UDC: 004.7.056:37.07
Professional paper

CYBER SECURITY IN EDUCATIONAL INSTITUTIONS

Yllka BAHTIRI[1*], Enkelejdë BYTYÇI[1], Florim IDRIZI[1], Shpend ISMAILI[1], Nexhibe SEJFULI - RAMADANI[1]

1 Department of Informatics, Faculty of Mathematics and Natural Sciences, University of Tetova
[*]Corresponding Author: e-mail: y.bahtiri211510@unite.edu.mk

Abstract

Data security is the main challenge of any internet communication, the world is facing many major cyber-attacks, and many jobs today cannot be done without the use of internet. It is impossible for a medium that transmits data to be secure all the time. The higher the speed of communication, the greater the chance of errors. Educational institutions face a range of cyber security threats, including malware infections and data misuse. This paper will analyze the types of cybernetic security threats faced by educational institutions in Kosovo and the impact they may have on students, teachers, and staff. It also examines the various strategies that can be implemented to reduce these risks, such as using passwords, regularly updating software and systems, and providing information security training to staff and students. The research is based on a review of existing literature and case studies, as well as interviews with cyber security experts and cyber technology professionals in the education sector in Kosovo.

Keywords: Cyber security, University, Cyber-attacks, Information data, etc.

1. Introduction

Security is the preservation of knowledge, data information.Cyber security is of great importance if we talk about it and activism in the field of technology.During the great use of technology, the awareness of cybercrimes and attacks that occur in various institutions that are hidden behind public perception increases a lot[1].Education for cyber security is one of the main topics in every institution of higher education; all academics in this field have given priority to the security of the data that is possessed in these institutions [2]

Cyber security is made for information security. Keeping information secure is a major challenge nowadays.

Given the unlimited number of free websites, the Internet undeniably has a recovered mode known as cybercrime. Governments and private sectors are taking many measures to control these cyber crimes.

Addressing cyber security is still a big deal [3] Cyber ethics is nothing but the code of the internet. Practicing cyber ethics is a good chance for the entire Internet to be correct and protected [4]

2. Cyber Security

Cybercrime is a growing term, icily it is an activity carried out by different people through computers and the Internet. Cybercrime refers to the part of misuse, receiving unauthorized documents, using illegal programs, disturbing either a person or an entire institution. Cyber crimes are committed by hacking the software and hardware of a respective institution. With the increase in the use of the Internet and technology, the increase in cyber crimes is inevitable. The Internet is the one that initiates a cyber attack, which is very popular in our society. [5]

3. Cyber Security in Educational Institutes

Every educational institution has sensitive data for academic staff, students and other employees.

There are several types of attacks that educational institutions face, among the most common ones we encounter are: phishing, DDoS attacks, ransomware and terrorist and internal threats.

Phishing is one of the attacks with the most popular techniques for educational institutions; universities receive millions of phishing emails every year [6].

Spear-fishing is one of the methods in university networks, where it provides access to all valuable data, whether personal, financial system and all research networks used within the university.

Many people use recent social events to take advantage of people.

An example is the time of the COVID-19 pandemic [7] Also, the beginning of an academic year increases the possibility of phishing emails that offer various free opportunities on the Internet [8]

Where the interest of the students is great to get the first information about their future and they can enter the site or hack their system without realizing it.

Another attack that happened in educational institutions is the DDoS attack. DDoS attacks.

In 2016, 63 UK universities had suffered from DDoS Attacks[9,10] while in 2019 DDoS attacks continued to be on the rise, with a successful attack on the University of Edinburgh making headlines [11].

In 2021, there was a 102% increase in such attacks targeting universities, colleges and schools with a DDoS attack occurring every three seconds [11].

Another attack that threatens educational institutions is the ransomware attack against schools, colleges and universities. It is important that all educational institutions take the appropriate measures to protect themselves from these attacks, but also in cases where they happen to recover quickly from ransomware attacks, how to keep the various data in reserve, especially the most important ones for the university, as well as a strategy for the data circulating on the Internet in relation to the respective university[12]

In addition to external or internal persons who may be a risk for an institution, students themselves may pose a risk and may be an easy target of phishing attacks, many students want to change their grades, then the test Theirs for revenge, whether against the friend or the teacher. [13].

