Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning

Article *in* International Journal of Scientific & Technology Research · March 2021

CITATIONS
16

READS
4,098

2 authors:

Arina Alexei
Technical University of Moldova
11 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Anatolie Alexei
Technical University of Moldova
23 PUBLICATIONS **24** CITATIONS
SEE PROFILE

Cyber security threat analysis in higher education institutions as a result of distance learning

Alexei Arina, Alexei Anatolie

Abstract— The Covid-19 pandemic had a major impact on the organization of studies in higher education institutions (HEIs). Distance learning was the only possibility to continue the educational process, since March 2020. Cloud computing, online learning platforms and video conferencing applications, whose use was quite limited in HEIs, in the conditions of the pandemic with Covid-19, have become the main assets for conducting online studies. Thus, the risk of DoS / DDoS attacks, cross-site scripting, spoofing, unauthorized data access and infection with malicious programs, but also the theft of personal data has increased dramatically. The research was based on identifying the classes of attacks with major impact, on the assets, but also making recommendations for increasing cyber security in e-learning conditions. Common recommendations include updating systems and managing security patches, implementing access policies at the application or resource level, classifying information, and using cryptographic protocols.

Index Terms— cloud computing, cyber security threats, HEIs, LMS platform, technology, video conference application, vulnerabilities.

1 INTRODUCTION

WITH the increasing use of modern technologies globally, the need to ensure cyber security has grown more and more in the last 20 years. But truly revolutionary, this need became in 2020 with the Covid-19 pandemic. The current reality is hyper-connected and complex, using several technologies, whose impact, on cybersecurity cannot be estimated yet.

Cyber security can be defined as protecting users from the risks associated with the use of modern communication technologies.

According to research by the Ponemon Institute [1], which conducts cybersecurity research, in 2020, the losses are on average of $ 3.86 million for a global data breach, the most affected were the field of health ($ 7.1 million) and the most affected country is the United States ($ 8.64 million). The impact of remote work caused by the Covid-19 pandemic increases the average cost of a data breach by $ 137,000 as a result of remote work. Thus, the average loss for a data breach is about $ 4 million.

Analyzing the data from the same research [1], it can be stated that in the field of education the losses related to a data breach were $3.90M, in 2020. A rather high level compared to research field, for example, where the losses related to a data breaches in 2020 were $1.53M.

Higher Education Institutions (HEIs) are increasingly affected by cyber-attacks, and the data reported in 2020 are completely appalling. Cyber criminals are interested in stealing personal data of students and employees, as well as taking control of devices and resources, access is possible through the use of various technologies of remote access and online learning platforms. The main purpose is not to gain access to the personal account, but to use personal credentials to attempt new phishing or spam attacks, but also for subsequent attempts to steal money.

With the spring of 2020, the field of education was even more affected, because the offline study was suspended due to the pandemic with Covid-19, and a new reality had to be implemented. Online study has become the main way of conducting studies in schools and universities.

The field was not prepared for such a challenge, several problems arose, which included: the use of technologies whose vulnerabilities have not yet been studied or discovered, untrained teachers for online courses and students who did not have the necessary devices (for example laptops) or fast internet connection to video streaming media. There were no clear cybersecurity policies, for online activities, in institutions that protect assets, employees and students.

Thus, in June 2020, Microsoft Security Intelligence [2] reported that the education industry accounted for 61 percent of the 7.7 million malwares encountered by businesses in the last 30 days - more than any other sector. Countries with the highest infection rate are reflected in table 1 [3].

Table 1. Countries with the highest infection rate

Country	Infection/users
Russia	59 infection/1000 users
Germany	39 infection attempts/1000 users
Austria	27 infection attempts/1000 users

After most higher education institutions have adopted the online method of teaching, or at best, the hybrid method which involved offline hours for types of activities with low attendance and online courses for tens or hundreds of students, and the risk of a new Covid-19 wave persist, the need to ensure cyber security for the new reality is very important.

The key technologies used in online education activities, have been identified in the first section of this article, based on several scientific articles, recently published in: International Journal in IT & Engineering, International Journal of Scientific & Technology Research, International Journal of Advanced Computer Science and Applications, Procedia Economics and Finance.

