ISSN 2277-3061

A REVIEW OF SECURITY THREATS BY THE UNAUTHORIZED IN THE E-LEARNING

Mohamed Munser Saleh1, Fauziah Abdul Wahid2
Faculty of Science and Technology, University Sains Islam Malaysia (USIM)
Bandar BaruNilai, 71800 Nilai, NegeriSembilan,Malaysia

Abstract

Computers have become an integral part of our everyday existence. They are used to store and to send among students' letters and sensitive documents, materials. In today's focused world, each Organization is endeavoring to enhance its proficiency and guarantee the nature of data asset. Computer networking technologies - intranet, web - have progressed to the point where data can be put away, transmitted, and available to people accessing the resource anytime and from anywhere. These advantages additionally push organizations into executing web based innovation without considering the security dangers that this involves.

Keyword

unauthorized; threats; E-learning security.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY
Vol. 14, No. 11
www.ijctonline.com, editorijctonline@gmail.com

1. Introduction

Technology is a critical instrument in applying and ensuring the successful e-learning. As being defined, e-learning means having people talking, composing, teaching and learning with each other online or in other words, utilizing computer-based systems(Yacob, Kadir et al. 2012).

E-learning is different from other e-services in the applications utilized; the methodology and the partner conduct molded nature of e-learning. Issues of dependability of the framework in course material, information security in the evaluating result, non-denial and abuse of e-learning, LMS are cases of social specialized security issue which is particularly identified with individuals. Individuals need to take after approach, methods and others exercises to guarantee the CIA is attained to. Individuals are relied upon to be the security controllers themselves. However, individuals likewise can be the vulnerabilities where danger can happen, in case: secret key imparting, non-denial, and malware infection (Alwi and Hayaati 2012).

2. Basic Security Requirements

The following basic security aspects should be meeting for e-learning platforms: authenticity, access control, confidentiality, integrity, availability, non-repudiation. A secure authentication is required to identify the user who will use the web application and to determine his access privileges. This mechanism prevents the attackers to access another user’s account, to view sensitive information or to perform unauthorized operations. Also, once authenticated, the user should have the possibility to change his password (Luminita 2011).

2.1 Access control - Users can't exchange or build the got benefits regardless of the fact that they team up without the culprit being recognized(Vasilescu, TATAR et al. 2011).

2.2 Confidentiality- Confidentiality refers to keeping the revelation of data to unapproved people or systems. Because of the way that learning material by its temperament must be appropriated to the outside, industrial espionage and information robbery are not real issues in e-learning. In any case, in specific situations, this is likewise of importance. Beside countermeasures against the physical burglary of capacity gadgets, persevering security executives need to set up countermeasures against electronic robbery, for example, the establishment of firewalls and interruption discovery instruments to hamper assailants from the outside(Kim 2013).

Confidentiality- guaranteeing that data is not uncovered to any unauthorized people. From an e-learning perspective, learners require the confirmation that the assignments they submit online are kept private and just unveiled to the expected inspector(Eswari 2011).

2.3 Integrity-measures are taken to protect information from transmission errors, however, users might likewise wish to be protected from a message being changed deliberately for malignant reasons, additionally defines what rights and services the end user is allowed once server access is granted(Mohammad, Awadhi et al. 2012).

Integrityis that just approved clients are permitted to alter the contents which incorporate creating, changing, appending and erasing information and metadata and the assaults on integrity are for the most part the endeavors made to effect change or devastate data in the E-Learning site without legitimate approval (Ahmed, Buragga et al. 2011).

2.4 Availability - a network service can be unavailable because of heavy movement conditions or hardware/software failures, yet a service can likewise be disrupted because of pernicious assaults that attempt to deny service(Eswari 2011).

Availability The E-Learning material e-substance, information (or metadata) is to be made accessible to the learner at the pointed out session when the client sign on to the framework for their session at the time to time, if the obliged material is not accessible the learner will lose premium and not get the at most utilization of learning framework. Mostly there are two sorts of assaults via blocking assault and flooding assault, e.g.: Denial of Service, Node assaults, Line assaults, Network foundation assaults(Nickolova and Nickolov 2007).

