ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 06, Issue 03, pp.4733-4735, March, 2019

RESEARCH ARTICLE

SECURITY THREATS IN ELECTRONIC LEARNING

***Pee Vululleh, Phd**

Faculty, Department of Engineering and Computer Science, Regent University, USA

ARTICLE INFO

Article History:
Received 17th December, 2018
Received in revised form
24th January, 2019
Accepted 10th February, 2019
Published online 30th March, 2019

Keywords:
E-learning, Security Threats, Security Issues.

ABSTRACT

Technological advances have made e-learning an increasingly central delivery system enhancing teaching and learning processes. Unlike face-to-face methods of teaching, which depend on physical structures, e-learning provides a potentially better alternative to face-to-face learning and makes learning easily accessible. With e-learning, education can be facilitated from virtually anywhere and at any time because of the convenience and affordability of the new technology. At the same time, however, new technology has introduced platforms that attract illegal activity. Consequently, e-learning is exposed to such threats, and security has, therefore, become one of its most pressing issues. This paper identifies and catalogs information regarding the security of e-learning systems and the protections needed to secure the users (i.e., instructors, students, and administrators) from authorized security threats.

INTRODUCTION

Electronic learning (e-learning) is a form of learning delivery that employs the Internet for communication between a source and a student. E-learning creates an interactive process that allows studentsto communicate with their teachers or other students. Sometimes, e-learning can be delivered via live channels, where students can electronically raise their hands and interact in real-time; at other times, such systems can deliver pre-recorded lectures. Whatever the process, there is always a teacher interacting and grading students' participation—quizzes, tests, assignments and discussion forums. Despite the many advantages that technology affords, such platforms can harbor illegal activities. Because online learning fundamentally uses the Internet, information generated in this context— notably personal or confidential information—is exposed to security threats. Criminal elements have always used new technologies to their advantage, and the advancement in e-learning has provided them with as many opportunities for innovation as it has legitimate users (Hampton, 2016). Security is an essential part of e-learning systems, as the success of such systems requires the protection of these valid users—instructors, students, and administrators—from unauthorized threats. The purpose of this paper is to identify and catalog information regarding security threats commonly apparent in e-learning environments.

E-Learning security

Users of an interactive computer system such as the Internet can only become comfortable with it to the extent they can trust it.E-learning security involves the process of detecting and preventing unauthorized access to such platforms (Mahmoud *et al*., 2016).

Corresponding author:* **Pee Vululleh
Faculty, Department of Engineering and Computer Science, Regent University, USA.

The term *detection* refers to whether successful or unsuccessful attempts have been made to break into the system. Measures of *prevention* ensure that unauthorized users cannot access the system in the first place.

Security is relevant in several aspects of e-learning systems

- Trust in an e-system is a necessary condition for user acceptance.
- With new e-systems come new threats.
- Projects involving e-learning systems are frequently beset with security issues.

Failure to apply proper security in e-learning systems can compromise student innovations or allow theft of personal information (Udroiu, 2017). E-learning security should protect study notes, demonstrations, references, academic integrity, students, instructors, and staff.

Online e-learning security threats

Because of the vast amount of sensitive data that they transmit and manage, e-learning systems are often the target for cyber-criminals. For example, in 2018, the United States government charged nine Iranian hackers for orchestrating a campaign to access and steal millions of records of sensitive information from over 300 American and foreign universities. In 2015, the Harvard University system was breached, although it remains unclear what information may have been accessed by the hackers. Similarly, in 2015, Pennsylvania State University announced that its computer system had been breached, which resulted in the theft of the personal information of over 18,000 users.

Among the biggest security issues facing e-learning is the intensity and persistence of attacks that aim to steal personally identifiable information (PII), disrupt schools' ability to operate, and damage schools' reputations.

Social media sneaks

Today, cyber-hackers infiltrate computer systems and install a piece of so-called *malware* that can give them control overan entire system and allow them access to extract data. Social media and the openness of the Internet has thus become a major problem for e-learning (Huu *et al*., 2016). Hackers commonly gather intelligence about university students, faculty, and employees and use this information to break into its computer systems. With state-sponsored attacks, these processes occur over longer periods, so these thieves deploy entire staffs that spend a lot of time performing reconnaissance on different universities.

Spear phishing threats

Spear phishing refers to an email spoofing attack that targets e-learning systems to gain unauthorized access to sensitive data (Gupta *et al*., 2017). The introduction and use of social media have helped spear phishing grow into a deceptive weapon with advanced sophistication. With spear phishing, hackers research an individual by name, place of work, residence, and friends' lists on social media sites like Facebook and LinkedIn. With this information, they craft a communication which includes links or an attachment for download that looks appears legitimate to that user. Once the recipient clicks the link or downloads the attachment, their computer system is immediately compromised. These download attachments introduce malware into the recipient's computer system, which in turn helps the hackers steal passwords that can provide them access to the institution network.

