International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 11, November 2017

ISSN: 2394-4404

Trends In Information System Security In Universities

Daniel Otanga

Dr. Samuel Mbugua

Kibabii University College

Abstract: ***Information system security is designed for critical information protection. Security in Information systems is a complex of organizational technical and legal measures that are used to protect information from unauthorized modification and unauthorized access. Due to dynamic changes in Information Technology (IT), new threats and vulnerability emerge and thus the need to consider appropriate approaches that can address the emerging security issues. This paper examines the trends in information system security in universities and seeks to explore the current security approaches in universities with a view of establishing effective security approaches. Through scrutiny of literature on trends in information system security, the paper presents the findings of the security approaches trends identified. The paper also attempts to forecast the future trends in information system security in universities and its implications to the level of information security requirements in the universities. Information security must be checked continuously to maintain the required security level in universities.***

Keywords: ***Information System Security, Information Technology, Trends, Approaches, protection, Threats, Vulnerability.***

I. INTRODUCTION

The current trends in Information Technology has seen Information System and devices integrated into every fiber of universities (JUCC, 2012). In their newsletter for IT professionals the JUCC noted that IT security had become the most important elements to ensure the integrity of universities information systems and resources. The newsletter enumerated some of the recent development in IT as Mobility, Lower Cost, Newer standards, mobile computing, cloud computing and IPv6.According to Miramare, (2010) mobile computing is a computing system in which a computer and all necessary accessories like files and software are taken out to the field.

Miramare, (2010)observed that scientists use mobile devices and web-based applications to systematically explore scientific aspects of their surroundings, ranging from climate change, environmental pollution to earthquake monitoring among others. The mobile revolution has enabled new ideas and innovations to spread out more quickly and efficiently at the same time creating security issues. According to Educause, (2011) Mobile devices have similar privacy issues as other online technologies. However, location-enabled mobile apps create an entirely new set of security issues on campus. Each of the listed technology has created security issues which are unique to their operational technology and thus the need to address the security for each individual technology as it arises.

Emerging trends in IT which includes but not limited to cloud computing and an increase in mobile devices connecting to corporate networks are prompting companies to review their IT security strategies (JUCC, 2012). Mobile computing according to Honicky, Palous and Brewer, (2010), is the technology which is emerging as a next generation significant tool for computing and has a tremendous impact on field of education and research of our society. Theft or loss of mobile devices means potential leakage of sensitive data related to personal identification, confidential material and financial information. By allowing staff or students to use hand held mobile devices to conduct academic research or administrative tasks, the impact on universities due to theft/loss event will become much more significant.

Cloud computing is a set of IT services that are provided to a customer over a network on aleased basis and with the

ability to scale up or down their service requirements. (Kuyoro, Ibikunle & Awodele, 2011). Usually cloud computing services are delivered by a third party provider who owns the infrastructure. According Kuyoro, Ibikunle & Awodele, (2011), Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing. These activities which occur in virtual networks and involve various users with varying applications as a result create security issues in organizations where such activities are applied.

Security in cloud computing is associated with issues such as data loss, phishing, botnet. According to Kuyoro, Ibikunle & Awodele, (2011), the security issues in cloud computing are as a result of putting your data, running your software on someone else hard disk using someone else CPU. Multi-tenancy model and the pooled computing has introduced new security challenges that require extra technology to tackle, hackers can for example use cloud to organize botnet as cloud often provides more reliable infrastructure services at a relatively cheaper price to start an attack (Ramgovind, Eloff, and Smith. 2010). Due to technology of using virtual systems where a system can be accesses remotely, a platform can be created to attack the systems or processes within the cloud. Users can not be guaranteed security of their data because they are not in control of the platform which is hosting them.

For mobile computing, the miss-configured wireless networks present a security hazard. Anyone with a wireless computer could have full access to a LAN unless restrictions are implemented (McKimmy, 2003). The university LAN contains sensitive information which should be guarded to avoid access by unauthorized people however there are challenges on how to deal with people using mobile devices to share resources on the network.

Due to application of emerging information communication technologies, ICT systems are now the basic core and reservoir of information in organizations (Bigioni, nd). The current generation of information systems is based on the internet which raises worrying security issues (CERT). Bigioni, (nd) further noted that the spread of wireless radio connections has opened new attack fronts. Due to varying needs of information systems users in universities, different applications are performed by users using their mobile devices which are integrated with the university information systems. This opens up security loop holes which if not detected and addressed can be detrimental to the universities information systems.

