransomware, and spyware, without permission. Viruses can destroy sensitive data, slow down the computer, or they can take control of it. A way for computer viruses to take control of the computer is to allow spammers to send emails from someone's account. Spyware can monitor online activities, collect personal information, or create unwanted pop-up ads in your browser. It is advisable to download software only from trusted websites to avoid being infected with spyware. Antivirus solutions scan the computer and incoming emails against viruses. Sometimes, antivirus software also includes antispyware. Frequently update the antivirus to protect against the latest versions of malicious software, preferably by using the automated update options.
- *Keep the firewall enabled* - Whether it's a software firewall or a hardware firewall on a router, the firewall must be active and up to date to prevent hackers from accessing private data.
- *Manage the operating system and browser* - Hackers are always trying to take advantage of vulnerabilities in the operating systems and web browsers. To protect the computer and personal data, the computer and browser security settings must be maintained at a medium or higher level. Update computer's operating system, including web browsers, and regularly download and install the latest software patches and security updates from vendors.
- *Protect all your devices* - Your devices, whether they are computers, laptops, tablets, or smartphones, must be password protected, better yet – implement MFA[7] if possible, to prevent unauthorized access. Stored information must be encrypted, especially if it is sensitive or confidential data. For mobile devices, store only the information you really need, in case the device is stolen or lost when you are away from home. If any of your devices is compromised, cyber-attackers can access all data through your cloud storage service provider, such as iCloud or Google Drive.
- *IoT devices* - present a higher risk of infection than other devices. While mobile, desktop and laptop platforms receive frequent software updates, most IoT devices still have the original firmware. If there are vulnerabilities in the firmware, the IoT

[6] SOHO = small office, home office

[7] MFA = multi-factor authentication

device will remain vulnerable. To make matters worse, IoT devices are designed to require Internet access. Most IoT devices are designed to require Internet access from the client network. The result is that IoT devices allow access to the local network and customer data. The best way to protect is for IoT devices to use an isolated network (guest SSID and/or different VLAN).

- *WIFI routers* - last but not least, update the to the latest firmware to prevent attacks such as Key Reinstallation Attacks [8]. This attack was discovered in 2017 and updated in 2018 and works against all modern protected Wi-Fi networks, so if the router manufacturer doesn't provide an updated version of firmware, it is advised to replace the router with a newer one.

4. RAU[8] Case Study

As a case study for our idea, the Romanian-American University is currently implementing a cyber-security focused project, called "Let's Protect our Future Better! Advanced Cybersecurity". Inside the framework of the project, we have registered 23% of the applicants for internship cyber-security related internship stages that were not students of computer science programs, but actually came from other fields of study such as tourism, law, management & marketing, physical education or economic studies. Every category of students was assigned to a specifically tailored internship stages, focused on their specific field in correlation with cybersecurity elements. There were devised different activities enhancing their knowledge and skills in sub-areas such as: cyberlaw (for law students), personal data protection (for management-marketing students), data regulations and public requirements (for tourism students), protection of medical-record information (for sports and kinesiotherapy students).

The students that were involved in this project have followed a selection process, so that they were accepted into toe project based on their previous background and letter of interest they attached. Each accepted student has gone through a process of professional counseling in order to be prepared for the courses in the field of cybersecurity, but also to be able to be directed to the sub-field that suits him best (cyberlaw, testing, personal data protection, software development etc.). The interest shown by the students for the activities of the project is also supported by the statistics below.

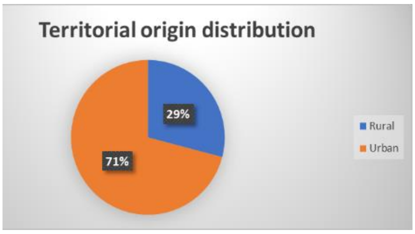


Fig. 2 Distribution of participants by domicile classification[9]

[8] RAU – Romanian-American University, Bucharest, Romania

[9] Source: RAU implemented project statistics, http://practica-cybersecurity.rau.ro/

The distribuition piechart shows that most of the enrolled students come from the urban area, a result that is actually consistent with the higher number of high school and university students that come from this area, compared to the rural one.

