Vulnerabilities, Threats and Countermeasures for Information Systems of Education Sector

Prof. Reshma Patil

MCA, Poona College of Arts, Commerce & Science, Camp, Pune, India,
reshmapatil86@gmail.com

Dr. Sachin Kadam

Institute of Management & Entrepreneurship Development, Pune, India
sachin.kadam@rediffmail.com

Abstract - Implementation of technologies is the usual respond to information systems security. Information Systems security is the top concern for everyone. Education sector is not an exception for the same. Educational institutes/universities consists critical information about stakeholders around it. Presented research revealed a framework for stakeholders of Online Admission Process of Education Sector to understand and assess the threats associated with their Information Systems. This framework also provides available countermeasures for the security threats and vulnerabilities of information system.

Keywords: Online Admission System, Confidentiality, Availability, Integrity, Threats, Vulnerability, Countermeasures, Hardware Devices, Software's, Network Devices, Data, Information Security, Information Systems.

I. INTRODUCTION

Innovation in Information Technology have lifted concerns about the risks to data related with weak IT security, comprising vulnerability to viruses, malware, attacks and compromise of network systems and services. Poor IT security may result in compromised confidentiality, integrity, and availability of the data due to unauthorized access.

Ensures that information is protected against unauthorized access or disclosure users (confidentiality), unauthorized or improper modification (integrity) and can be accessed when required (availability). [19]

Now every organization uses Internet and computer network so there is a need for new security countermeasures to reduce the threats and challenges inherent from these new technologies, software applications and network devices. [1]

II. ONLINE ADMISSION SYSTEMS STAKEHOLDERS

Stakeholder is a person or organization that can affect, be affected by, or perceive themselves to be affected by a risk eventuating. [19]

Following are the stakeholders who are involved in online admission systems:

Student, Teacher/Counselor, Administrator, Information Technology, CET Head, Assistance of CET Head, Network Expert, Accountant/Cashier, Bank Personnel, Librarian, Director, Software Developer

III. POTENTIAL THREATS WITH EXPLANATION

The study identified a dozen categories of threats by examining previous works and publications.

1. Hardware Error/Failure- Failure of hardware because of dust, temperature variation, voltage variation, etc. [5]
2. Malfunction of Equipment- Malfunction of Equipment can be caused at any time by inherent errors in the control program. [4]
3. Deliberate Software Attacks- When an individual or group designs software to attack systems, they create malicious code/software called malware. [4][12][20]
4. Hacking- Hacking attack is prone to malicious attacks, system intrusion, break-ins and unauthorized system access from hackers and crackers. [20]
5. Deliberate Acts of Espionage or Trespass- Unauthorized accessing of information, Shoulder surfing, hidden camera, etc. [14][15]
6. Software Malfunction, Act of Human Error or Failure- [12]
7. Act of Human Error or Failure- It includes acts done without malicious intent. It is caused by: Inexperience, improper training, incorrect assumptions, etc. [12]
8. Denial of Service- Denial of Service is an attack when the system receiving too many requests and cannot return communicate with the requestors. [12][14]
9. Network eavesdropping- Interception of communications by an unauthorized party. [12][14]
10. Repudiation- Repudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. [14]
11. Deliberate Acts of Theft- It means illegal taking of another's property -physical, electronic, or intellectual [15]
12. Deliberate Acts of Information Extortion- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return [15]
13. Phishing- Phishing is an attempt to obtain confidential information from an individual, group, or organization. [24]
14. Spoofing- Spoofing is attempting to gain access to a system by using a false identity. [2]

IV. VULNERABILITIES, POTENTIAL THREATS AND POSSIBLE COUNTERMEASURES

1. **Vulnerability**: A weakness in an information system or service that can be exploited by a threat. [19]
2. **Threat**: The potential cause of a risk. [19]
3. **Countermeasures**: A risk treatment implemented to reduce the likelihood and/or impact of a risk. [19]

