https://doi.org/10.52326/ic-ecco.2021/NWC.05

Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions

Alexei Arina[1], Nistiriuc Pavel[2], Alexei Anatolie[3]
Technical University of Moldova, 168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova
arina.alexei@tse.utm.md[1], pavel.nistiriuc@fet.utm.md[2], anatolie.alexei@adm.utm.md [3]

***Abstract*— Higher Education Institutions (HEIs) have always been the target of cyber attacks due to the information assets they hold. The move to online study as a result of restrictions imposed in the spring of 2020 has led to increased cyber security threats to academia due to the vulnerabilities of online learning platforms and video conferencing applications. The hypothesis of this paper was that Moldovan Higher Education Institutions had to face cyber security challenges similar to international higher education institutions, through the empirical study, the use of the questionnaire-based survey to collect quantitative data from stakeholders of the institutions.**

The results of the survey conducted between September and November 2020, showed that HEIs in Moldova are targeted by cyber attacks as well as international ones and the nature of threats is mostly the same, namely: malware, phishing and DoS attacks.

***Keywords*— threat; attack; HEIs; malware; phishing; DoS/DDos; third-party software.**

I. INTRODUCTION

The use of Information and Communication Technology in academia has transformed the way we approach learning and educational activities in general. The Covid 19 pandemic, that began in the spring of 2020 and continues to this day, has been an impetus for the transition from traditional classes to online education. IT departments have had to cope with the growing requirements to ensure the continuity of the educational process, such as high volume of data storage, centralized configuration of video conferencing applications and emails, online learning platforms; they represented only some of the challenges of the new reality.

HEIs from the Republic of Moldova, as well as the international academic environment, had to face new challenges. And the resulting digital progress is impressive. In addition to the online learning platforms used for real-time access to educational resources and online exams, the range of digital services has grown significantly. Here we can mention the electronic libraries, the implementation of university management systems, online admission, etc.

Thus, in the near future, Moldovan HEIs could implement new services to increase their profits, by attracting more potential students who, due to the fact that they are abroad, do not opt for universities in the Republic of Moldova. Many international researchers believe that as distance education becomes more prevalent, countries and Higher Education Institutions, that do not provide distance education courses will need to look at this option to retain and expand their student population [1], [2]. According to the latest research conducted by 2023, the online education market will grow by an average of 16.4% annually [3]. A recent global survey by Pearson Education, an academic publishing organization, showed that 90% of 7,000 respondents believe that online education will continue to play a very important role in the field, even after the end of the Covid-19 pandemic [4].

The digitization of HEI and academic distance learning are undeniably beneficial, but new problems arise with regard to the protection of communication networks. Problems related to threats, vulnerabilities and cyber-attacks targeting the communication networks used to carry out online activities. The ISO27000 information security standard defines the cyber threat as: "the potential cause of an unwanted incident, which can lead to damage to a system or organization"; vulnerability as: “weakness of an asset or control that can be exploited by one or more threats”, and cyber-attack as: “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset ”[5].

The data in the security reports reflect a significant increase in cyber security attacks in higher education institutions as a result of distance learning in 2020 [4], [6].

The purpose of this article is to reflect the results of the survey conducted by the authors in September-November 2020, which was attended by eight stakeholders from the largest higher education institutions in the Republic of Moldova. A stakeholder can be “any group or individual who can be affected or is affected by the achievement of the firm’s objectives” [7].

https://doi.org/10.52326/ic-ecco.2021/NWC.05

The survey focused on identifying real cyber threats and attacks in the Moldovan academic environment in 2020, in order to identify the cyber security challenges faced HEIs and whether they are similar to those of international HEIs, analysed by the authors in published scientific articles [4], [6] and international cyber security reports [8]–[10].

The hypothesis to be demonstrated in this scientific article is that Moldovan Higher Education Institutions face the same cyber security challenges as international HEIs, through empirical study.

