DEVELOPING A HOLISTIC NETWORK SECURITY ARCHITECTURE, THAT IS FOCUSED ON BUSINESS GOALS, TECHNICAL NEEDS AND SYSTEM USERS FOR BUSINESSES IN KENYA.

Githinji, Stanley Muturi
Lecturer, Faculty of Computing and Informatics
Kenya Methodist University, 45240 - 00100, Nairobi, Kenya
Tel: +254- 0721250516, Email: Stanleygithinji@yahoo.com / Stanley.githinji@kemu.ac.ke

Abstract

Securing the information systems is not the goal of the security policy the goal is to secure the business. That is any practice or procedure that threatens the confidentiality, integrity, and availability of organization information should be guarded against within Network Security Architecture. Security managers can't stop web 2.0 technology; users now depend upon these new applications for business benefit, personal communication, and entertainment. It is too late for security managers to advocate blocking this traffic altogether. This research found that 60 % of business security attacks are from internal and there is an increased need for web 2.0 applications at 70 % in the next two years. This research provides a holistic network security architecture that will guide businesses in the process of developing a successful well-formulated security architecture that is focused on business needs, technical needs and users who according to this research are the key stakeholders on success of proper implementation of NSA and security policy for medium and enterprise organization.

Keywords: *NSA, Web 2.0, CIO, IT, DMZ, IPS, IDS*

Introduction

Background

Business applications security products have one fundamental strict security "allow or deny" access metaphor. This may be appropriate for dealing with malicious code, but there may be a middle ground here where they are not applicable. Securing network application and enforcing on policies and procedures demands an end-to-end network security architecture (NSA) strategy across the enterprise.

NSA is a subset of network architecture specifically addressing security relevant issues. It is a security technology architecture, which is closely related to Information Technology (IT) architecture, and it's a desired structure of an enterprise's technology components and technical safeguards. With security technology architecture in place, an enterprise has a framework for more informed decision making and a guide for ongoing planning, design, and implementation activities. Network security mechanisms, such as network firewalls and network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), are generally a convenient and scalable point to apply security controls and are an important locale for defining chokepoints zones. Zones define logical or physical boundaries around a group of systems, for the De Militarized Zone (DMZ) pattern in web applications. Checkpoints define places to cross boundaries into and out of zones, where special security considerations are applied.

Research Objective

i. To determine how business are adopting web 2.0 applications.
ii. To determine security challenges that business are facing as a result of Web 2.0 technology.
iii. To develop a holistic Network Security Architecture for that is focused on business goals, technical needs and system users for businesses in Kenya.

Scope and Limitations

The researcher targeted small, medium and large organizations that have adopted information technology in their organization work flow. The research respondents will be chief information officer (CIO), senior IT managers and system administrator who are involved in implementation, managing and securing business applications.

The major limitations in this research was that the questionnaire contain sensitive questions on security setup of organization and respondent may think that the researcher is performing social engineering by trying to understand their security setup. The researcher made it optional for respondent to indicate their organization details.

Materials

Network security architecture has in the past been studied by various groups of network engineers and interested network security companies. Today network security design flaws are almost awakening for many organizations.

According to Avizienis, Laprie, Randell, and Landwehr (2004), security encompasses the aspects of availability, confidentiality, and integrity. The main attributes of dependability are availability, reliability, safety, integrity, and maintainability.

Web applications are already in widespread use and are here forever so it is important to understand how these systems impact IT assets like the network. It turns out that the effect can be quite profound. Web 2.0 applications such as facebook, twitter, and youtube can greatly influence network security and performance because of unpredictable traffic patterns and added vulnerabilities as new applications bridge the un-trusted outside world and the internal network.

According to enterprise strategy group (2009), the key to managing new Internet applications is providing secure access to the right employees while controlling bandwidth utilization. These are dynamic activities that can change on a moment's notice based upon characteristics like where the employee is physically located and what other traffic has bandwidth priority. The NSA can accommodate these kinds of requirements.