According to some research, cyber attacks are also investigated among students, in the educational context, students are special cases and have more access than other external personnel.

Due to the trust that is given to the student [to access the official website of the university as well as the applications used within the university, it is easier to carry out a cyber attack.[14].

Students should be guided to be in the interest of the institution to curb the desire to carry out an attack on the institution where it is registered [16].

Universities must maintain a balance in order to manage the threats that may be presented by the students themselves, recognizing the capacity they possess, and prioritizing the data that must be absolutely confidential[15].

4. Examples of cyber security in different universities

In South Africa, section 51(6)(g) of the Cybercrime and Cybersecurity Bill specifies some guidelines regarding the development and implementation of cyberspace analysis in Southern Africa, also includes training, education programs of development in relation to cyber security.

Awareness is conceptualized as consisting of knowledge, skills and actual behavior and attitudes of these elements.(16)

Another research related to cyber security was also done in Saudi Arabia.

The government of Saudi Arabia has proposed various cyber security frameworks based on all IT systems.

This research presents a Cyber Security Maturity Assessment Framework (SCMAF) for HEIs in Saudi Arabia. SCMAF is a platform that can serve all the people even in different institutions except for higher education, where it can serve as a web by taking the network that is offered on the Internet, providing the data. The development of digital infrastructure is a key objective of Saudi Arabia 2030.

During the data transfer there is the possibility of different attacks from different organizations, and the main goal is to avoid cyber attacks and the information remains safe[17]

Even in my country in educational institutions in Kosovo, cyber security is a growing problem. Curricula for educational systems include information and competencies of communication technology (ICT) and online services offered by these institutions. Schools face problems related to ICT. Many schools are not equipped with ICT equipment and many institutions have a limited number of teachers available for ICT-related knowledge.

Universities and higher education centers offer study programs in various fields related to cyber security, they also offer training for cyber security specialists. Regardless of these possibilities, TIK courses remain limited, and this is one of the reasons why students or staff cannot protect themselves from attacks that come to the systems in which they have accounts and have all their personal data. [31]

5. Cyber security challenges

Cyber security faces many challenges including data loss, privacy concerns, risk management in cyber development. Cyber security education is an important topic of attention for everyone, as it can cause a global shortage of cyber security experts. For example, the 2019 Cybersecurity Workforce Study [18] estimates that there is a shortage of 4.07 million cybersecurity experts. The status of the cyber security education system, which due to the lack of supply and demand cannot provide enough graduates to meet the needs of the industry [19] Developing a professional framework with good skills is the main goal of every educational institution. The NICE framework links theoretical concepts to real-world practice.

It defines job roles and related tasks, as well as the knowledge, skills and abilities (KSA) that are needed for specific roles to perform assigned tasks. The combined framework consists of three levels: Categories, Specialized Areas and Job Roles.[20] The category level groups work and workers to perform the function regardless of the professional title they possess. The categories contain groups of cyber work that are otherwise called specialized areas[20].

6. Cyber attacks

During the last years, with the great use of technology, a problem has been presented that affects our daily life: cybercrime. In educational institutions, this problem is more open due to the use of different types of networks and the equipment connected to those networks.

This problem is also affected by the educational and research activities carried out by the academic staff, academic assistants, students, as well as computer and research systems in various fields. The members of an educational institution can be the first victims of different types of attacks such as (social engineering, DDOS attacks, trojans, viruses, and worms), for this reason favorable variants must be found to avoid cybercrimes.

The first variant is the restriction of access to some parts of the educational institution or even to some parts of the official website of the university. The seriousness of this part is very important since cyber attacks can be destroyed, but after they happen and take the data of the institution, in this way the creation of security barriers can limit access for all the people of an institution. Members of the educational institution may be victims of cyber attacks and may not be able to exit or stop the attack while it is happening.

Cyber attacks also in higher education institutions target the personal data of the staff aiming to deceive the banking system or the system of other institutions where that person is registered.

The frequency of cyber attacks increases proportionally with the increase in the number of devices that can be connected to an institution's servers. [21] Phishing is a method of identity theft, the people who carry out these attacks, any information is valid to get what they want.

In institutions of higher education, when a phishing attack occurs, hackers or attackers send emails or messages to clients from various companies or institutions important to the university.

