CYBERSECURITY RECOMMENDATIONS AND BEST PRACTICES FOR DIGITAL EDUCATION

Miroslav NEDELCHEV, Delyan SLAVOV

"Vasil Levski" National Military University, Artillery, Air Defense and CIS Faculty, Shumen, Bulgaria (nedel4ew@abv.bg, slavovd@yahoo.com)

DOI: 10.19062/2247-3173.2023.24.6

Abstract: *In light of Covid-19, there has been an increasing trend over the past few years to use e-learning platforms more frequently. Hackers use various methods to play with the human mind of the learner or instructor, using their unexperienced internet habits. The article examines the risks and benefits of using augmented, mixed, and virtual reality applications in e-learning. Good practices for cyber risk assessment and measures to improve cyber security are shown.*

Keywords: *digital education, cybersecurity risk, network security*

1. DISTANCE LEARNING

With the development of modern computer and communication technologies and Internet connectivity, it becomes possible to create digital learning content by simulating different types of activities, such as driving a robot, car, plane, etc. At the same time, computer-aided technologies for training, design and training are getting a big boost in development.

It is apparent that information and communication technologies (ICT) must be used in education. The "e-Europe" program aims to successfully integrate ICT systems into educational institutions. It can benefit all stakeholders and solve difficulties of a different kind, such the issue of traditional classrooms' time and space constraints [1]. Additionally, students and teachers have access to a wealth of current and varied information through the use of ICT and related software and hardware, which can help students learn and teachers create lesson plans.The dynamic nature of information technology development has led to the rapid development of learning approaches, upgrading from classrooms to providing learning materials on flash/CD and moving into the world of e-learning and cloud technologies.

Electronic learning (e-learning) is a course in which the delivery of learning content is in an electronic format. Communication between users and knowledge control is done with the help of computer technology.

The flexibility and cost of online education are its two main benefits. Students who have more flexibility can access lectures whenever they want, making it easier for them to balance their family obligations, career commitments, and course loads. The cost-effectiveness of online education is another major draw; classes there are far less expensive than those at regular colleges. A student can acquire an education at a fair price regardless of background thanks to the extensive reach of online learning. Their improved standard of living is a result of this education [6]. E-learning can be divided into several types:

- CBT – Computer-based training);
- TBT - Technology-Based Training – technologies are used in training. It usually takes place outside the "classroom";
- Web-based training – self-study using the resources of a Web browser;
- Distance learning.

2. RISKS AND BENEFITS OF USING VIRTUAL, MIXED AND REALITY APPLICATIONS

In many cases, a combination of several types is used in the implementation of e-learning, and in the last 10 years, in addition to entertainment, virtual, augmented and mixed reality technologies have been widely used as a supplement to technology-based learning and allow the combination of high technologies and traditional learning approaches.

- VR - virtual reality is a computer-generated reality with a 3D image and in most cases with sound.
- AR - augmented reality refers to computer-aided perception or representation that augments the real world with virtual objects. With integrated cameras in mobile devices, additional objects or information can be included in the current image of the real world.
- MR - in mixed reality, either augmented reality (Augmented Reality), which requires AR-glasses, or augmented virtuality in the sense of connecting with reality is expanded.

The benefits of using such technologies are time-proven and can include:

- Education independent of time and place, but only of hardware and software connectivity;
- Personalized and flexible training;
- Learning through experience - acquired information is perceived as experience;
- Ability to judge environment and extract context;
- Ability to standardize a certain environment and study the behavior of learners;
- Ability to analyze and review the actions that led to one or another scenario;
- Introduction of uniform evaluation criteria;
- Ability to introduce policies for mandatory and recommended activities to be performed;
- Ability to simulate dangerous experimental situations, in order to carry out experiments without the participants being physically endangered;
- Ability to quickly and easily switch from one virtual environment to another virtual environment.

