 doi:10.20944/preprints202211.0128.v1

Cyber security threats to educational institutes: a growing concern for the new era of cybersecurity

Syed Adnan Jawaid

University: Washington University of Science and Technology

Email: adnan.jawaid@hotmail.com

Abstract:

Background: The outbreak of the Covid-19 pandemic has significantly affected the operations of higher education institutions. Due to the limited use of video conferencing and cloud computing in these facilities, distance learning became the only option available to them.

Objective: The study focused on identifying the most common types of attacks that can affect e-learning assets.

Results: There was a lack of clear cybersecurity policies for educational institutes and universities in 2020, according to a report by Microsoft Security Intelligence. The report showed that the education industry was the most targeted sector for malware attacks in the last 30 days.

Conclusion: The recommendations for improving the security of e-learning systems. Some of these include implementing policies that restrict access to the resources and applications, updating security patches, and using cryptographic protocols.

Keywords: Cyber security threats, Cyber security threats to educational institutes, growing concern for the new era of cybersecurity, new era of cybersecurity

 doi:10.20944/preprints202211.0128.v1

1. INTRODUCTION

The following paper has been dealing with the issues that have been faced by people during the COVID-19 outbreak mainly due to the factor of data breaching. The outbreak of the Covid-19 pandemic has significantly affected the operations of higher education institutions. Due to the limited use of video conferencing and cloud computing in these facilities, distance learning became the only option available to them [1].

Due to the rise of distributed denial of service (DDoS) attacks and the increasing number of attacks on e-learning platforms, the risk of unauthorized access to the data has increased significantly. This study aimed to identify the various types of attacks that can affect the assets of e-learning institutions. It also made recommendations for improving the security of these platforms [2].

In 2020, it was reported that over half of Higher Education Institutions were affected by cyberattacks. The data stolen from these institutions included the personal information of their employees and students. Cybercriminals can also access these resources through various online learning platforms. The primary goal of these attackers is to obtain the login credentials of their victims so they can use them to perform spam or phishing attacks. In the case of Covid 19, which led to the mandatory social distancing in higher education institutions, many of these activities had to be carried out remotely in order to comply with international health commissions' regulations [3].

2. REASONS FOR TECHNOLOGICAL USE IN EDUCATION

A survey conducted by Pearson Education revealed that over 90% of respondents believe that online learning will continue to be a vital part of the education field following the end of the Covid-19 pandemic. To minimize the risk of attacks, it is important that the various technologies used by universities are secure. One of the most common tools that universities can use to manage their online

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 November 2022 doi:10.20944/preprints202211.0128.v1

learning is the cloud computing. This type of system allows them to store and organize their data, as well as organize online classes [4].

During the pandemic, the cloud became the primary service that was used to store and access academic materials. It also allowed students to improve their academic performance and develop new skills without the need for them to be physically present in the institution. The use of simulation environments and virtual laboratories has allowed students to create new skills without the need for them to be physically present in the institution [5].

3. TECHNOLOGY THAT IS EFFECTED BY CYBER ATTACK

The use of the cloud computing system by universities has allowed them to improve the efficiency and academic performance of their students. They can also manage their various operations through a variety of cloud service models. One of these is the Infrastructure as a Service, which allows universities to run their software on a virtual infrastructure [6].

One of the most common types of cloud services that universities can use is the Platform as a Service (PaaS), which allows them to develop and manage applications through a variety of programming languages. This type of system can be very beneficial for students who are studying information technology. Another type of cloud service is Software as a Service, which allows educational institutions to use various applications on a cloud platform [7].

Due to the increasing popularity of online learning, many universities have started using a hybrid method of teaching, which involved both offline hours and online courses. However, the risk of a new Covid-19 wave still persists, and this is why it is important that the security of this method is maintained [8].

 doi:10.20944/preprints202211.0128.v1

The first section of this article talks about the various technologies that are used in online education. These are based on the scientific articles published in different journals. The second section of this article talks about the various security risks that are associated with the use of online education. This is done through the analysis of the scientific literature and the multiple security reports that are delivered by companies such as IBM, Microsoft, and ENISA. The last section of this article is dedicated to discussions about the impact of these security breaches on the operations of online education institutions [9].

 doi:10.20944/preprints202211.0128.v1

4. CRITICAL ANALYSIS

This article aims to provide a comprehensive overview of the various aspects of the cyber security issue that affects people who work from home. It also explores how the security of a remote working system has changed over the years. Despite the numerous security breaches that have occurred, the security of a remote working system is still not strong enough to protect itself [10].