Common Vulnerabilities of Hardware Devices

1. Susceptibility of equipment to humidity, dust[4]
2. Susceptibility of equipment to temperature variations[4]
3. Susceptibility of equipment to voltage variations [4]
4. Lack of care at disposal [4]
5. Lack of physical protection to equipment [12][13]
6. Inadequate or irregular backup [4]
7. Sensitive to Viruses and Trojan Horses [13]
8. Lack of Authorization could breaks into computer system [20]

Threats of Hardware Devices

1. Hardware Error/Failure[5]
2. Hardware Error/Failure[5]
3. Malfunction of Equipment [4]
4. Information Leakage [10]
5. Deliberate Acts of Theft [12][13]
6. Malfunction of Equipment [4]
7. Unauthorized installation of software [8]
8. Hacking [20]

Countermeasures of Hardware Devices

1. Ensure clean and dust free environment.
   Humidity measuring instruments like (Hygrometer) should be installed in the sensitive equipment room. Vacuuming is important where dust collects, such as under raised floors. Dust generating activities should be carried out well away from dust-sensitive equipment. [6][7][8]
2. Temperature readings should take throughout equipment areas. Heat measuring instruments like (Thermometer) should be installed in the sensitive equipment room.[6]
3. Verify UPS functions properly when voltage variant. Use voltage regulator to protect hardware against temporary increase in power. Use circuit breakers to protect hardware against sustained increases in power. To avoid discontinuity in work, two independent supply sources should be exist so that one can be used if the other fails. [6][7][8][9]
4. Use document shredder to chew up CDs, DVDs. Securely Wipe Magnetic Drives. Establish and implement organization-specific procedures and technologies for the disposal of materials. [10][11]
5. Keep an inventory of all equipments. Buy microcomputers with a lock that disables the keyboard and removal of the case. Introduce a system for logging equipments into and out of the building. Do spot checks to make sure that staff are not carrying computers, peripherals or consumables off the site without authorization. Position microcomputers so that they are not visible from public areas or not easily accessible. [6][7][8][13]
6. Verify UPS functions properly when electricity fails or voltage variations. UPS is free of the electricity load relating to the tube-lights, fans, etc. Power supply to computer equipment is through UPS system only. [6]
7. Keep frequent backups of critical data and essential software. Support staff should keep records of software authorized for use on each machine and undertake spot checks to ensure that staff is not using unauthorized software. [10][13]
8. Periodic review of security controls, System authorization should be done properly, Data cryptography, Do system audit. [21]

Common Vulnerabilities of Network Devices

1. Access to the network by unauthorized persons [14]
2. Inadequate Cabling Security [4]
3. Information can transfer outside of the organization
4. Open Physical Connections, IPs and Ports [14]
5. Anyone with a wireless device can connect to wireless network, if it is not secure
6. Routers with the encryption features turned off [17]
7. Default password of router is not changed [17]
8. Router is turned on when you don't use it [17]
9. Poorly configured wireless access points can compromise confidentiality [17]

Threats of Network Devices

1. Deliberate Acts of Espionage or Trespass [14][15]
2. Information Leakage [13]
3. Information Leakage [13]
4. Information Leakage [13]
5. Unsecured Wireless Access Points [16]
6. Information Leakage [13]
7. Misuse of Software, Data, and Services [6][7][8]
8. Hacking [17]
9. Deliberate Acts of Espionage or Trespass [15]

Countermeasures of Network Devices

1. Use Strong Authorization. Use tamper-resistant protocols across communication links. [14]
2. Do not route network cables through areas that are accessible to the public. Use locked cable trays [13]
3. Monitor the usage of lines to which modem is attached. Disable modem lines outside working hours. [13]
4. Disable unused protocols and unnecessary ports. [14]

5. Use Strong Authorization
6. Manufacturer often deliver wireless routers with encryption features turned off. You must turn it on. [17]
7. Change your router's pre-set password for administration. Change password according to your organization's policy. Enforce password management. [18]
8. Turn your router off when you are not using it. [17]
9. Eliminating rough access points. Properly configuring all authorized access points. [17]

Common Vulnerabilities of Software's

1. Unclear or incomplete specifications for software development [4] [12]
2. Poorly documented software [12]
3. No or insufficient software testing [4][12][14]
4. Lack of authentication & identification mechanism [4][12]
5. No 'logout' when leaving the work station [14]
6. Lack of audit trail [14]
7. Well known flaws in the software [12][20]
8. Wrong allocation of access rights [12]
9. Inadequate or irregular backup [4]
10. User rights are not reviewed regularly [4]
11. Lack of access control policy [4]