Some of the disadvantages include vertigo, loss of spatial orientation, nervousness, addiction but also vulnerability to malicious attacks – denial of service, voice theft, fingerprinting, eye tracking, malware use, hacking attacks, ransomware and denial of service attacks, spoofing, fraud and data theft, privacy and data integrity issues, etc. [6]

Online classes are more vulnerable to cyber-attacks than computer-based learning, especially from the point of view of end-user security. Cyber risks that can threaten [3] the safety of online learners include [8]:

- Deliberate software attacks (viruses, worms);
- Software bugs and errors - problems of a technical nature at the physical and channel level;

- Human errors due to ignorance or mistakes;
- Intentional unauthorized access, espionage or intrusion to collect data);
- Sabotage/vandalism damage to information or system);
- Equipment damage;
- Intentional theft (unlawful taking of equipment or information);
- Theft of intellectual property;
- Deviations in the quality of service due to outdated technologies;
- Extortion to disclose information.

Given the observed increase in the use of virtual/augmented reality technology, potential cyber vulnerabilities and threats must be considered. Cyber-attack scenarios [5] related to VR/AR can include:

• Illegal recording and data theft of user behavior – Hackers record user behavior in their VR/AR environment and threaten to publicly release the recording unless a ransom is paid

• Inserting information or data into VR/AR to mislead or entice users to select items that exfiltrate personal information

• Sabotaging the availability of VR/AR devices to disrupt important workplace meetings

• Using fake VR/AR apps that steal personal information or exfiltrate behavioral data

• Replacing educational or training content with malicious content or taking over the VR/AR ecosystem and demanding a ransom.

3. MEASURES TO REDUCE CYBER RISK

In order to apply adequate measures to a specific distance learning system, it is necessary to conduct a test and analysis/evaluation of the e-learning system.

Nevertheless, to have a secure environment for use, a cybersecurity requirements must be met, the following elements [2] must necessarily be included:

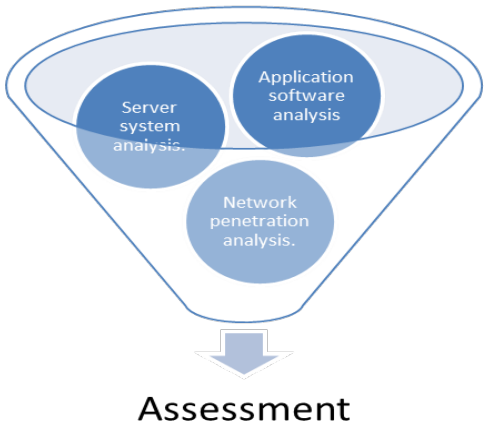

FIG.1 Assessment of e-learning system

An example methodology for assessing the cyber security of an electronic learning platform is shown in Table 1.

Table 1: Cybersecurity e-learning platform methodology [2]

№	Activity / Test phase	Instruments	Expected Output
1.	Information Gathering (Reconnaissance)	- Netdiscover; - Nmap/ZenMap; - Dnesenum; - DNSMap.	- IPs; - Network topologies; - Active services; - Used applications
2.	Vulnerability Scan (Scanning phase)	- OpenVas; - Nessus Scanner; - Nmap; - BED	- Network Vulnerabilities; - OS Vulnerabilities - Web Vulnerabilties; - DB Vulnerabilities
3.	Network Security Assessment: (Testing the network services and components)	- Cisco torch; - Cisco Auditing Tool; - Cisco Global Exploiter; - Aircrack-ng; - Fluxion; - Ghost Phisher; - Nmap	- users, passwords; - firmware vulns. exploits - misconfigurations; - Authentication Control; - Traffic encryption
4.	OS Security Assessment	- OpenVas Scanner; - Nessus Scanner; - Metasploit - Core Impact; - Searchsploit.	- users, passwords; - OS vulns. Exploits; - Configuration check; - Security Update Status
5.	Web Security Assessment (Web App check)	- Burpsuite; - Webscarab; - Owaspzap; - Nikto; - Metasploit	- XSS; - SQLi; - webApp (apache, nginx) vulnerabilities; - Update status; - Denail of Service; - URL manipulation
6.	DB Security Assessment	- Sqlmap; - Sqlninja; - Oscanner;	- users, passwords; - SQLi; - Privilege and role grants; - Data encryption; - Authorization Control; - Configuration Checking; - Update Status.
7.	Final Penetration testing report (detailed pentesting process overview)		- Assessment Overview; - Found Vulnerabilities; - Risk Factors; - Tools used; - Summary of Findings; - Evidence - Remediation and patching; - References
8.	Cybersecurity requirements definition	- Using Penetration testing report as a detailed cyberhealth estimation overview of the target network/system.	- Personalized cybersecurity policy; - Personalized cybersecurity recommendations