In order to prevent unauthorized access to the audio and video calls made from a company's servers, it is recommended that they use end-to-end encryption. Although E2E is commonly used in applications, it is only used to protect documents and correspondence. For instance, the ZOOM application uses a combination of UDP and TCP connections to encrypt its communications [11].

The article also provides an overview of the various issues that companies face due to the security breaches that have occurred. After reading the article, one will be able to resolve these issues and its findings are reliable. E2E encryption is not widely used in video conferencing due to the complexity of the technology involved. According to Matthew Green, a computer science professor at Johns Hopkins University, group video conferencing is not ideal for using end-to-end encryption [12]

5. ADVANTAGES OF TECHNOLOGY

One of the main advantages of cloud computing is its ability to provide a variety of educational services, such as simulations and virtual laboratories. These tools allow students to develop their skills without the need for physical presence in the institution. The adoption of this technology in higher education has also increased the efficiency of the institutions [13].

In terms of communication, the use of virtual learning tools such as Zoom, GoToWebinar, and Cisco WebEx was the main source of this type of communication. There are also various other applications that are used in this area, such as Microsoft Teams, Adobe Connect, and Livestorm. According to a

 doi:10.20944/preprints202211.0128.v1

report released by Datanyze, the world's leading provider of technography, the three most used VCA tools in 2020 were Zoom, GoToWebinar, and Cisco Webex [14].

This process was carried out through the review of various publications that were published in various digital libraries, such as ScienceDirect, Springerlink, and IEEE Xplore. The analysis of the security reports that were delivered by companies that specialize in providing cyber security solutions was also carried out [15].

According to a report by ENISA, in 2020, the educational field was targeted by cyberespionage groups due to the interest in the COVID-19 research results. Another report by Kaspersky revealed that the number of attacks on educational institutions has increased significantly due to the increasing number of distance learning courses [16].

6. STEPS TO REDUCE THE CYBER ATTACKS

The review provides an overview of the extent to which the complexity of systems and software will only get worse as the number of tools and resources used to manage them continues to increase. This is why it is critical that IT leaders understand the need to continuously improve their capabilities. Unfortunately, many educational institutes lack the resources and bandwidth to properly prepare for a cyber security incident [17].

One of the most important factors that educational institutes should consider when it comes to protecting their data and devices from attacks is having a comprehensive strategy that includes both procedural and technical measures. This can be done through the use of multi-factor authentication or two-factor authentication. To ensure that students follow the school's internet safety policies, it is also important that they turn on notifications when there are signs of suspicious activity [18].

 doi:10.20944/preprints202211.0128.v1

One of the most important factors that educational institutes should consider when it comes to protecting their data and devices from attacks is having a comprehensive strategy that includes both procedural and technical measures. According to Soto, it's also important that students and faculty members are aware of the risks associated with using online platforms. He strongly advises them to create an acceptable use policy that clearly states what is and is not allowed in order to make their students and faculty members more aware of the guidelines [19].

Without the proper resources to properly manage their systems and software, many educational institutes turn to third-party vendors to provide them with the necessary support and resources to improve their remote learning experience. However, it's important to note that these vendors are not always created equal [20].

7. RESULTS

The results of this survey suggest that data breaches in education are a concern, as they can involve the sensitive and private information of students and teachers. Educational institutes are typically targeted due to the amount of data they have on their systems. A denial-of-service attack occurs when a network or server resource gets flooded with requests [21].

Many educational institutes lack the necessary security measures to protect themselves from unauthorized access to their networks. This is because many of them do not use the same level of protection when it comes to protecting their data. Turning off the data logging feature on school servers can allow attackers to access their networks without a trace [22].

The term phishing refers to an email that appears to be from a legitimate organization or person. It then asks for sensitive information, such as credit card numbers or personal information. Most of the time, these types of emails are accompanied by ransomware, which is a type of malware that can extort from

 doi:10.20944/preprints202211.0128.v1

a victim. Educational institutes are especially vulnerable to these types of threats due to how kids are less likely to be aware of the harmful effects of these types of links and emails [23].

Unpatched and outdated hardware and software can allow attackers to access educational institutes' networks and systems. This is because they are more vulnerable to these types of threats due to how they lack the necessary resources and manpower to properly patch and update their systems. Although updating and patching systems is the most common attack prevention method, educational institutes often lack the necessary resources and staff to properly address these issues [24].

Cyberbullying is a type of behavior that occurs online, and it can cross the line into criminal and unlawful conduct. According to the Cyberbullying research center, around 37% of students have experienced this type of bullying [25].