Security issues in mobile computing according to Goswamiet al, (2013) consists of confidentiality, Integrity, Availability, Legitimate, and Accountability. He noted that wireless networks have relatively more security requirements than wired networks. Advancement in technology is leaning much on mobile computing and cloud computing and as such organizations adopting the evolving technology must ensure that they adjust their security approaches and establish information security framework to match the security challenges brought as a result of the evolving technology. According to Goswamiet, (2013) mobile computing technology which is among the new emerging technology enables mobile personnel to effectively communicate and interact with fixed organizational information system while remaining unconstrained by physical location. The organizations information system may be having its internal security structure which must be harmonized by the external security brought about by the mobile devices. A survey by Symantec found out that mobile computing was the most risky program launched by companies with nearly quarter characterizing the level of exposure as high or extremely high (Symantec, 2012).

According to Will Pro, (2012), There are seven areas of security that companies must ensure to address as a core of a successful, comprehensive mobility program, these are; Data encryption, Password enforcement, Device management, Compliance and configuration management. Data access, Trust and confidence and enabled and ease of use. He noted that if the named factors are put in place, then a company's mobile computing program will achieve more than increased security. Will Pro further noted that whether running Android, iOS, Windows phone or another platform, measures can be taken to increase security on smartphones. Mobile devices are distinct from laptops and therefore require a specifically tailored approach to security. Bring Your Own Device (BYOD), Technology varied mobile devices with different applications are brought into universities and used by staff and students alongside the university information system. This process has brought security challenges which require university administration to deal with security of individual mobile devices that access its information system.

II. VULNERABILITIES IN MOBILE SYSTEMS

Vulnerabilities are weak points in a system which can be exploited to attack the system. According to Wanja and Anapam, (nd) security is much more difficult to maintain in mobile ad Hoc networks than in wired networks. Some of the vulnerabilities outlined by Wanja and Anapam include lack of secure boundaries, threats from compromised nodes, lack of a centralized management facility, restricted power supply and scalability. Based on the vulnerabilities outlined it can be noted that mobile networks are not safe; there is no clear line of defense because of the freedom for the nodes to join, leave and move inside the network; the nodes can be compromised by the adversary and thus perform malicious behaviors that cannot be detected. Lack of centralized management can cause problems when coordination is required; continuously changing scale of network has set requirement to the scalability protocols and services in mobile systems. Therefore the mobile systems will need more robust security scheme to ensure the security of the network.

III. APPROACHES TO INFORMATION SECURITY

ENISA concentrates on issues of raising information security awareness, Computer Emergency Response Teams (CERTs), identity, privacy and trust as part of information security in general, reliable communications networks and services, and information security risk management. Access to LAN by unauthorized mobile devices can be prevented by establishing Message Authentication Code (MAC) addresses,

a unique number that identifies its Network Interfacing Card (NIC). Unknown computers can then be denied access if their MAC address is not on an authorized list (McKimmy, 2003).

For cloud computing, service providers provide different levels of protection against data loss or corruption, According to Taiwhenua, (2014), some of the protection include data backup services. The use of cloud services may need an agency to develop implement and test its own data backup strategy to ensure that it can sufficiently recover from an incident that result in data loss or corruption, (Taiwhenua, (2014). According to Taiwhenua, (2014) agencies maintain a robust process for managing the lifecycle of identities that ensures;

Permissions are approved at the appropriate level within the organization.

Role Based Access Control (RBAC) is sufficiently granular to control permissions.

Users are only granted the permissions they require to perform their duties.

Users do not accumulate permissions when they change roles within the organization.

User accounts are removed in a timely manner when employment is terminated.

The above listed processes can form a security framework which can take care of the environment and the organizations management approach on handling users of mobile devices with different needs and applications on organization networks. A comprehensive security policy could be necessary to take care of all the process listed. Due to the mobility of the nodes and the continuously changing topology in the ad hoc network, it becomes difficult to collect reasonable evidences for a node if it only relies on the single-layer detection method, where it may be vulnerable for the setting of the threshold. As a result, the concept of multi-layer or cross-layer detection mechanism can be utilized as noted by Zhang, (2000) and Lee, (2000). This concept can address the dynamic structure of nodes in the ad hoc networks

Other security approaches in cloud computing as noted by FBI, (2012) include; Access can be restricted to the email payload for cloud mail through the use of end-to-end encryption. This process however it was observed that it would limit the cloud services ability to perform some recovery or protective services due to email inaccessibility. The technical report by FBI also noted that Cloud storage solutions may allow end-to-end encryption using user held cryptographic keys.