Network security is a responsibility for the whole institution. Network administrators and protectors can maintain up-to-date knowledge of threats and counter measures through exchange of information with peers, government and others. The contribution of users cannot be underestimated in the security of any network and related information. [3]

Cybersecurity policy and requirements for e-learning platforms includes:Requirements for System (server) administrators; Account policy; Permissions and Access policy; Network Security Policy Data Loss Prevention frontend web application and backend DBMS security policy; Update and Patch Policy;

Requirements for e-learning software (front-end, application) administrators: Requirements for users – teachers and instructors; Safety and security rules; General password requirements; Requirements for users – students and learners;Safety and security rules;**Error! Bookmark not defined.** Anti-Malware Policy; General password requirements

Measures to improve cyber security of VR/AR systems: [5]

- Using secure messaging between VR/AR devices and a centralized content system
- Encrypting incoming and outgoing connections to and from VR/AR devices and a centralized content system
- Use appropriate identity and authentication mechanisms and a centralized ecosystem to manage agent communications with the master server
- Protecting the applications and firmware that are installed on the devices
- Installing anti-tampering software on user firmware
- Storing the key by applying security concepts – such as encryption or data masking
- Protection against device and identity impersonation
- Force authentication of communication between VR/AR devices
- Monitoring for unusual behavior of the VR/AR device, application and ecosystem.

4. CONCLUSION

To maintain a high degree of common cyber hygiene and cyber resilience, all personnel must adhere to the established standards and the cybersecurity policy. A platform that is based on the internet can never be completely safe because it allows network access and hacker assaults are always evolving. Administrators must be knowledgeable and qualified in order to respond effectively to emerging trends and threads. The systems and software are kept up to date, cybersecurity awareness training is given to all users, and social engineering is still a successful attack vector.

ACKNOWLEDGEMENT

The creation of this paper was possible by the active support of the participants in National Science Program "Security and Defense" financed by the Ministry of Education and Science (MES) of the Republic of Bulgaria.

REFERENCES

[1] P. Aleksiev, 2015 E- governance development in EU and the place of Republic Bulgaria in the process, Public Administration, New Bulgarian University https://ebox.nbu.bg/pa2015/10_P.%20Aleksiev.pdf;

[2] I. Bandara, F. Ioras, K. Maher,2014, *Cyber security concerns in e-learning education*, Proceedings of ICERI2014 Conference, 17th-19th November 2014, Seville, Spain ISBN: 978-84-617-2484-0, pp 0728-0734;

[3] Y. Dechev, 2016, Study of the opportunities of information technology for maritime training PhD dissertation;

[4] Digital Competences for Improving Security and Defence Education (DIGICODE) 2023, Project KA226 Strategic Partnerships for Higher Education: 2020-1-PL01-KA226-096192, Cybersecurity requirements for e-learning platforms in digital security and defence education –Intellectual output 03;

[5] V. Dissanayake, 2018, *A review of Cyber security risks in an Augmented reality world*, https://www.researchgate.net/publication/339941469;
[6] L. Nikolov, R. Dimov, 2020, *Malware in Social Engineering*, CONFSEC, https://www.researchgate.net/publication/349339696_Malware_in_Social_Engineering;
[7] K. Ritesh, *Virtual and Augmented Reality (VR/AR) Cybersecurity Challenges*, available at https://www.linkedin.com/pulse/virtual-augmented-reality-vrar-cybersecurity-kumar-ritesh/;
[8] G. Sebastian, 2022, *Online Education From a Security Risk and Controls Perspective*, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/online-education-from-a-security-risk-and-controls-perspective.