Inappropriate content can also be easily accessed by students through their devices if the policies or content filtering are not enforced properly. Online predators are more likely to target students due to the increasing number of students learning remotely. They can use their online platforms to build trust and manipulate their victims [26].

8. **DISCUSSION**

The research article covers every aspect of the cyber security issue due to remote working. For cybercriminals, educational institutes are an ideal target due to the amount of personal information they collect and the large budgets they have available. These organizations typically have little or no security measures in place. In February 2021, a cyber-attack occurred at Simon Fraser University, which is a university in British Columbia. It affected about 200,000 individuals. The attackers were able to access the university's server and collect various sensitive data, such as student and staff IDs [27].

 doi:10.20944/preprints202211.0128.v1

Last year, about 250,000 individuals who worked at the same university were affected by a similar data breach. In 2020, it was revealed that hackers were able to steal the personal information of over 300,000 teachers in Quebec. Despite the arrests of the attackers, many cases of identity theft were still reported [28].

Across the Atlantic, the number of universities that reported a data breach remained the same. In 2020, a report revealed that almost half of UK universities had experienced a security issue. Despite the country's post-secondary institutions having over 2.3 million students, a report revealed that only 46% of staff members had received security training in the 12 months prior to the publication of the report. Then, a case like the Blackbaud ransomware attack, which was first reported in the summer of that year, became an example of how international organizations can be affected by a data breach [29].

Several universities in Canada, the U.S., and the UK were affected by the attack. Blackbaud confirmed that it paid the ransom to cyber criminals. The company also said that the ransom included the stolen data, such as student and staff IDs, phone numbers, and donation histories [30].

The number of attacks that occurred during the year highlighted the need for educational institutes to improve their data protection measures. Aside from regular training sessions, employees should also regularly be informed about the latest security threats. These threats include ransomware, phishing attacks, and malware [31].

Phishing attacks are usually carried out by cyber criminals in order to trick teachers into giving up their personal information, such as their tax and identity information. Having a good understanding of the signs of these attacks is very important to prevent them from happening in the first place. To improve the security of educational institutes, employees, and students, organizations should have the necessary resources and training [32].

 doi:10.20944/preprints202211.0128.v1

One of the most important steps that educational institutes can take to improve their security is regularly updating their software. Doing so will prevent unauthorized access to their systems. Another important step that they can take is to install anti-virus and anti-malware software. These two tools can help prevent the spread of malware and other harmful software on their devices. Various forms of training are also available for faculty and staff members to improve their skills in identifying and preventing cyber-attacks. These include training sessions on phishing and social engineering [33].

Despite the various advantages that educational institutions provide, they are still vulnerable to cyber-attacks. Due to the global pandemic, hackers have the opportunity to develop new and harmful software. This is why it is important that educational institutes regularly update their security software. One of the most important steps that educational institutes can take to improve their security is regularly training their employees on the latest techniques and procedures that cyber criminals use to attack their systems. This training will help them identify the best ways to protect their data [34].

9. CONCLUSION

This article aimed to discuss the security concerns faced by educational industry. The article also presented a literature study that describes the various attacks that occurred. One of the most important factors that a video conference should consider when it comes to security is the protection of its users' personal data. This can be done through the theft of email, the transmission of data, and the control over the devices used by the participants. There are three main areas that can be considered when it comes to conference security: pre-call policies, access rules, and security.

Due to the increasing popularity of remote video conferencing, security threats related to this technology have been identified. In order to prevent these types of breaches, it is important that the users take the necessary steps to safeguard their data. Due to the nature of remote activities, cyber security has been a challenge for organizations. This is why it is important that they take the necessary

 doi:10.20944/preprints202211.0128.v1

steps to identify and prevent threats and activities that are carried out in their facilities. Besides this, the increasing number of students and faculty members using online platforms has also increased the financial losses that the education industry has experienced.

10. RECCOMENDATION

Due to the increasing number of people using online platforms, it has been observed that the migration of data to the cloud has increased the challenge of information security. This is why it is important that the organizations take the necessary steps to update their systems and applications. Besides this, it is also important that they implement effective patch management and automation processes [35]. One of the most important factors that an organization should consider when it comes to protecting its data is having policies that restrict the access to its applications and stored data. This can be done through the creation of a restricted access policy. Another important step that an organization should take is to implement secure protocols. This can help prevent unauthorized access to the corporate network. The implementation of the Covid-19 regulations has increased the importance of protecting the various assets of higher education institutions [36].

 doi:10.20944/preprints202211.0128.v1

11. Bibliography

(1)

Arina, A.; Anatolie, A. *Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning*; 2021.