The second section identified the security risks of key assets, based on the scientific literature studied and in-depth study of security reports, delivered by companies specializing in cybersecurity, such as IBM, Ponemon Institute, Microsoft

Arina Alexei is currently pursuing a doctoral program in Telecommunications Systems, Networks and Devices at the Technical University of Moldova. E-mail: arina.alexei@tse.utm.md

Security Intelligence, ENISA, Datanyze, Kaspersky.
And the last section was reserved for recommendations and discussions, to reduce the impact of security breaches related to online study in HEIs.

2 Technologies

In the conditions of the pandemic with Covid 19, when social distance became mandatory, a large part of the activities carried out in HEIs, had to be carried out remotely, in order to comply with the legal provisions issued by health commissions around the world. Thus, distance learning became the only possibility that ensured the continuity of the educational process.

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.

In this situation it is necessary to identify technologies that allow remote study and work, threats technologies and solutions to secure them.

2.1 Cloud Computing

Cloud Computing (CC) [4] has many benefits for HEIs, from storing data and organizing online classes, to migrating university network infrastructure, or using the resources provided by the cloud. Under the conditions of the pandemic, the cloud became the basic service for accessing resources and storing information in academic environment. Also, CC services directly contributed to ensuring the quality of education, when online study was the only possibility. The use of virtual laboratories and simulation environments have allowed the creation of skills, which no longer depend on the physical presence of students in institutions. The adoption of CC into higher education promotes a good students' academic level and efficiency [5]. Within the HEIs, CC services were widely implemented until 2020. Universities typically use the following cloud service models [6]:

1) Infrastructure as a Service (IaaS) offers virtual infrastructure to implement and run the software, including applications and operating systems [7]. Especially important for students studying information technology;

2) Platform as a Service (PaaS): this model of cloud services supports the development of applications through programming languages, services and tools offered by cloud platform providers. For example, an instructor may design a virtual customized laboratory for students using a PaaS [7];

3) Software as a Service (SaaS) allows the use of applications by educational institutions through a cloud platform via the Internet. SaaS benefits are that it eliminates licensing costs, installation and software maintenance [7].

2.2 Learning Management Systems (LMSs)

LMSs were implemented until the pandemic, but during this period, were fully exploited. Complex courses were created, which had several types of activities, such as seminars, lessons, glossaries, practical tasks, assessment tests. According to the LMS Market report [8], in European HEIs, LMSs leaders are: Moodle (65%), Blackboard (12%), Ilias (4%) and Sakai (3%).

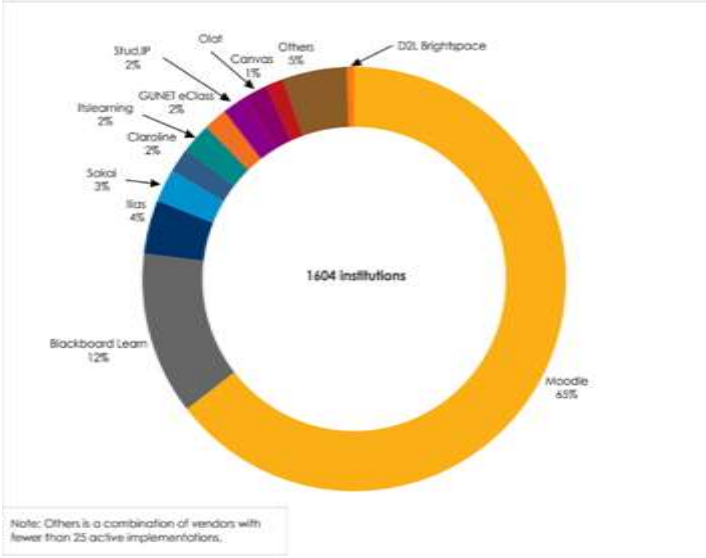

Fig.1 LMSs Distribution Percentage of European HEIs [8]

Analyzing the data provided by Google Trend, for the period 2019-2020, there is a massive increase of interest in various LMS platforms, both in Europe and globally. It is also attested that Moodle is the most popular LMS.

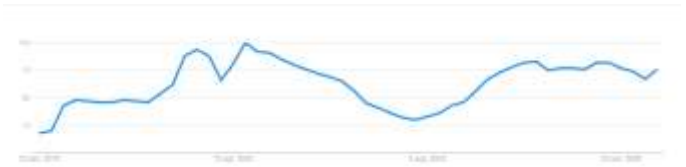

Fig.2 Global interest level for Moodle 2019-2020 (by Google Trend)

2.3 Video conferencing applications (VCA)

VCA in these conditions, was the main source of communication. In this regard there are several applications, such as Zoom, GoToWebinar, Cisco WebEx, Livestorm, ON24, Adobe Connect, Microsoft Teams. Application concept is the same, different technologies used. According to the report submitted by the company Datanyze [9], the world leader in technography, top three VCA used in 2020, globally: Zoom, GoToWebinar and Cisco Webex.