Smartphone risk

Students, faculty, and staff use a variety of devices to connect to e-learning systems. These devices are vulnerable to attackers because they are not secure compared to the institution's primary computer systems. With their lesser computing power and their users' inability to install security software because of the device's limited memory. Cell phones (smartphones) are the worst security risk. Moreover, the software hackers' cost to hack phones and steal passwords and other PII is very low (Burkart and McCourt, 2017). Physical theft of such devices also presents a major risk. If any member of a university system loses a phone, the phone may find its way into the hands of a hacker and provide that hacker with a means of entry into an institution's computer systems.

Creating a secure e-learning environment

E-learning is dependent on information and communication technologies; thus, security should be a top priority as it gives users the confidence to use the systems. E-learning security mechanisms should support authentication, authorization, and confidentiality (Al-Alkeen *et al*., 2017; Halabiand Bellaiche, 2017).

Authentication

In e-learning systems, authentication is the process of validating users' (students, instructors, administrators, and staff) identities (Halabi and Bellaiche, 2017). Password sensure the security and confidentiality of stored data. Some of this data includes instructor, student, and staff names along with grades, addresses, schedules, evaluations, and other data belong to individual or organizational users. Password-guessing is one of the most common ways that hackers break into e-learning systems. It is the responsibility of each user of e-learning systems to make sure that all their account passwords are as difficult to guess as possible. More importantly, there are many protocols for protecting passwords that the major platforms are constantly creating for access protection. For example, *Captcha* is one technique that can help in authenticating user identities and in preventing spammers and viruses. *Captcha* can be positioned during the enrollment process to ensure that users signing up for e-learning deliverables are actually the correct studentto enroll. The software can also be used to monitor the number of attempts made by a user to log in to the system. This procedure can help limit unauthorized users, given that the users have fewer opportunities to discover the correct password by random selection.

Authorization

In e-learning, authorization occurs after a user's identity has been successfully authenticated by the system, which then grants the user access to information and resources. In other words, once a user's identity (username and password) has been verified (authenticated), the next step would be to determine the extent of the information to which the user is allowed access (authorization). When a user (student or instructor) enters their username and password to the system and the system confirms these data to be the correct credentials, the next step would be to determine which information that user can access. For example, there is no need for a student or instructor in "course A" to be given access to "course B", and so there is reason for someone in staff payroll to be given access to confidential student's records. A secure e-learning system helps prevent data leakage and reduce the chances of other cyber-attacks.

Confidentiality

In e-learning, confidentiality is the equivalent of privacy. Confidentiality involves the measures undertaken to ensure confidential users' (students, instructors, and staff) information is not accessible by unauthorized individuals while making sure that the right users can, in fact, gain access to it.Many e-learning systems have built-in security measures. As such, a regular update to the systems is a good idea to ensure that the latest version of a platform's security add-ons is in place. The e-learning systems' providers should be contacted for helpful advice on security measures currentlyoperative. In order to sure these security mechanisms work, there should be accountability tests performed as an audit.

Conclusion

Technological advances in e-learning systems have provided humans with the ability to learn anywhere and at any time. These systems possess massive amounts of data about students, faculty, donors, staff, research programs, governmental information, and all manner of confidential material, which makes them tempting targets for cybercriminals. Technological advances have also provided us with the ability to detect and respond to data breaches instantly. Effective online learning systems security depends on creating an environment and organizational structure where management understands and supports security efforts and

encourages the users to exercise caution. Security teams should ensure that instructors, staff, and students are aware of their security and support roles and are willing to accept these obligations, especially when the protective activities involve some consumption of personal time. After all, security is the responsibility of everyone.

REFERENCES

Al-Alkeem, E., Shehada, D., Yeun, C., Zemerly, M. and Hu, J. 2017. New secure healthcare system using cloud of things. *Cluster Computing,* 20(3), 2211-2229. doi:10.1007/s10586-017-0872-x

Burkart, P. and McCourt, T. 2017. The international political economy of the hack: A closer look at markets for cybersecurity software. *Popular Communication,* 15(1),37 -54. doi:https://doi.org/10.1080/15405702.2016.12699 10.

Gupta, B., Tewari, A., Jain, A. and Agrawal, D. 2017. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), 3 629-3654. doi:3629-3654. doi:10.1007/s00521-016-2275-y.

Halabi, T. and Bellaiche, M. 2017. Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications,* 33, 55-65. doi:10.1016/j.jisa.2017.01.007.

Hampton, K. 2016. Persistent and pervasive community: New communication technologies and the future of community. *American Behavioral Scientist*, 60(1), 101-124. doi:10.117 7/0002764215601714

Huu Phuoc Dai, N., Kerti, A. and Rajnai, Z. 2016. E-Learning Security Risks and its Countermeasures. *Journal of Emerging research and solutions in ICT*, 1(1), 17-25.

Mahmoud, A., Barakat, M. and Ajjour, M. 2016. Design and development of elearning university system. *Journal of multidisciplinary engineering science studies (JMESS),* 2(5), 498-504. Retrieved from http://www.jmess.org/wp-content/uploads/2016/05/JMESSP13420106.pdf

Udroiu, M. 2017. The cybersecurity of elearning platforms. 3, p. 374. Carol I" National Defence University.

****