(2)

Stone, M. Cyber Security Threats to Schools & How to Prevent Them https://www.verizon.com/business/en-nl/resources/articles/s/cyber-security-threats-to-schools-and-how-to-prevent-them/.

(3)

Singar, A. V.; Akhilesh, K. B. Role of Cyber-Security in Higher Education. *Smart Technologies* 2019, 249–264. https://doi.org/10.1007/978-981-13-7139-4_19.

(4)

Leenen, D. L. *ICCWS 2018 13th International Conference on Cyber Warfare and Security*; Academic Conferences and publishing limited, 2018.

(5)

Chapman, J. *How Safe Is Your Data? Cyber-Security in Higher Education*; 2019.

(6)

Verma, P.; Dumka, A. Perspectives of Blockchain in the Education Sector Pertaining to the Student's Records. *Advances in Information Communication Technology and Computing* 2020, *135*, 419–425. https://doi.org/10.1007/978-981-15-5421-6_42.

(7)

Magomedov, I.; Murzaev, H.; Zolkin, A. The European Proceedings of Social and Behavioural Sciences EpSBS ICEST 2020 International Conference on Economic and Social Trends for Sustainability of Modern Society CYBER LITERACY as ONE of the MAIN DISCIPLINE NECESSARY in MODERN TIME. *The European Proceedings of Social and Behavioural Sciences* 2020. https://doi.org/10.15405/epsbs.2020.10.03.117.

(8)

Kulkarni, D.; Al, E. Leveraging Blockchain Technology in the Education Sector. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 2021, *12* (10), 4578–4583. https://doi.org/10.17762/turcomat.v12i10.5202.

(9)

Ajmi, L.; Hadeel; Alqahtani, N.; Ur Rahman, A.; Mahmud, M. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* 2019, *21*. https://doi.org/10.1109/cais.2019.8769470.

(10)

Venter, I. M.; Blignaut, R. J.; Renaud, K.; Venter, M. A. Cyber Security Education Is as Essential as "the Three R's." *Heliyon* 2019, *5* (12), e02855. https://doi.org/10.1016/j.heliyon.2019.e02855.

(11)

Huang, X.; Li, Z.; Ding, D.-W. Finite-Time Attack Detection for Nonlinear Complex Cyber-Physical Networks under False Data Injection Attacks. *Journal of the Franklin Institute* 2022. https://doi.org/10.1016/j.jfranklin.2022.07.050.

(12)

Fu, Y.; O'Neill, Z.; Yang, Z.; Adetola, V.; Wen, J.; Ren, L.; Wagner, T.; Zhu, Q.; Wu, T. Modeling and Evaluation of Cyber-Attacks on Grid-Interactive Efficient Buildings. *Applied Energy* 2021, *303*, 117639. https://doi.org/10.1016/j.apenergy.2021.117639.

(13)

Yu, Y.; Liang, Y. Secure Multitarget Tracking over Decentralized Sensor Networks with Malicious Cyber Attacks. *Digital Signal Processing* 2021, 103132. https://doi.org/10.1016/j.dsp.2021.103132.

(14)

Sengan, S.; V, S.; V, I.; Velayutham, P.; Ravi, L. Detection of False Data Cyber-Attacks for the Assessment of Security in Smart Grid Using Deep Learning. *Computers & Electrical Engineering* 2021, *93*, 107211. https://doi.org/10.1016/j.compeleceng.2021.107211.

(15)

Li, L.; Wang, W.; Ma, Q.; Pan, K.; Liu, X.; Lin, L.; Li, J. Cyber Attack Estimation and Detection for Cyber-Physical Power Systems. *Applied Mathematics and Computation* 2021, *400*, 126056. https://doi.org/10.1016/j.amc.2021.126056.

(16)

Zhao, J.; Liu, X.; Yan, Q.; Li, B.; Shao, M.; Peng, H.; Sun, L. Automatically Predicting Cyber Attack Preference with Attributed Heterogeneous Attention Networks and Transductive Learning. *Computers & Security* 2021, *102*, 102152. https://doi.org/10.1016/j.cose.2020.102152.

(17)

Stacey, P.; Taylor, R.; Olowosule, O.; Spanaki, K. Emotional Reactions and Coping Responses of Employees to a Cyber-Attack: A Case Study. *International Journal of Information Management* 2021, *58*, 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298.