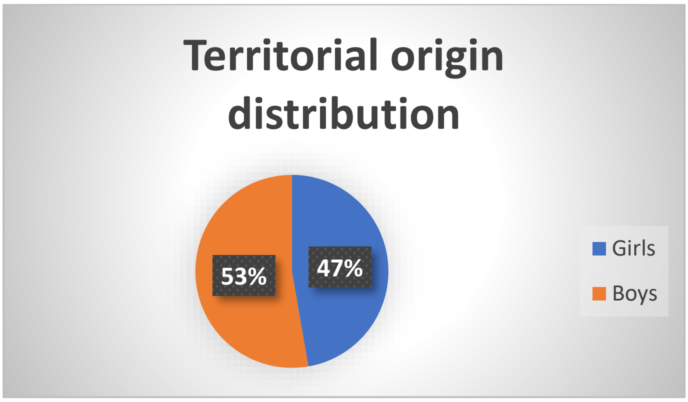


Fig. 3 Distribution of participants by sex[10]

It is interesting to mention that the result of the distribuition by sex is almost equal between male and female participants, while the statistics for Computer Science study programs, focused on cyber-security, show a rather different distribution with around 76% of the students being males.

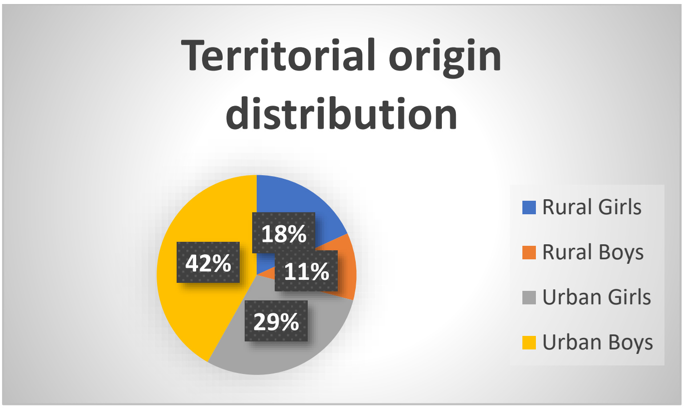


Fig. 2 The distribution of participants based on a compound territorial and sex indicator[11]

Not surprisingly, the combined result of applying both the territorial and sex criteria shows us a majority of participants as being males from urban areas, followed by the percentage of female participants coming also from the urban areas. There is a small surprise for the last position – the lowest percentage of participants comes from rural areas and are males.

[10] Source: RAU implemented project statistics, http://practica-cybersecurity.rau.ro/

[11] Source: RAU implemented project statistics, http://practica-cybersecurity.rau.ro/

Again, this is different from the normal Computer Science study programs focusing on cybersecurity, which have the rural & females compound category on the last position.

These statistics support the idea that basic cybersecurity education can be successfully delivered to all kind of students, regarding not only the fields of study they come from, but also their distribution based on type of origin (urban/rural) and sex (female/male).

5. Conclusions

At the end of the internship stages, the successful graduation of the programs was at an excellent level, with 100% successful internships for the non-computer science students. This figure also adds to our idea that short-term, specific-field of study, trainings for higher education students, in the area of cybersecurity, can prove very successful. These trained students will act as a multiplier and forward the spread of good-practices to their colleagues and (future) employers, thus increasing the all-around level of cyber-security defense even without the use of highly skilled, highly trained and highly expensive, cyber-security professionals.

Of course, the dedicated professionals are and will always be needed, as more complex and technically-subtle cyber-attacks are not even visible, let alone mitigated, by the above-mentioned category of “light-cyber-security” specialists.

References

[1] https://www.rferl.org/a/russian-tv-hacked-ukraine-anonymous/31740663.html - Radio Free Europe Radio Liberty; last access: June 18, 2022

[2] https://www.darkreading.com/attacks-breaches/ddos-attacks-delay-putin-speech-russian-economic-forum - Dark Reading; last access: June 18, 2022

[3] https://www.bloomberg.com/news/articles/2022-06-17/kremlin-says-cyberattack-delays-putin-s-forum-speech-by-1-hour - Bloomberg Europe Edition; last access June 18, 2022

[4] https://www.malwarebytes.com/wannacry - last access: June 19, 2022

[5] https://www.infosecurity-magazine.com/blogs/your-employees-reusing-passwords/ - last access: June 19, 2022

[6] https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/ - last access: June 18, 2022

[7] Tăbușcă, A., Tăbușcă S., Basic Cyber Defence Education for Everyone, Journal of Information Systems & Operations Management, Vol. 16.1, Bucharest, pp 253-263, May 2022

[8] https://papers.mathyvanhoef.com/ccs2018.pdf - Release the Kraken: New KRACKs in the 802.11 Standard - last access: June 19, 2022