The text in the phishing e-mail varies from one phishing attack to another, displaying technical errors that must be selected by entering the data of the person to whom it is sent, continuing until the messages that promise certain profits that the attack requires. This type of attack is almost as old as the Internet itself. Cyber attackers also use social engineering to deceive users, infecting their computer with various viruses, obtaining personal data, and thus also obtaining bank information and money in the bank, as well as any work data, scientific or research they do on the Internet.

Ransomware attacks are another type of attack that occurs from malicious software that is designed to prevent access to a computer system until a certain amount is paid. Ransomware is another attack that can happen in higher education institutions, where data is exchanged with ransomware attackers [22].

DOS Denial of Service is the denial of DDOS service distribution. These are two of the most dangerous threats facing higher education institutions. DOS - Denial of Service is a cyber attack on an individual computer or on many computers that limits or prevents the legitimate user from accessing his personal resources. [23] In most educational institutions, there is a lack of staff with certain experience in cyber security, as well as a lack of material for the purchase of high-performance equipment, leading to the conclusion that it is impossible to monitor the equipment owned and the network activities that occur during the day. The people who are part of the IT teams are an important cause of the IT systems.

Part of the IT team must ensure that the equipment and old choices benefit from the benefits that any software that works all the time can have. [24] In educational institutions, many members of the academic staff and students do not have specific knowledge of cyber security, for this reason the use of technology also increases the attacks that can occur within the institution. To use technology without jeopardizing the security of an institution, we must develop and implement a defense strategy against digital attacks that occur. The development of cyber security culture can make an IT user verify the authenticity of the sender's mail requesting various personal information.[25]The achievement of a cultural plan of the cyber society is unknown. This can be done in four steps as follows: [26]

1. Acknowledgment of the film, which has a role in the realization of the culture plan of cyber Americans.
2. Measure the current level of cyber society culture of targeted audit at the academic level.
3. Designing a cultural plan of cyber societies in this institution.
4. Implementation of an updated cultural plan of cyber friends in the environment
5. Acquiring the most advanced, efficient programs against cyber attacks.[27, 28]

7. Structures Management Information System - SMIS

The management system used in universities serves students and academics, as well as staff working in the institution. Access to the system is granted through a unique username and password, which is given to each member of academic staff and registered student.

Each student has his own unique username and private password, which he uses to access his personal account within the Student Management Information System (SMIS).

SIEM (Security Information Event Management) Security Information and Event Management (SIEM) is a system that can analyze security events in real time, while providing long-term log storage, historical reporting and trend analysis.

These serve as alerts for events that may occur in the system, SIEM is able to provide information security.[27] Research, G. (2011). How to deploy SIEM technology. Technical report.

The use of the SIEM system is determined by the need to secure the information.

In this application, all important data or news, notifications that students should have, whether for lectures, exercises, schedule, personal academic progress, are available. There are different models of this system that are used by all institutions of higher education, they may have different differences between themselves such as in logo, name, design, operation, port, they all have the same role and types of data. which they possess are for the staff and students who are registered.

Care must be taken for students who complete their academic studies, access is prohibited, as they may misuse the information that a professor can display, or the data of other students. [27]

8. Evaluation of the use of the SMIS application

Regarding the SMIS application, the questionnaire conducted with the students provided valuable insights. Here is a summary of the findings:

- **Cyber Security Knowledge**: 68.2% of the students had prior knowledge about cyber security, understanding its importance in protecting data stored on digital devices, including educational institutions.
- **Awareness of the SMIS Application**: 27.5% of the students had prior knowledge of the SMIS application, with some hearing about it from their parents or siblings, while the others were unaware of it.
- **Data Misuse**: None of the students reported any instances of their data being misused within the university system.
- **Preferences for Online Program Usage**: 87.9% of the students preferred receiving information through the online application, appreciating the convenience of accessing it anytime and anywhere.