(18)

Chaturvedi, M.; Sharma, S.; Ahmed, G. Study of Baseline Cyber Security for Various Application Domains. *IOP Conference Series: Materials Science and Engineering* 2021, *1099* (1), 012051. https://doi.org/10.1088/1757-899x/1099/1/012051.

(19)

Crick, T.; Davenport, J. H.; Irons, A.; Prickett, T. A UK Case Study on Cybersecurity Education and Accreditation https://ieeexplore.ieee.org/abstract/document/9028407?casa_token=PhunqBgwCGEAAAAA:rVtrd3DxyasWdAbc44mPcIoVjCKIY9Ai1gU-9qP35f-V8E7V47uQGQZmNuIZYFoQs2tClnlY. https://doi.org/10.1109/FIE43999.2019.9028407.

(20)

Liu, N.; Nikitas, A.; Parkinson, S. Exploring Expert Perceptions about the Cyber Security and Privacy of Connected and Autonomous Vehicles: A Thematic Analysis Approach. *Transportation Research Part F: Traffic Psychology and Behaviour* 2020, *75*, 66–86. https://doi.org/10.1016/j.trf.2020.09.019.

(21)

Bada, M.; Nurse, J. R. C. Chapter 4 - The social and psychological impact of cyberattacks https://www.sciencedirect.com/science/article/pii/B9780128162033000046.

(22)

Muthuppalaniappan, M.; Stevenson, K. Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care* 2020, *33* (1). https://doi.org/10.1093/intqhc/mzaa117.

(23)

Pranggono, B.; Arabo, A. COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters* 2020, *4* (2). https://doi.org/10.1002/itl2.247.

(24)

Bada, M.; Nurse, J. R. C. Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs). *Information and Computer Security* 2019, *27* (3), 393–410. https://doi.org/10.1108/ics-07-2018-0080.

(25)

Catota, F. E.; Morgan, M. G.; Sicker, D. C. Cybersecurity Education in a Developing Nation: The Ecuadorian Environment. *Journal of Cybersecurity* 2019, *5* (1). https://doi.org/10.1093/cybsec/tyz001.

(26)

Tvaronavičienė, M.; Plėta, T.; Casa, S. D.; Latvys, J. Cyber Security Management of Critical Energy Infrastructure in National Cybersecurity Strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development* 2020, *2* (4), 802–813. https://doi.org/10.9770/ird.2020.2.4(6).

(27)

Deborah Oyedotun, T. Sudden Change of Pedagogy in Education Driven by COVID-19: Perspectives and Evaluation from a Developing Country. *Research in Globalization* 2020, *2*, 100029. https://doi.org/10.1016/j.resglo.2020.100029.

(28)

Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H. N. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems* 2020, *62* (1), 1–16. https://doi.org/10.1080/08874417.2020.1712269.

(29)

Zeadally, S.; Adi, E.; Baig, Z.; Khan, I. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access* 2020, *8*, 1–1. https://doi.org/10.1109/access.2020.2968045.

(30)

Hart, S.; Margheri, A.; Paci, F.; Sassone, V. Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers & Security* 2020, 101827. https://doi.org/10.1016/j.cose.2020.101827.

(31)

Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from Home during COVID-19 Crisis: A Cyber Security Culture Assessment Survey. *Security Journal* 2021, *35*. https://doi.org/10.1057/s41284-021-00286-2.

(32)

Lallie, H. S.; Shepherd, L. A.; Nurse, J. R. C.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-

Attacks during the Pandemic. *Computers & Security* 2021, *105*, 1–20. https://doi.org/10.1016/j.cose.2021.102248.

(33)

Ricci, J.; Breitinger, F.; Baggili, I. Survey Results on Adults and Cybersecurity Education. *Education and Information Technologies* 2018, *24* (1), 231–249. https://doi.org/10.1007/s10639-018-9765-8.

(34)

Newman, C.; Edwards, D.; Martek, I.; Lai, J.; Thwala, W. D.; Rillie, I. Industry 4.0 Deployment in the Construction Industry: A Bibliometric Literature Review and UK-Based Case Study. *Smart and Sustainable Built Environment* 2020, *ahead-of-print* (ahead-of-print). https://doi.org/10.1108/sasbe-02-2020-0016.

(35)

Herath, T.; Herath, H. S. B. Coping with the New Normal Imposed by the COVID-19 Pandemic: Lessons for Technology Management and Governance. *Information Systems Management* 2020, *37* (4), 277–283. https://doi.org/10.1080/10580530.2020.1818902.

(36)

Crumpler, W.; Lewis, J. *The Cybersecurity Workforce Gap*; 2019.