The paper is organized as follows: the second section will reflect the analysis of cyber threats in 2020 that have affected HEIs internationally, the third section will describe the method used to demonstrate the hypothesis, the fourth section is for results and limitations, and the last will reflect the authors' conclusions.

II. BACKGROUND

In 2020 the education domain had a loss of $ 3.90 million for data breach, according to IBM & Ponemon Institute [8], which conducts cybersecurity research. Referring to another study realized by CheckPoint [9], a leading provider of cyber security solutions to governments and corporations globally and in Europe too, the average number of weekly cyber-attacks per academic organization in July-August 2020, increased by 24%. In contrast, the overall increase in the number of attacks in all sectors in Europe was only 9% [6].

The new challenges of 2020 are due to the vulnerabilities of video conferencing applications and online learning platforms [6].

The use of online learning platforms has increased in 2020. The data provided by Google Trend (figure 1), for the period 2019-2020, showed a massive increase of interest in various learning platforms, both in Europe and globally. Complex courses were created, which had several types of activities, such as seminars, lessons, glossaries, practical tasks, assessment tests. It is also attested that Moodle is the most popular learning platform [4].

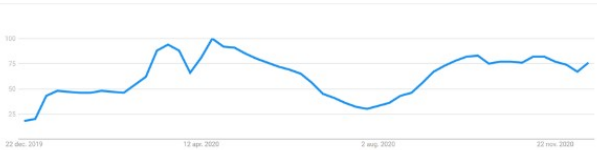

Figure 1. Global interest level for Moodle 2019-2020 [4]

A really impressive increase in use, during the pandemic with Covid-19, had the applications for teleconferencing, because the vast majority of activities and events planned offline, migrated, due to the new conditions of activity, in the online environment [4]. According to the report submitted by the company Datanyze, the world leader in technography, top three teleconferencing applications used in 2020, globally were: Zoom, GoToWebinar and Cisco Webex [4], [10].Thus, if in December 2019, the ZOOM application registered 10M daily users, in March 2020, ZOOM registered about 200M daily users [11].

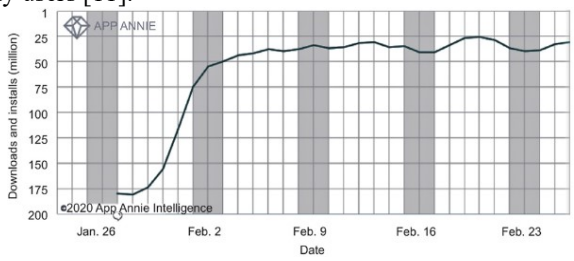

Figure 2. Zoom application usage [12]

The number of users who encountered various threats, in 2020, related to online learning platforms and video conferencing applications increased by 20455% [6], [13].

In June 2020, Microsoft Security Intelligence reported that 61% of the 7.7M malware attacks recorded in the last 30 days, were related to the education domain, more than any other sector of the industry [13]. The malware that has targeted educational domain the most in 2020 is ransomware [6]. Ransomware is malicious software that allows a hacker to restrict access to authorized users, such as students or university staff, by encrypting disks and then requesting a form of payment to lift the restriction [14], [15].

The same report [13], shows that DOS/DDoS attacks have increased, in educational domain, by 350-500% in 2020 compared to the same period in 2019 [6]. Denial of Service (DoS) attack is executed to determine a specific category of information warfare where a malicious user blocks legitimate user from accessing network services by exhausting the resources of the victim system [16]. The substantial increase in DoS / DDoS attacks in HEIs is primarily due to distance learning, as the vast majority of university services, such as: access to the university library, study hours, access to course resources, exams and intermediate assessments, admission to studies; this year have been in the online environment, and disruption of these services shall interrupt academic activity [6].