Threats of Software's

1. Software Malfunction, Act of Human Error or Failure [12]
2. Act of Human Error or Failure [12]
3. Denial of Service [12][14]
4. Network eavesdropping, Brute force attack, Dictionary attack, Cookie replay attack, Credential Theft, Forging of rights [12][14]
5. Cookie Replay Attack [14]
6. Repudiation [14]
7. Technical Software Failures or Errors, Deliberate Software Attacks [4][12][20]
8. Denial of actions [12][23]
9. Deviations in Quality of Service by Service Providers [15]
10. Elevation of privilege [14]
11. Exception Management (Denial of Service) [14]

Countermeasures of Software's

1. Specification for the development of software should be clear and complete. It should not contain ambiguity.
2. Ensure the documents of software are properly written. Document should describe the content and purpose of the document.
3. There should be a separate test plan. Use common testing problems as a checklist. Ensure the availability of testing experts. [14].
4. Use authentication mechanisms that do not transmit the password over the network such as Kerberos protocol or Windows authentication. Make sure passwords are encrypted (if you must transmit passwords over the network) or use an encrypted communication channel, for example with SSL. Use strong passwords that are complex, are not regular words, and contain a mixture of upper case, lower case, numeric, and special characters.
5. Use an encrypted communication channel provided by SSL whenever an authentication cookie is transmitted.
6. Use a cookie timeout to a value that forces authentication after a relatively short time interval. Enforce account lockout for end-user accounts after a set number of retry attempts. Allows the user to choose to not save credentials, or force this functionality as a default policy. [14]
7. Use a cookie timeout to a value that forces authentication after a relatively short time interval. System logs out automatically if the user is inactive for a specified time [14]
8. Create Secure Audit Trails. Use Digital Signature. [14][22]
9. Stay current with the latest operating system service packs and software patches. Block all unnecessary ports at the firewall and host. Disable unused functionality including protocols and services. Harden weak, default configuration settings [14]
10. An access control policy shall be established, documented, and reviewed based on business and security requirements. Ensure that users' access rights should review at regular interval using a formal process. [6][7][8]
11. There should be a regular contract for maintenance of the UPS and the preventive maintenance is carried as per contract. The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS. UPS is free of the electricity load relating to the tube-lights, fans, etc. UPS functions properly when electricity fails. [6][24]
12. Enforce least privileged service account to run processes and access resources. Log Critical application level operations. Use platform-level auditing to audit login and logout events, access to the file system, and failed object access attempts. Back up log files and regularly analyze them for signs of suspicious activity.
13. Thoroughly validate all input data at the server. Use exception handling throughout your application's code base [14]

Common Vulnerabilities of Data

1. Disclosure of information either accidently or deliberately either verbally or in writing to any unauthorized person or organization [25]
2. Writing down passwords and sensitive data [3]
3. Emails containing maliciously-crafted attachments [24]
4. Misappropriation of scanned photo and signature [2]

Threats of Data

1. Deliberate Acts of Espionage or Trespass, Deliberate Acts of Theft, Deliberate Acts of Information Extortion [15]
2. Spoofing user identity [14]
3. Phishing [24]
4. Spoofing [2]

Countermeasures of Data

1. Ensure that personal information is retained only for the period of time for which it is required. Ensure that access to personal data is restricted only to authorized persons. Ensure that all personal data is obtained for specified purposes and only processed for those purposes. Avoid giving personal data by telephone. Ensure that accurate, up-to-date personal details are provided to the University and notify the University immediately of any changes or errors. [25]
2. Do not store secrets in plaintext. Do not pass credentials in plaintext over the wire. Ensure that sensitive information is deleted or destroyed appropriately. [3][14]
3. Organization should install professional enterprise-level e-mail security software. Software should check both incoming and outgoing messages to ensure that spam messages are not being transmitted. Organizations should provide regular internet security training to staff to ensure user- awareness about e-mail scams. Delete suspicious e-mails. Report any potential incidents. Look for digital signatures. Ensure anti-virus software and definitions are up to date. Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses. Do not open suspicious e-mails. Do not click on suspicious links or attachments in e-mails. Do not call telephone numbers provided in suspicious e-mails. [18] [24]
4. The scanned photo and signature must be kept as a PDF file and stored in a restricted folder. Document must be protected where signature is saved. [2]