IV. THREATS TO MOBILE DEVICES

Threats to mobile devices include malware, loss or theft, communication interception, exploitation and interception (Juniper Networks, 2011). Witheres (2012) observed that, Mobile Device Management (MDM) offers features to assist in configuring mobile devices such that they more closely comply with usage policies. Withers, (2012) noted that a list of features available in MDM can include remotely locking and wiping lost or stolen devices, application management, password enforcement, inventory and asset management, security and policy compliance, remote location of lost devices, integration with enterprise services such as e-mail and certificate authorities, backup and restore services. This in essence can ensure university data is not exposed to unauthorized people. A variety of MDM solutions are offered by vendors, with a diversity of architectures and specifications.

V. SUMMARY

ICT innovations are dynamic and thus driving the current trends in IT bringing enhanced functionalities, simplified operations and improved IT cost-effectiveness. This gives rise to more complex or unknown risks of IT that have an impact on IS security strategy in universities. To cope with the dynamic nature of IS risks, universities need to adopt a more proactive approach to assess the security risks of IS trends and strengthen the IS security implementation by utilizing updated techniques and management approaches. This can only be possible if the university is able to establish its security concerns and develop a framework which can address such concerns. Every organization's approach to security should be comprehensively tailored in a way that strikes a balance between its business needs and sensitivity of its data.

REFERENCES

[1] Bigioni, nd, The ICT security issues and trends
[2] Educause, (2011); The future of Mobile Computing EDUCAUSE webinar
[3] Federal Bureau of Investigation; (2012) - Criminal Justice Information Services (CJIS) Security Policy, Version 5.0, Technical report
[4] Guswamiet et al (2013), Limitations of mobile Computing; International Journal of Advanced research in Computer Science and software engineering
[5] http://www.juniper.net/us/en/local/pdf/whitepapers/2000372-en.pdf*006)*, Las Vegas, Nevada
[6] Jim Parker, AnandPatwardhan, and Anupam Joshi; (2006). Detecting Wireless Misbehavior through Cross-layer Analysis, in *Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC'2*
[7] JUCC, (2012); Trends in IT Security; A newsletter for IT Professionals, issue 13
[8] Juniper Networks. (2011). Mobile Device Security - Emerging Threats, Essential Strategies. Key Capabilities for Safeguarding Mobile Devices and Corporate Assets. Retrieved from
[9] Kuyoro, Ibikunle & Awodele, (2011); Cloud Computing Security Issues and Challenges International Journal of Computer Networks (IJCN), Volume (3) : Issue (5)
[10] McKimmy, P.B. (2003). Wireless mobile instructional labs: Issues and opportunities. International Journal of Instructional Media, 30 (1) :111
[11] Miramare, (2010); mobile computing: the emerging technology, Sensing, challenges and applications United Nations Educational, Scientific and Cultural Organization and International Atomic Energy Agency *of the 6th*

International Conference on Mobile Computing and Networking Boston, Massachusetts,

[12] R J Honicky, Eric Brewer, and Eric Palous (2010), "Towards a societal scale scientific instrument" published in "m-Science sensing, computing and dissemination" Editors: E. Canessa and M. Zennaro, ICTP ICTP Science Dissemination UnitSymantec White Paper, (2012) State of Mobility Survey,

[13] S. Ramgovind, M. M. Eloff, E. Smith. (2010). "The Management of Security in Cloud Computing" InPROC 2010 IEEE International Conference on Cloud Computing

[14] Taiwhenua, (2014); All-of-Government Cloud Computing, information security and privacy consideration

[15] Will Pro, (2012); Basic Principles for Increasing Security | htcpro.com

[16] Withers, S. (2012). Mitigating mobile information security risk with mobile device management (MDM) Retrieved from http://www.voiceanddata.com.au/articles/52333-Mitigating-mobile-informationsecurity-risk-with-mobile-device-management-MDM

[17] Y. Zhang and W. Lee, (2000) Intrusion Detection in Wireless Ad-hoc Networks, in *Proceedings*