The leader of cyber threats in HEIs was phishing. It is a social engineering attack wherein a phisher attempts to lure the users to obtain their sensitive information by illegally utilizing a public or trustworthy organization in an automated pattern so that the internet user trusts the message, and reveals the victim's sensitive information to the attacker [17]. According to new research conducted by Barracuda Networks [18], HEIs were targeted in June-September 2020 by more than 3.5M phishing attacks, more than 25% of phishing attacks occur in the educational sector. In the UK, according to a Jisc survey, phishing is the biggest threat to corporate network security in HEIs [19].

According to the data presented in this section, it can be concluded that cyber-attacks in the international

https://doi.org/10.52326/ic-ecco.2021/NWC.05

academic environment have increased as a result of distance learning.

III. METHODOLOGY

The method used by the authors to identify the challenges and approach of cyber security in HEIs in Moldova was the survey based on the questionnaire.

To conduct this survey, 8 stakeholders from 8 largest HEIs in Moldova were contacted. A special invitation email was sent to the selected sample (university stakeholders) so as to ensure that data collection was limited to the specific target group. The survey was based on online platform, namely Google forms. To ensure data confidentiality, anonymous participation was enabled, and the results were stored in a local database for further analysis.

Before finalizing the survey tool, we conducted a small pilot study to evaluate the reliability and validity of the tool. The main purpose of the pilot study was to verify whether respondents are able to understand and answer all the questions [20]. Two methods were selected for the study. The first method was to present the survey tool to IT experts, with several years of experience working on cybersecurity issues. And the second method was the analysis of international practices in this area, useful resources were identified in the UK, which at the government level [21] has implemented annual surveys that identify the state of cybersecurity in national HEIs. Based on the feedback received from IT experts, several minor changes were made to the questionnaire. The research design is reflected in figure 3.

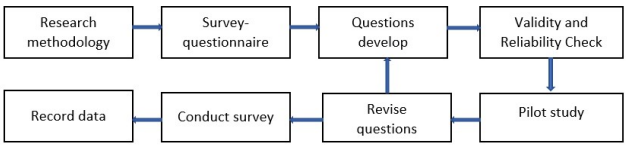

Figure 3. Questionnaire Research Design Procedure

The survey was created to demonstrate the hypothesis of this study. Response choices to the multiple-choice questions were based on issues and concerns related to Cyber Security Threats in HEIs. The survey took approximately 10 min to complete.

Survey results were recorded in Google Forms and an Excel spreadsheet was used to collect eight stakeholders' responses. Descriptive statistics of the responses to the survey are presented in graphs. The descriptive statistics provide summaries about the sample's answers to each of the questions as well as measures of variability (or spread) and central tendency [22].

IV. RESULTS AND LIMITATIONS

In this section, we present the results obtained. The survey was conducted in the month of September to November in 2020, deals with the status of cyber security threats that have hit respondent's organization. It was found that 80% of higher education institutions in Moldova were attacked in 2020 (institutions that participated in the survey). Based on these responses, further explanations are provided. The distribution of cyber threats that HEIs have had to deal with, is reflected in Figure 4.

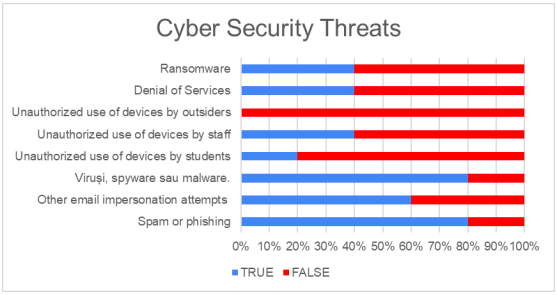

Figure 4. Cyber threats facing HEIs in 2020

Thus, it can be seen that the biggest challenges for stakeholders in 2020 were spam or phishing attacks (80%) and attacks with malicious programs: viruses, worms or Trojan Horse (80%). Ransomware or DoS attacks were recorded by 40% of respondents. And threats targeting unauthorized use of university devices by staff, such as computers, servers or network devices, were recorded by 40% of organizations. Unauthorized use of the devices by students or outsiders was not a threat, probably the main reason being that the educational process took place mostly online, so visits by students or outsiders were not frequent and were recorded.