Table 2. Use of VCs globally

Ranking	Technology	Domains	Market Share
1	Zoom	30583	36,15%
2	GoToWebinar	18486	21,85%
3	Cisco Webex	14628	17,29%

The same video conferencing applications are leaders in Europe, according to the report [9], in the following countries: Germany, Bulgaria, Italy, the Netherlands, Sweden and Switzerland.

3 Research methodology

The research process includes reviewing various publications in top digital libraries, such as IEEE Xplore, ScienceDirect and SpringerLink published between 2011 and 2020 but also detailed analysis of various security reports for 2019-2020 years, made by companies specializing in cyber security solutions.

Threat analysis in HEIs is a very important research area, according to the report submitted by ENISA [10], in 2020, educational field has been targeted by cyberespionage campaigns due to interest in COVID-19 research results. An additional confirmation is the data reported by Kaspersky [3], which reports an increase in DoS / DDoS attacks by 350%, compared to 2019, attacks targeting educational resources, much of the increase is due to distance learning services.

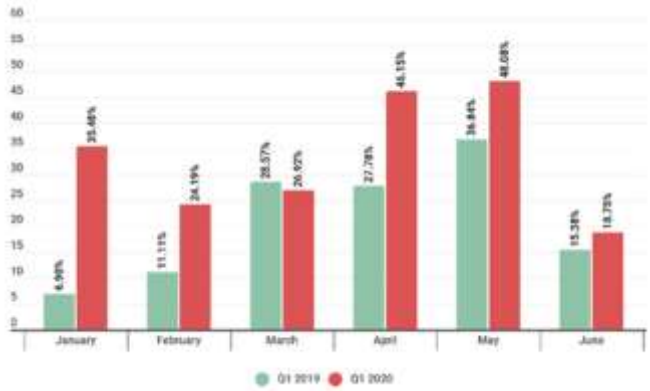

Fig. 3 Percent of the total number of DDoS attacks that affected educational resources: Q1 2019 vs Q1 2020 [3]

Analyzing the figure above, the monthly growth rate of DDoS attacks in 2020 vs 2019 can be calculated, it was reflected in figure 3.

Percent increase when compared to 2019	January: 550%	February: 500%	March: 350%	April: 480%	May: 357.14%	June: 450%

Fig.4 The percent growth in the number of attacks on educational resources when compared to the same month of the previous year

3.1 Security Threats of CC services

The main security threats of CC can be classified into 5 categories [11], [12]:

1) *Shared Technologies Vulnerabilities* - because of scalable infrastructure used by cloud service providers. All layers of shared technology can be attacked to gain unauthorized access to data, like: CPU, RAM, hypervisors, applications, etc. Navati et al. demonstrate [13], that if attackers could exploit vulnerabilities in the hypervisor then they gain access to the physical host where other neighboring virtual machines (VM) reside.
2) *Data Breach* - users' data can suffer both from accidental data loss and from malicious intrusive actions. A form of such attack is when a virtual machine can use a shared component like processor's cache to access the data of another virtual machine running on the same physical host.
3) *Account or Service Traffic Hijacking* - a user can lose control over its own account. Occurs as an effect of using one-step authentication, for example, password-based authentication.
4) *Denial of Service (DoS)* – it is a common attack in cloud environment, attackers just need to use all CPU, RAM, disc space and network bandwidth, to make service unavailable. A great disadvantage of cloud services in case of DoS attack is that in case of resource request, the cloud environment will increase the number of allocated resources. This means that on the one hand the cloud system counters the effects of the attack, but on the other hand it supports the attacker in his evil activity, by providing him with more resources [14].
5) *Malicious Insiders* - can be both the staff members and employees of the company providing cloud services. They could obtain sensitive information, which traditionally would not have access**.**

The human factor has a big impact on cloud services. Security threats can come from [15]:

1) *External users*, can launch many attacks against the cloud infrastructure through the network. They can affect data confidentiality; integrity and the availability of the CP's data centers.