2.5 Non-Repudiation -guarantees that no gathering in an operation can deny partaking in the operation. We can likewise characterize the system of Nonrepudiation as the component concentrate on the way that the sender of the message cannot deny having sent the message later on (Rjaibi, Rabai et al. 2013).

Non-Repudiationis the last step in information security where the learner has to be provided with e-learning services without any possible fraud, such as when computer systems are broken into or infected with Trojan horses or viruses, to deny the works or changes done by them in the system(Luminita 2011).

2.6 Authentication -In e-assessment, it is insufficient to assume correctness of a student based only on an identity. The e-appraisal security framework requires demonstrated that the personality guaranteed to really fit in with the holder who put away the data. Subsequently, when the security framework requests a response to the "is it truly you?" Doubt; it basically asks for a proof of the guaranteed character. Confirmation information is regularly a mystery which ought to be known to the understudy and the security framework alone. When all is said in done, client validation is characterized into three classifications:

(1) Something the user knows (knowledge)

(2) Something the user has (possession)

(3) Something the user is (biometrics) (Apampa, Wills et al. 2010).

Authentication: a user may want to be sure that a received message was sent by the user whom they purport to be and not by someone masquerading as another. _ Authentication involves validating the end users' identity prior to permit them server access (Mohammad, Awadhi et al. 2012).

2.7 Privacy Is necessary to ensure non-disclosure of information given to each user. Privacy is required to ensure the security of information related to each user. E-learning framework security administration, privacy and access control are now pulling in all that much consideration because of the most recent patterns in training frameworks improvement and endeavor to make an electronic record of an understudy so as to empower the versatility of examining. Access control ought to anticipate unapproved access to imparted assets. Gathering such a prerequisite in E-Learning frameworks is extremely mind boggling since it is important to ensure the substance, administrations and individual information not just from the outer clients of a framework, additionally from the advancement and managerial inward clients of a framework(Sabic and Azemovic 2010).

3. Security Threat Source

A threat can be caused by internal, external or both external and internal entities.

3.1 Internal threats: Internal threats occur when somebody has authorized access to the network with either a record on a server or physical access to the system. A risk can be inward to the organization as the result of employee action or failure of an organization process.

3.2 External threats: External threats can emerge from people or organizations working outside of an organization. They haven't approved access to the PC systems or network. The most clear outside dangers to PC systems and the occupant information are characteristic catastrophes: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network (Jouini, Rabai et al. 2014).

4. Types of Security Threats

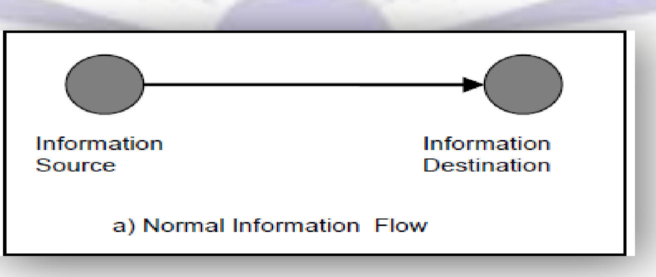
There are these requirements:

- Secrecy - only authorized users have access
- Integrity - only authorized users can make changes
- Availability - the assets are not kept from authorized users

In general Categories:

- Interruption - prevents availability
- Interception - breaks the secrecy or confidentiality of the data
- Modification - attacks the integrity
- Fabrication - attacks the authenticity

Information security threats can be viewed in many different perspectives such as threat source – factor (vulnerability) – threats (action) – implications (attack). These different perspectives are connected and it is vital that they are understood in order to assess the possible risk and design controls appropriate to an organization(Alwi and Hayaati 2012).