When asked what are the 3 most common threats to your institution, stakeholders selected from a list of 10 options: DoS or DDoS attacks (40%), Phishing and Social Engineering (20%), Ransomware (20%) and MITM attacks (20%), the results are graphically shown in figure 5.

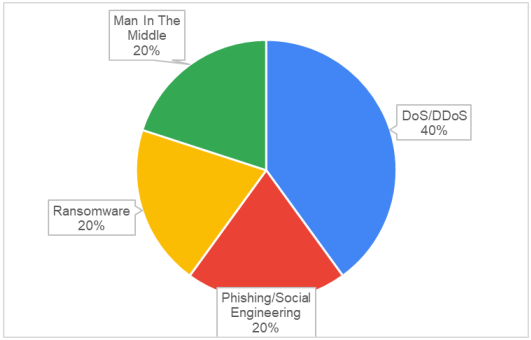

Figure 5. Frequent cyber threats

Although the findings presented in this paper provide important points for assessing cyber security threats,

https://doi.org/10.52326/ic-ecco.2021/NWC.05

several limitations need to be highlighted, which we plan to improve in the future. The questions covered in the survey should be checked by several cybersecurity experts. The preliminary data produced valuable results; however, further research needs be carried out on universities. The sample size must be increased, which may improve the findings.

V. Conclusions

Ensuring cyber security in HEIs is a current priority, especially in the context of the Covid 19 pandemic. Empirical studies can elucidate the real challenges in this area. Thus, based on the results of various security studies and reports conducted in 2020, a hypothesis was developed targeting HEIs in Moldova regarding the security threats faced by stakeholders during the pandemic. The hypothesis was to determine through quantitative data analysis, questionnaires-based surveys, which network threats targeted university networks in 2020, and which, in the opinion of stakeholders, are the most common security threats in HEIs in the Republic Moldova.

The results of the survey reflected a high rate of cyber-attacks taking place in HEIs in Moldova, so that 80% of respondents said that in 2020, the institution they represent was targeted by cyber-attacks. This means that, although Moldovan academic institutions are not as well known in the international arena, ensuring cyber security must be a priority. Cyber security threats remain the same as in international HEIs. It is advisable for HEIs to create cybersecurity frameworks that will target the completeness of the security measures that need to be implemented to secure the academic environment. Also, annual government surveys, similar to those in the UK, which aim to identify the level of cyber security in education, given the dynamic digital development in this field, will allow the adjustment of recommended protection measures to real threats.

References

[1] M. Nakamura, "The State of Distance Education in Japan," Quarterly Review of Distance Education, vol. 18, no. 3, pp. 75–87, 2017.

[2] P. Fidalgo, J. Thormann, O. Kulyk, and J. A. Lencastre, "Students' perceptions on distance education: A multinational study," International Journal of Educational Technology in Higher Education, vol. 17, no. 1, Dec. 2020, doi: 10.1186/s41239-020-00194-2.

[3] A. Shahzad, R. Hassan, A. Y. Aremu, A. Hussain, and R. N. Lodhi, "Effects of COVID-19 in E-learning on higher education institution students: the group comparison between male and female," Quality & Quantity, Aug. 2020, doi: 10.1007/s11135-020-01028-z.

[4] Alexei Arina and Alexei Anatolie, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 10, no. 3, Mar. 2021.

[5] ISO 27005. https://www.iso.org/news/2008/06/Ref1139.html (accessed Jul. 19, 2021).

[6] A. Alexei, "NETWORK SECURITY THREATS TO HIGHER EDUCATION INSTITUTIONS," in CEE e|Dem and e|Gov Days, May 2021, pp. 323–333. doi: 10.24989/ocg.v341.24.