2) *Internal users* - a major risk of using CC is multitenancy, as a user's private data can be accessed and viewed by unauthorized persons sharing the same resources. These risks are present for both PaaS and SaaS models CC [16].

3) *The Cloud Provider* itself might be an attacker. Employees

could exploit their privileged position to steal sensitive users' information through either physical or logical manipulation of the hardware platform [15].

3.2 Security Threats of LMS Platforms

Before analyzing the threats of online learning platforms, it is necessary to describe the basic principles to ensure the quality of online courses. This aspect will be described in the light of the three principles of information security: confidentiality, integrity and availability.

The principle of confidentiality is very important when taking an online test or exam, as it must be ensured that their content will not be available until the scheduled time, and that the student's test will not be accessible to his / her colleagues.

Learning platforms have several technical and human vulnerabilities, so that the number of vulnerabilities officially discovered and included in the CVE list [17], of the most used learning platforms is more than 400. Learning management systems [18] are client/server web applications that, among rest, handle user requests coming from clients such as web browsers. Thus, access to critical security resources (databases and files) on the server are needed to perform user demand.

The most critical security flaws, as discussed in literature, are classified into four groups: authentication, availability, confidentiality and integrity attacks [19].

1) Authentication threats:

- *Unsecured communications* using unsecured application level protocols, such as HTTP, allowing transmission of unencrypted traffic.
- *Improper management of active sessions and unauthorized authentication* is related to complex authentication mechanisms. The authentication algorithm and various features make this process quite vulnerable. The critical features are: changing the password, forgetting or remembering the password or updating the account.

2) Availability threats:

- *Flooding DOS attacks* that flood the server with packets to make it inaccessible service to authorized users.
- *Logical attacks* exploit existing LMS flaws to crash remote server or significantly decrease its performance [19].

3) Confidentiality threats:

- *Insecure cryptographic storage* is based on a fact that sensitive information does not have appropriate encryption [18].
- *Insecure direct object reference* usually occurs when LMS uses object references directly in web interfaces without authorization checks being implemented. Mentioned object references can be files, database records and primary keys and are contained either by URL or form parameters [19].
- *Information leakage and improper error handling*, unintentional disclosure of sensitive data and unneeded information through error messages. LMS can leak sensitive information about its logic, configuration and other internal details (e.g. SQL syntax, source code, etc.). LMS systems not often use cryptographic functions properly to protect data and qualifications or use weak encryption algorithms. In both situations, valuable data is relatively easy to access by attacker who can conduct identity theft and similar crimes [19].

4) Integrity threats:

- *Buffer overflow* occurs when an LMS module (e.g. libraries, drivers, server components) tries to store data into an available buffer without validating its size by inserting larger values than expected.
- *Cross Site Request Forgery attack* trying to perform actions on behalf of an authenticated user [20]. When a user is logged into LMS, attacker can deception his browser into making a request to one of LMS task URLs which will cause a change on the server [19].
- *Cross Site Scripting*, a remote attacker can inject and execute arbitrary HTML codes and scripts in the user's browser in the context of the vulnerable website. Successfully exploiting this vulnerability can allow a remote attacker to steal potentially sensitive information, change the look of the webpage, phishing, and downloading attacks.
- *Failure to restrict URL access*. Some LMS resources is limited to a small subset of advantaged users (e.g. administrators). This weakness allows an attacker to retrieve URLs by guessing the address and perform illegal operations on defenseless LMS data [19].
- *Injection flaws*, when data provided by user (e.g. in form fields) is sent to content checking routines as part of a command or query. In such attacks, interpreter fail to detect or respond to character sequences that may be interpreted wrongly, which then results in execution of malicious code by LMS. Finally, attacker could be able to create, update, read or delete all data available to LMS [19].
- *Malicious file execution* is based on a fact that LMS fails to control or disallow execution of uploaded files (homework or image, file) [19].

3.2 Security Threats of VCAs

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. Thus, if in December 2019, the ZOOM application registered 10M daily users, in March 2020, ZOOM registered about 200M daily users [21].