The reality is that existing enterprise security architectures continue to have gaps and vulnerabilities. Well established best practices and countermeasures fail to provide the highest levels of protection for many businesses. According to IDC (2008) enterprise security survey, over 50% of participants executives were only somewhat confident or not confident in their security systems. The consequences of a single breach in security can have several and lasting effects on a business.

The impact of an event can damage an enterprise's reputation and credibility. In turn, customer retention suffers. The direct financial impact of a security breach can be substantial. The costs of forensic analysis, employee downtime, and staff time and labor to remediate the effects of a breach are significant. According to Strong and Volkoff (2004) , The organizational aspects involved in the implementation of an enterprise system have been presented as presented in informal roadmap for enterprise system implementation highlighted the key processes involved and by identifying the challenges that need to be managed in the course of implementation.

Methods

This study employed a descriptive survey that was conducted targeted CIO, IT Managers and system administrators. The research was done in four phases:

I. Data Collection
II. Data analysis
III. Development of Holistic NSA
IV. Conclusion and Further Research

Data Collection instrument for this study was a questionnaire. The main aim was to capture the views of the respondents who are involved in development and implementation of business applications. They filled in questionnaires that contain open ended and closed ended questions.

Results

This research focused on development developing holistic NSA that is focused on business goals, technical needs and system users for businesses in Kenya. Respondent views and preference will be used to design holistic NSA. Respondent to this research were CIO, IT managers and System administrators. The results of this study were presented based on the various items asked.

Study findings indicated that 65 % of business security threats are from inside the organization while 35 % are outside threats. 61 % of businesses plans planned to adopt web 2.0 technology in the next 24 months and only 60 % of the res[pendent shared their security vision with software and hardware vendors,40 % of the respondents adopt technology without sharing their security plans during request for proposals.

The researcher found that the major security challenges that business are facing today are from internal threats at 60 %. There is also increased bandwidth demand as most of organizations have already using web 2.0 applications in various work flows skype and IT telephony having highest users. The research found that only 65 % of the respondent determines application bandwidth utilization. According to this survey twitter and linkedIn are the major social networking sites that business has allowed staff to access and only 10 % of businesses that don’t allow any of the social networking sites.

There is also a security gap between businesses and vendors who are supplying IT equipments, 40 % of respondent indicated that they don't share their IT security vision with vendors. This may results to cases where by business are procuring IT equipments that don't meet business security needs.

Organizations are bound to move to development of NSA as security managers may not stop Web 2.0 applications. They are also not aware of user requirements, business requirements and appropriate security technologies to counter inside attacks. Organizations need to include system users in security implementation plans for them to have a secure system and minimize internal attacks.

Web 2.0 application have fundamental problem that all security managers adhere to a strict security "grant or deny" access rule. Controlling the use of Web 2.0 applications is not an issue of security alone but it requires an end to end approach that will require integrations of organizational level, workflow level, informational level, technical level and system user level.