- **Application Usage Platforms**: 79.9% of the students confirmed having the opportunity to use the application across different platforms.
- **Purposes of SMIS Usage**: Students primarily used the SMIS application for registration (50.7%), checking grades (80.5%), receiving exam notifications (99.9%), accessing literature (63.1%), and checking personal data (48.5%).
- **Access Method**: Students predominantly accessed the application using a password (100%), with some also relying on email authentication (80.3%) and number authentication (23.6%).
- **Frequency of App Usage**: Students reported varying usage frequencies, with 49.9% using the app weekly, 22.7% using it monthly, and 28.3% using it daily.
- **Encountered Problems**: 67.2% of students reported encountering problems while using the application, while the remaining 33.8% had no issues or experienced problems with data retrieval.
- **Data Modification**: None of the students reported any changes or modifications to t
- **Ease of Use**: 75.5% of students found the university application easy to use, while 24.5% considered it normal in terms of usability.
- **Reliability of Information**: 43.3% of students found the application very reliable in providing accurate and up-to-date information about their academic progress, while 27.4% considered it reliable and 29.3% remained neutral.
- **Satisfaction with Features and Functionality**: 67.2% of the students were very satisfied with the features and functionality of the system, while 32.8% of the students were somewhat satisfied.
- **Application Support**: 60.3% of students considered the application's support team very responsible in dealing with technical issues and problem resolution, while 39.7% remained neutral.
- **Reporting Suspicious Activities**: 70.4% of students reported suspicious activities encountered while using the application, while 29.6% did not report such activities.

These findings provide insights into the students' awareness, usage, and satisfaction with the SMIS application, highlighting areas of success as well as potential areas for improvement.

9. Conclusions

Cyber security holds immense importance for educational institutions, particularly for students in today's digital age. It is the responsibility of educational institutions to ensure that students are well-informed and educated about data protection on the internet.

Through their academic programs, students can gain access to materials related to cyber security, helping them stay safe in the digital landscape. It is crucial for academic staff, regardless of their field of study, to possess knowledge about protecting personal data, securing materials posted in information management applications, and safeguarding student records. In the event of any type of hack or cyber-attack within an educational institution, staff members must be promptly notified. They should also receive timely alerts about potential attacks or viruses that may compromise their accounts.

Based on the questionnaires conducted with students, several conclusions can be drawn. Students pursuing distance learning are more actively engaged with the faculty's applications, staying informed about lectures, materials, training opportunities, and reviewing their personal data.

Many students had not used applications like SMIS before enrolling in the faculty, but they were able to access the SMIS application on various platforms and retrieve the necessary information. The majority of students expressed confidence and felt secure using the SMIS application, believing that their data would not be modified by unauthorized individuals, whether from outside or inside the faculty. Students also trusted the security measures in place to prevent unauthorized access to their accounts.

Students spend a significant amount of time using the SMIS application to receive notifications and download educational materials.

In conclusion, it is vital to educate students about the potential risks of account hacking, early warning signs of data theft, and the types of external attacks or viruses they may encounter. They should be informed about malicious websites and phishing emails to prevent unauthorized access to their computer systems.

Given the rapid development of various artificial intelligence devices, it is essential for everyone to stay informed and continuously learn about cyber security. By fostering a culture of cyber security awareness, educational institutions can help students navigate the digital landscape safely and protect their valuable data.

Referenca

[1]. Sebastian Karius, Mandy Kn¨ochel, Sascha Heße, Tim Reiprich"Machine Learning and Cyber Security" This is a manuscript of an article published by De Gruyter in the journal it - Information Technology on 04 September 2023.

[2]. Sara Ricci1, Jan Hajny1, Edmundas Piesarskas2 , Simon Parker3 , and Vladimir Janout1 "Challenges in Cyber Security Education" Supported by European Unions Horizon 2020 research and innovation program (grant No 830892 "SPARTA").

[3]. Amit Kumar Assistant Professor, Department of Computer Science & Engineering, Maulana Azad College of Engineering & Technology, Patna, Bihar, India "Cyber Security Issues and Challenges - A Review" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, May-June-2022.

[4]. Dr. Sushma Ran, Dr. Harish Mittu "Cyber-Security Behaviour: A Study of Higher Education Students", Elsevier-Cyber Security, Volume No. 127-(2023).

[5]. Redscan, The state of cyber security across UK universities: An analysis of Freedom of Information requests, Redscan Cyber Security Limited, London, 2020, [Online]. [Accessed 09 December 2023].