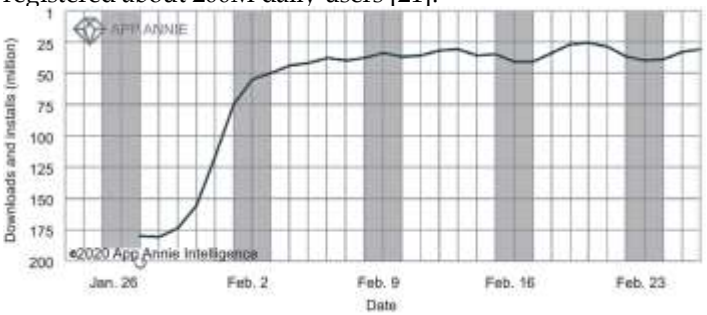

Fig. 5. Usage of the Zoom application [22]

Cyber security is very important when a video conference takes place, starting with the theft of personal data, such as

email, with which users connect and ending with the data being transmitted or the security of end-user devices and control over them. Thus, the key elements of conference security can be grouped into three key areas [23]:

1) **Pre-call policies** are settings for the applications before beginning conference itself, setting access rules (eg. via email).

2) **Policies for data transmissions** are very important for securing video conferencing, because data is transferred using both private and public networks. It may include policies for accessing the conference after it has begun, or notifying the user who initiated the conference when it is being watched, or unauthorized re-broadcasting of the conference.

3) **Post-call policies** are about archiving different metadata, such as: shared presentations, video and audio recordings.

Analyzing the threats identified in 2019-2020, of the most used VCAs worldwide [9], the following threats can be reported [24]:

- *Decrypt video and audio call*, on company servers, which are not always in the sellers' home country. Although it is reported that applications use end-to-end (E2E) encryption, it is only used to encrypt correspondence and documents. For the ZOOM application, which uses a combination of TCP and UDP, TCP connections take place via the TLS protocol, and UDP connections are encrypted with AES using a key negotiated over a TLS connection. This type of encryption is known as transport encryption as when using the HTTPS protocol and not E2E [25]. As an argument why E2E encryption is not used, we use the statements of Matthew Green, cryptographer and professor of computer science at Johns Hopkins University, who emphasizes that: "group video conferencing is difficult to encrypt E2E. This is because the service provider needs to detect who is speaking in order to act as a switchboard, which allows it to send a high-resolution video stream from the person currently speaking or selected by a user. for the rest of the group, and send low-resolution video streams to other participants. This type of optimization is much easier if the service provider can see everything because it is unencrypted" [25]. But in this case, the records on the company's servers are unencrypted and the applications have access to the content, and can later use it to provide information to governments, for example. Companies, of course, say they will protect this data, but the risk of use persists anyway.
- Take control of Windows and MacOS workstations, webcam and microphone, or distribute obscene content. Such actions have taken place in both the United States and Europe.
- Exposing details from physical space. Unlike hacking e-mail or computer hacking video application can analyze and study the surroundings. Users need to ensure the security of their physical space. Any detail from which certain details about the user can be deduced can then be used by social engineering. Social engineering is one of the most widespread attacks. Attackers can observe how their targets and manners speak, which can then be used for impersonation and identity theft.

4 RECOMMENDATIONS AND DISCUSSION

Recommendations for securing distance learning and devices in HEIs will be classified according to the assets involved in the process and their vulnerabilities. The recommendations were developed following an in-depth study of cyber security risks and threats related to the remote study assets.

In order to secure CC services, it is advisable to take into account the actions set out in Table 3.

Table 3. Recommendations for CC security

Actions	Arguments
Systems maintenance	The maintenance of ICT systems is a key process, which ensures proper operation by early detection of factors that can lead to hardware/software failures.
Security patch management	Software manufacturers develop security patches that solve problems identified in the operation process. Installing security patches will eliminate the vulnerabilities.
Hypervisor upgrade	For new features issued by the manufacturer, which corrects vulnerabilities.
Audit of access rights	The classification of access rights for different groups of users makes it impossible to take control and unauthorized rights in case of impersonation or sniffing attacks.
Implementing user authorization policies	The implementation of authorization policies on different user groups will limit access to shared resources.
Development of Aspect-Oriented Programming (AOP) solutions [16]	AOP solutions would create system configurations-oriented student / employee, using the same source code.
Use of encryption protocols	The use of protocols that encrypt communications / data with powerful algorithms will protect data from unauthorized access.
Data encryption	Even if the data is stolen or lost, the unintelligible form will protect it.

Actions to be taken to secure LMS platforms are shown in Table 4.