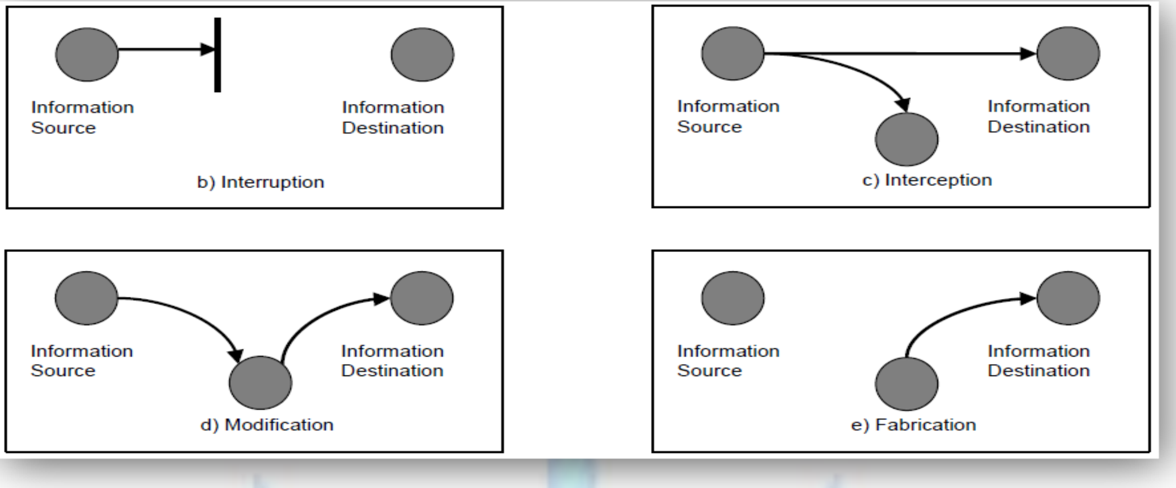


Figure1 Outcome of Security Breach(Source: Stallings, 2007).

5. Conclusion and Future Work

Unauthorized is one of the threats that pose an obstacle to increase efficiency and ensure the quality of the content. It is necessary protect the assets against these threats. And must be maintained at these conditions Secrecy, Integrity, Availability. To achieve these conditions, we need to assess these risks and following the steps in the evaluation: system characterization, threat assessment, vulnerability analysis, impact analysis, and risk determination.

6. References

[1]Ahmed, S., K. Buragga and A. K. Ramani (2011). Security issues concern for E-Learning by Saudi universities. Advanced Communication Technology (ICACT), 2011 13th International Conference on, IEEE.

[2]Alwi, M. and N. Hayaati (2012). "E-learning stakeholders information security vulnerability model."

[3]Apampa, K. M., G. Wills and D. Argles (2010). "User security issues in summative e-assessment security." International Journal of Digital Society (IJDS)**1**(2): 1-13.

[4]Eswari, P. L. (2011). A process framework for securing an e-learning ecosystem. Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, IEEE.

[5]Jouini, M., L. B. A. Rabai and A. B. Aissa (2014). "Classification of security threats in information systems." Procedia Computer Science**32**: 489-496.

[6]Kim, H. (2013). "E-learning Privacy and Security Requirements: Review." Journal of Security Engineering**10**(5): 591-600.

[7]Luminita, D. C. (2011). "Information security in E-learning Platforms." Procedia-Social and Behavioral Sciences**15**: 2689-2693.

[8]Mohammad, S., A. A. Awadhi, A. Kananah and M. A. Job (2012). "Security Management Policy of LMS in AOU Bahrain Branch." International Journal of Information**2**(6).

[9]Nickolova, M. and E. Nickolov (2007). "Threat model for user security in e-learning systems." International Journal" Information Technologies and Knowledge**1**(1): 341-347.

[10]Rjaibi, N., L. B. A. Rabai and A. B. Aissa (2013). A basic security requirements taxonomy to quantify security threats: an e-learning application. The Third International Conference on Digital Information Processing and Communications (ICDIPC2013), The Society of Digital Information and Wireless Communication.

[11] Sabic, A. and J. Azemovic (2010). Model of efficient Assessment System with accent on privacy, security and integration with E-University components. Education Technology and Computer (ICETC), 2010 2nd International Conference on, IEEE.

[12] Vasilescu, C., E. L. TATAR and A. Codreanu (2011). Integrating Information Security in an E-Learning Environment. Conference proceedings of" eLearning and Software for Education"(eLSE).

[13] Yacob, A., A. Z. A. Kadir, O. Zainudin and A. Zurairah (2012). "Student Awareness Towards E-Learning In Education." Procedia-Social and Behavioral Sciences**67**: 93-101.