[7] B. L. Parmar, R. E. Freeman, J. S. Harrison, A. C. Wicks, L. Purnell, and S. de Colle, "Stakeholder Theory: The State of the Art," The Academy of Management Annals, vol. 4, no. 1, Jan. 2010, doi: 10.1080/19416520.2010.495581.

[8] Kaspersky, "Education Report," 2020. Accessed: Dec. 09, 2020. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_0409 2020_2.pdf

[9] JISC, "Cyber Impact Report," 2020. Accessed: Dec. 09, 2020. [Online]. Available: https://repository.jisc.ac.uk/8165/1/cyber-impact-report.pdf

[10] Ponemon Institute and IBM, "Cost of a Data Breach Report," 2020. Accessed: Jan. 09, 2021. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report

[11] Check Point Research, "Cyber Security Report," 2020. Accessed: May 30, 2021. [Online]. Available: https://www.checkpoint.com

[12] Datanyze, "MARKET SHARE: Web Conferencing," 2020. Accessed: Dec. 05, 2020. [Online]. Available: https://www.datanyze.com/market-share/web-conferencing--52/Datanyze%20Universe

[13] Gina M. Vitiello and Chamberlain Hrdlicka, "Video Conferencing and Recording: Know the Risks Before You Connect." Accessed: Dec. 03, 2020. [Online]. Available: https://www.law.com/legaltechnews/2020/04/23/video-conferencing-and-recording-know-the-risks-before-you-connect/

[14] Z. R. Alashhab, M. Anbar, M. M. Singh, Y.-B. Leau, Z. A. Al-Sai, and S. Abu Alhayja'a, "Impact of coronavirus pandemic crisis on technologies and cloud computing applications," Journal of Electronic Science and Technology, Nov. 2020, doi: 10.1016/j.jnlest.2020.100059.

[15] R. Brewer, "Ransomware attacks: detection, prevention and cure," Network Security, vol. 2016, no. 9, Sep. 2016, doi: 10.1016/S1353-4858(16)30086-1.

[16] A. K. Maurya, N. Kumar, A. Agrawal, and R. A. Khan, "Ransomware Evolution, Target and Safety Measures," International Journal of Computer Sciences and Engineering, vol. 6, no. 1, Jan. 2018, doi: 10.26438/ijcse/v6i1.8085.

[17] S. kumarasamy, "Distributed Denial of Service (DDOS) Attacks Detection Mechanism," International Journal of Computer Science, Engineering and Information Technology, vol. 1, no. 5, Dec. 2011, doi: 10.5121/ijcseit.2011.1504.

[18] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Frontiers in Computer Science, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[19] Barracuda, "Threat Spotlight Spear Phishing Education," 2020. Accessed: Dec. 12, 2020. [Online]. Available: https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5-2020L.pdf?mkt_tok=eyJpIjoiTVdNellXVmlOREExTURoaSIsInQiOiJJM1ErR0FRaHFsc2YyU2dMdEhmUVFSVW1XYkxBYzB3T1JqSzgrZlVZZ25paGx4c25sRWN0S0pWSW5wa3RqTEFMRm83cFJmazlcL2dhK3FHZFZWMVQyXC9KOVpzVjdXb3VEMWlUVXg0blp2cjFaend1NGRZaU5VZkNsK2NhaDhzUFFIIn0%3D

[20] Hamed Taherdoost, "How to Design and Create an Effective Survey/Questionnaire; A Step by Step Guide," International Journal of Academic Research in Management , vol. 5, no. 4, pp. 37–41, 2016.

[21] "National Cyber Security Center." https://www.ncsc.gov.uk/ (accessed Aug. 29, 2021).

[22] P. Fidalgo, J. Thormann, O. Kulyk, and J. A. Lencastre, "Students' perceptions on distance education: A multinational study," International Journal of Educational Technology in Higher Education, vol. 17, no. 1, Dec. 2020, doi: 10.1186/s41239-020-00194-2.