Table 4. Recommendations for securing LMS platforms

Actions	Arguments
Software update and patch management	Updating platforms and installing patches will correct identified platform vulnerabilities.
Use of encryption protocols	The platforms use the http protocol by default, but it is not secure, so it is necessary to activate the SSL certificate that will encrypt the communication.
Limiting the type of content to load on the platform	To limit the risk of cross-site scripting attacks, it is necessary to limit the type of content that students can upload, because rich HTML content or used plugins, such as flash, make this type of attack possible.
Limited access by default	Ports on devices must be opened only when it is absolutely necessary. Access rules must be strictly limited. Allowed scripts are only those created by the platform developers.
Classification of information	Classification by the level of security required for the information will limit unauthorized access to it.
Implementation of procedures	The development of procedures is very important. Answering questions such as: system operators have been trained in cybersecurity, how platform users access resources, roles have been created and information classified; will allow to develop and implement maximum efficient procedures.

Remote video conferencing has become the new norm in 2020, when studies in HEIs began to take place online. The security threats of remote VCA were announced in the previous point, and now it is necessary to analyze the actions that can be taken to prevent security breaches. Thus, in table 4, actions and arguments were identified.

Table 5. VCAs security recommendations

Actions	Arguments
Updating apps	Failure to update VCA may result in theft, destruction, or compromise of conferences. Automatic application update should be applied. Patch management must be done permanently.
Providing secure remote connection	VCA are not secure by default, as Wi-Fi networks, used by students-staff. Changing the default passwords for routers and Wi-Fi networks, but also the use of secure protocols, such as WPA-2, will increase the security of the remote connection.
Access control	Control rules need to be set, such as: using an access code or password, activating waiting-room options, blocking the conference shortly after it starts, and manually adding / removing conference participants. It is important that the host can connect first.
Distributed information management	Information that may be shared in video conferencing may be stolen, or some users may enter malicious files. Thus, it is necessary not to allow the transfer of sensitive information, which cannot be transmitted by email, due to the secrecy, in the conference, because the risks are similar. Limiting the types of files that can be distributed is a good practice that would limit the upload of potentially malicious (.exe) files. It's also important to restrict the sharing of chat attachments.
Records management	Recordings made at the conference may be stolen or published without authorization. In this regard, it is necessary that all participants be warned that registration has started and that the storage should be done in accordance with the policies adopted at institution level. Thus, it is good that the recording of the conference can be done only by the host, or at least it is necessary to set up alerts.
Configure alerts	Video conferencing can be redistributed, and setting email forwarding alerts, for example, is an important factor. This way the host will be able to verify the authenticity of the user who did it and if necessary, will reschedule the session.

For a good security of online platforms and applications, it is necessary to take into account the provisions of OWASP (Open Web Application Security Project) [26], which is a comprehensive framework to ensure the security of web applications.

5 Conclusions

The academic environment went through a rather difficult period in 2020, as a result of the pandemic with Covid-19. An ongoing challenge has been to ensure cyber security in remote activity. Addressing security, in terms of the specific nature of remote activities and identifying security assets and threats in HEI, is an important step to ensure cyber security. Moreover, the financial losses this year in the education, increased, as a result of online activities. The migration of local stored data in the cloud, brings new challenges in the field of information security, but this is inevitable, for the convenience of users and easy access to the requested information.

As a result of the research, the following conclusions can be drawn:

1) Updating information systems and applications, patch management and automating these processes will ensure a consistent level of security.

2) To control access to information is very important, so the development of access policies for applications and stored data, is mandatory, in order to minimize unauthorized access or compromise of data. Classifying information for restricted access is an important step.

3) The use of secure protocols will allow end users to protect their home network and institutions to protect the corporate network. The transmitted data will be protected and encrypted.

4) Educating staff and students in the field of information security will reduce the effort of the IT team, and will increase, through distributed efforts, cyber security.

Ensuring cybersecurity in HEIs is a complex process, due to distributed systems and multiple challenges, and the research is far-reaching in this area. Covid-19 has brought essential changes in the organization of studies in higher education institutions, new assets must be protected.

References

[1] Ponemon Institute, "Cost of a Data Breach Report," 2020. Accessed: Dec. 01, 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

[2] Micah Castelo, "Cyberattacks Increasingly Threaten Schools — Here's What to Know," EdTech: Focus on K-12, 2020.

[3] Kaspersky, "Digital Education: The cyberrisks of the online classroom," 2020. Accessed: Dec. 06, 2020. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf.