[6]. H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, Computers & security 105 (2021) 102248.

[7]. J. Chapman, How safe is your data? cyber-security in higher education, HEPI Policy Note 12 (DOE-SLC-6903-1) (2019) 1–6.

[8]. J. Chapman, A. Chinnaswamy, A. Garcia-Perez, The severity of cyber attacks on education and research institutions: A function of their security posture, in: 13th International Conference on Cyber Warfare and Security (ICCWS 2018), 08-09 March 2018, Washington DC, Academic Conferences International, Reading, 2018, pp. 111–119, [Online].

[9]. The Severity of Cyber Attacks on Education and Research Institutions: A Function of Their Security PostureChapman, John; Chinnaswamy, Anitha; Garcia-Perez, Alexeis. International Conference on Cyber Warfare and Security; Reading, (2018).

[10]. J. Chapman, How safe is your data? cyber-security in higher education, HEPI Policy Note 12 (DOE-SLC-6903-1) (2019) 1–6.

[11]. netscout, Ddos threat intelligence report: Unveiling the new threat landscape, https://www.netscout.com/threatreport/ddos-threat-intelligence-report/ accessed: 2023-05- 19 (2022).

[12]. NCSC, Further ransomware attacks on the uk education sector by cyber criminals. alert, version 2.2,

[13]. M. J. Maranga, M. Nelson, Emerging issues in cyber security for institutions of higher education, International Journal of Computer Science and Network 8 (4) (2023) 371–379.

[14]. Cybersecurity, I. S. Agency, Insider threat mitigation guide, Security Week, [Online]. [Accessed 28 October 2023] (11 2020).

[15]. Harjinder Singh Lallie, Andrew Thompson , Elzbieta Titis, Paul Stephens," Understanding Cyber Threats Against the Universities, Colleges, and Schools" , Article · July 2023 https://www.researchgate.net/publication/372655992_Understanding_Cyber_Threats_Against_the_Universities_Colleges_and_Schools

[16]. (ISC)2 : cyber security workforce study 2019: Strategies for Building and Growing Strong cyber security Teams (2023)

[17]. ECSO: Gaps in European Cyber Education and Professional Training (2023).

[18]. Sara Ricci1[, Jan Hajny1, Edmundas Piesarskas2 , Simon Parker3, and Vladimir Janout, " Challenges in Cyber Security Education", Supported by European Unions Horizon 2020 research and innovation program, (grant No 830892 "SPARTA").

[19]. TIRZIU, Andreea–Maria, 2023: Protection and security of information at the level of national public authorities from Romania.

[20]. Cert-Ro, 2023. Report on the evolution of threats in 2017

[21]. GUNES KARABULUT, Kurt; BUYUKCORAK, Saliha; CEPHELI, Özge, 2023. Hybrid Intrusion Detection System for DDOS Attacks

[22]. LOBBAN, Iain, 2023. 10 Steps to Cyber Security.

[23]. B. Fisher & J. Sloan (Eds.), 2023. Campus crime: Legal, social and policy perspectives. Springfield, IL: Charles C. Thomas.

[24]. The European Union Agency for Network and Information Security (ENISA), 2023. Cyber Security Culture in Organisations

[25]. Alin - Ciprian COJOCARIU, Ion VERZEA, Rachid CHAIB, "ASPECTS OF CYBER SECURITY IN HIGHER EDUCATION INSTITUTIONS", Chapter · May 2020 . DOI: 10.1007/978-3-030-44711-3_1 https://www.researchgate.net/publication/341750996_Aspects_of_Cyber-Security_in_Higher_Education_Institutions

[26]. Jarot S. Suroso and Caesario Putra Prastya, "Cyber Security System With SIEM And Honeypot In Higher Education", Conf. Ser.: Mater. Sci. Eng. 874 012008, 2020.

[27]. Rajesh Chandarman[I]; Brett van Niekerk[II]" Students' cybersecurity awareness at a private tertiary educational institution" , SciELO.org publisher.

[28]. Iman Almomani1,2, Mohanned Ahmed1, Leandros Maglaras3" Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia" September 9, 2021,publisher -PeerJ Computer Science.

[29]. https://qkss.org/en/publikimet/kosovos-take-on-cybersecurity Consulted: 21/08/2023