V. CONCLUSION

Information threat leads to great financial losses. Educational sectors are struggling against security attacks.. This paper shows the potential threats to information systems of online admission systems also presented countermeasures for the vulnerabilities and threats associated with online admission systems. Implementing the countermeasures in organizations help organization to protect their information's assets reduce security vulnerability and threats.

REFERENCES

1. Abdullah Alshboul, "Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks", Communications of the IBIMA, vol. 2010, Article ID 486878, 9 pages
2. Lesley Barrington, "Use of Scanned Signatures Procedure, Information Security Suite of Policies", Southern Health NHS Foundation Trust, Version 1, July 2015
3. "HyperCourseware Vulnerability Report CMSC498N: Seminar in Cybersecurity: Secure Maryland", University of Maryland College Park, April 7, 2014
4. Dejan Kosutic, "ISO 27001/ISO 22301 Knowledge Base Catalogue of Threats and Vulnerabilities", http://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/27001 Academy
5. "Information Technology Threats and Vulnerabilities", http://www.hq.nasa.gov/security/it_threats_vulnerabilities.htm
6. RBI,DBS;CO, "Checklists for Computer Audit, https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/33400.pdf
7. "Cisa Review Manual 2010", ISACA, 2010
8. ISO 27001: 2013 transition checklist, http://www.nationalwatermission.gov.in/sites/default/files/ISMS%20Checklist.pdf
9. "The need for security", https://www.utica.edu/faculty_staff/qma/needforsecurity.pdf
10. "Countermeasures against Information Leakage, Information-technology Promotion Agency", IT Security Center, July 1, 2014 Seventh Edition
11. "Securely Disposing of Computers and Other Storage Devices", The SANS Institute, January 2011
12. "Document on Examples of typical threats", http://wireless.ictp.it/school_2015/presentations/secondweek/IoTSecurity_document.pdf
13. "Information System Security Review Methodology, A Guide for Reviewing Information System Security in Government Organizations", ISSAI 5310, Issued by EDP Audit Committee, International Organization of Supreme Audit Institutions, October 1995
14. "Improving Web Application Security: Threats and Countermeasures", June 2003, https://msdn.microsoft.com/en-us/library/ff648641.aspx
15. Michael E. Whitman, "Enemy At The Gate: Threats To Information Security", COMMUNICATIONS OF THE ACM, August 2003/Vol. 46, No. 8
16. Ateeq Ahmad, "Type of Security Threats and It's Prevention", Int. J. Computer Technology & Applications, Vol 3 (2), 750-752, ISSN- 2229-6093
17. Min-Kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities,

Threats & Countermeasures", International Journal of Multimedia and Ubiquitous Engineering, Vol. 3 No. 3 July 2008
18. "Cybersecurity Awareness Course Library: Common Cyber Threats: Indicators and Countermeasures", http://cdsetrain.dtic.mil/cybersecurity/data/pdf/Common_Cyber_Threats_Indicators_and_Countermeasures.pdf
19. "All-of-Government Risk Assessment Process: Information Security", February 2014
20. LAITH T KHRAIS, "Highlighting the Vulnerabilities of Online Banking System", Journal of Internet Banking and Commerce, December 2015, vol. 20, no. 3
21. Manpreet Chandhok, Oyediran Oyepeju, Chisanga Mkasanga, Joy Das, "Management Information Systems Strategy and Security Risks", University Student Record System Report University of Bedfordshire
22. "Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds Reserve Bank of India" https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
23. Mohammed Rafiq, "Database Security Threats and Its Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, ISSN: 2277 128X
24. "Data Security: Top Threats to Data Protection", Privacy Technical Assistance Center, Dec 2011
25. Ulster University, Data Protection Policy - 2014/15