[4] Sally Adam, "Coronavirus and remote working: what you need to know." https://news.sophos.com/en-us/2020/03/12/coronavirus-and-remote-working-what-you-need-to-know/ (accessed Dec. 02, 2020).

[5] A. Elgelany and W. Gaoud, "Cloud Computing: Empirical Studies in Higher Education A Literature Review," International Journal of Advanced Computer Science and Applications, vol. 8, no. 10, pp. 121–127, 2017, doi: 10.14569/IJACSA.2017.081017.

[6] V. H. Pardeshi, "Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation," Procedia Economics and Finance, vol. 11, 2014, doi: 10.1016/S2212-5671(14)00224-X.

[7] Ananthi Claral Mary.T and Dr.Arul Leena Rose.P.J, "Implications, Risks And Challenges Of Cloud Computing In Academic Field – A State-Of-Art," INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, vol. 8, no. 12, pp. 3268–3278, Dec. 2019.

[8] MindWi res LLC, "e-Literate European LMS Market Dynamics," 2016. Accessed: Dec. 03, 2020. [Online]. Available: https://www.dropbox.com/s/2wnhrfpooa1kid6/e-Literate%20European%20LMS%20Market%20Dynamics%20Fall%202016.pdf?dl=0.

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

[10] E. U. A. for C. Enisa, "Sectoral/ thematic threat analysis," 2020.

[11] W. J. Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing," 2011. Accessed: Dec. 02, 2020. [Online]. Available: https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-computing.

[12] D. A. B. Fernandes, L. F. B. Soares, J. v. Gomes, M. M. Freire, and P. R. M. Inácio, "Security issues in cloud environments: a survey,"

International Journal of Information Security, vol. 13, no. 2, Apr. 2014, doi: 10.1007/s10207-013-0208-7.

[13] M. Nanavati, P. Colp, B. Aiello, and A. Warfield, “Cloud security,” Communications of the ACM, vol. 57, no. 5, May 2014, doi: 10.1145/2593686.

[14] R. v. Deshmukh and K. K. Devadkar, “Understanding DDoS Attack & its Effect in Cloud Environment,” Procedia Computer Science, vol. 49, 2015, doi: 10.1016/j.procs.2015.04.245.

[15] L. Coppolino, S. D’Antonio, G. Mazzeo, and L. Romano, “Cloud security: Emerging threats and current solutions,” Computers & Electrical Engineering, vol. 59, Apr. 2017, doi: 10.1016/j.compeleceng.2016.03.004.

[16] W. J. Brown, V. Anderson, and Q. Tan, “Multitenancy - Security Risks and Countermeasures,” Sep. 2012, doi: 10.1109/NBiS.2012.142.

[17] https://www.cvedetails.com/product/3590/?q=moodle, “Moodle: Vulnerability Statistics,” MITRE Corporation. https://www.cvedetails.com/product/3590/?q=moodle (accessed Dec. 04, 2020).

[18] Zlatko Stapić, Tihomir Orehovački, and Mario Đanić, “Determination of optimal security settings for LMS Moodle,” in 31st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2008), 2008, pp. 84–89.

[19] S. Kumar and K. Dutta, “INVESTIGATION ON SECURITY IN LMS MOODLE,” International Journal of Information Technology and Knowledge Management, vol. 4, no. 1, pp. 233–238, 2011.

[20] M. V. Eekelen, R. Moussa, Engelbert Hubbers, and Roel Verdult, “Blackboard Security Assessment,” CTIT technical report series, 2013.

[21] Gina M. Vitiello and Chamberlain Hrdlicka, “Video Conferencing and Recording: Know the Risks Before You Connect.”

[22] 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.

[23] SCOTT GODE, “Video Conferencing Security Issues and Opportunities,” UnifySquare,2020. https://www.unifysquare.com/blog/video-conferencing-security-issues-and-opportunities/ (accessed Dec. 02, 2020).

[24] Kaspersky, “The problems with videoconferencing apps,” 2020. Accessed: Dec. 07, 2020. [Online]. Available: https://www.kaspersky.com/blog/videoconference-software-security/35196/.

[25] Micah Lee and Yael Grauer, “ZOOM MEETINGS AREN’T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING,” The Intercept, 2020.

[26] OWASP, “OWASP Application Security Verification Standard.” 2020, Accessed: Dec. 15, 2020. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/.