Holistic Network Security Architecture

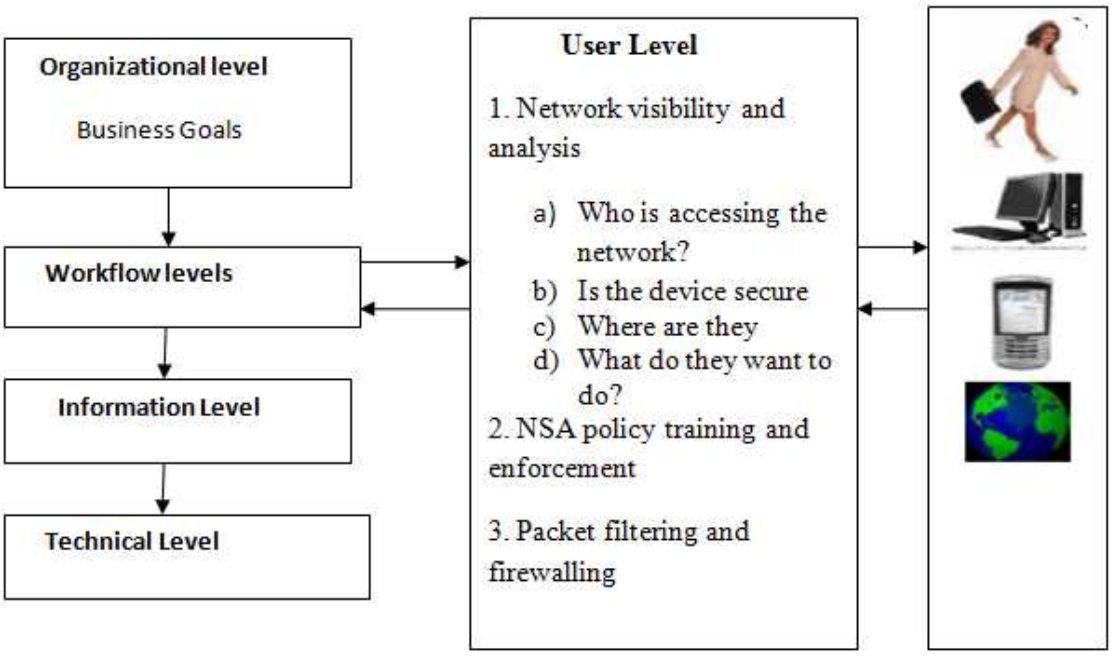

Figure 1: *A holistic Network Security Architecture Source*, S. Githinji, 2014

Explanation of Holistic Network Security Architecture

There are five levels of security architecture as shown in figure1 above. At organizational level, security strategies are developed and a corporate security culture has to be established. The workflow level entails day-to-day core business processes need to be aligned with the company's security strategy applications that businesses have adopted. At information level security managers need to determine which information they need to protect and technical infrastructure needs required securing applications and system users the fourth level is technical level encompasses aspects such as network security, Internal firewalls, IDS,IPS, antivirus software and hardware dependability.

Security at fifth level user levels encompasses network visibility and analysis determining who is accessing the network and where are they from? Determining whether the devices that they are using to connect to business applications are secure. Determining what they want to do when they gain access, IT security policy training and enforcement should also be done at user level.

Web 2.0 Technology is very dynamic and some security technologies that business will adopt now will be overtaken by technology, the researcher calls for continuous review of security technologies on new internet application and how to secure against outside attacks as from the survey there is still 40% of external attacks. There is also need for continuous improvement of holistic NSA at all levels to ensure that organizations security needs at met all levels.

Conclusion and Recommendations

A comprehensive NSA must focus on business goals, workflow requirements, information level, and technical level. Technical mechanisms include things such as firewalls, intrusion detection, access control lists, and filtering routers. More emphases need be addressed at the user level include as they are the main people interacting with business workflow level.

Organization's NSA is only as good as the policies and procedures designed to maintain it at user level, and such policies and procedures must also be put into practice If security managers, developers, and users are not aware of such architectures, policies and procedures, they will not be effectively executed hence compromising on overall system security. Key importance for security managers in implementation and assurance of information security is the establishment of a holistic Network Security Architecture as granting and denying access to users or installing latest firewalls may not stop insider or outsider attacks; rather, it requires a complete end-to-end solution called holistic Network Security Architecture.

This research will enable organization to proactively secure network application and enforce on security policies and procedures using NSA strategy that are focused on business goals, technical needs with increase in demand for web application.

REFERENCES

Anderson, R. (2001). *Security engineering: A guide to building dependable distributed systems*. New York: John Wiley & Sons Inc.

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions of Dependable and Secure Computing, 1*(1), 11-33.

Bingi, P., Mir, A., & Khamalah, J. (2000). The challenges facing global e-commerce. *Information Systems Management, 17*(4), 26-34.

Enterprise Security Group. (2009*). NSA Meets Web 2.0.* Retrieved June 12, 2011, from http://www.juniper.fr/us/en/local/pdf/whitepapers/esg-nsa-meets-web-2.0.pdf

IDC. (2008*). Uncovering the Hidden costs of Spam in the Enterprise.* Retrieved June 9, 2011, *from http://www.ngtafricasummit.com/media/whitepapers/Symantec_NGTAFR.pdf*

Strong, D. M., & Volkoff, O. (2004). A roadmap for enterprise system implementation. *IEEE Computer, 37*(6), 22-29.