Architecture: Security Infrastructure

Name

Institution

Professor

Date

Architecture: Security Infrastructure

Security Infrastructure System

According Comizio, Dayanim & Bain (2016) information security system includes the firewall, routers, and proxy servers. The most common attack on this layer is the Denial of service attack which involves flooding the connection point to the outside world with unproductive traffic bringing communication with the internet to a halt. A firewall is located between a network of computers and the internet to protect the computer systems from threats posed by an internet connection. It prevents unauthorized access to the system it is configured to protect.

 Routers are used to connect different networking segments forming the backbone of the internet. They operate by examining each received packet and use algorithm to determine the optimal path for data to reach its destination. To prevent security risk for routers, use of strict passwords and encryption communication when accessing a remote router is recommended. A proxy service firewall acts as a go-between the internet and the internal network of computers and is placed between the two environments. Proxy service ensures internal client computer do not interact directly to the outside resources.

Switches are the backbone of most Ethernet based local networks. They are more efficient than hubs since each port on a switch is a separate collision domain. Administrative access to switches must be controlled using passwords and enhanced communication protocol for remote access.

Host Protection

This ensures protection from threats from the internal workstations connected to the network. The threats include attack from within or attack on data by someone coming through the firewall. Formulating and implementing User Access Policy, updating regularly the patches for the workstation operating system, limiting the Network Resources Access from workstation, and installation and update of anti-virus are some of characteristics relating to workstation security.

Data Protection

Having different passwords for different accounts as well as enabling encryption for all laptops and desktops are all precautionary steps in information security. Implementation of security policies, processes, procedures, and products does not achieve security but reduces the likelihood of security failures to occur.

Physical threats

Physical threats predisposed to computer systems could be intentional, accidental and even natural. Considering the computer systems installed in a busy facilities such as a banking can be great affected by physical threats leading to damage of the storage facility, network connectivity and limiting the readability and effectiveness in delivering the services. It requires the establishment of physical security control measures. These physical threats range from internal, external or human. The potential physical threats includes fires, vandalism and theft, unstable power supply, floods and earthquakes, humidity level in the building, and intentionally generated errors from unauthorized access of the systems. Insider fraud is a stint consigned to a wide range of criminal activities committed by the banking workers or service provider, and normally falls into three groupings: theft from clients, theft from the organization, and exploitation of position. It is an emergent problem amongst business organizations. In addition, the integration of a third party in the banking premises is critical to virtually all business corporates, as significant they are, third parties expose firms to a wide variety of hazards (Kenney, 2016). It is particularly factual when it moves toward accessing key organization information and their imperative roles to sensitive matters of functions and critical projects to a business.

The development of a new payroll architecture system which covers multiple distance depend on the Wide Area Network so as to connect numerous smaller networks which includes local area network (LAN) or metro area networks (MANS). The WAN is created to allow the development of a payroll program for large organization that will serve the entire nation (USA). It only requires a small amount of data sets to help an engineer visualize the needs of an organization in the case of a system failure which are controlled remotely and separated from the rest of the system. Through architecture, it is possible for each organization to develop own payroll systems in consideration of their specifications.

The construction of a payroll program to facilitate the services of a large organization with widespread branches in the Unites States of America has significant changelings. Considerably, the administrator must select the appropriate application of architectural design to determine all the drawbacks experienced in the previous design system. On the other hand, the organization must have an extensive data center which connects to all offices via WAN. Therefore appropriate architecture to be applied in such a scenario requires a WAN diagram to facilitate project management and foster system documentation. Documentation of the information technology architecture will provide an enhanced visual illustration of the system network. It is primarily the function of a WAN to create a link between the local area networks of the offices spread across the USA.

In reference to the payroll program, the crucial elements are centered on the application of appropriate architecture that is effective in serving the purpose of the present situation. All requirements proposed by the organization must be met effectively. As such an effective system would help in the combination of all architectural elements and designs which are elastic, cost-effective, and technically sound so as to sustain and manage the organizations information needs. A comprehensively built payroll program proposed in the use case scenario will prompt increased speed and accuracy in the processing of wages. Automation of the system will significantly reduce error occurrence often experience in the employees’ checks, prompt efficiency and ease paperwork needed for information management.

Payroll software is a program that offers platform for the organization to easily access information concerning the employees, spend buildings, spend intervals and also inform on the daily registry of the workers. The payroll system makes its easier for the accountants to determine compensation as agreed by payment rate intervals; it is easier and efficient to create a structured paycheck.

The construction of high-end payroll software needs to be included in the resource planning of a larger enterprise to source an integrated software package tailored to serve the needs and demands of the subjective organization (Lokuge, Sedera & Grover, 2016). A payroll program is part of wider scope system, similar but superior to ERP which can be supplied by only one vendor (administrator) (Bradford, 2015) Considerably, it is a constituent of the HRMS, which is integrated with the financial systems that results creation of customized interfaces in the diverse systems.

Graphical Representation

Potential ethical issues

This could go a long way compromising and exposing the organization to numerous risks and violation to right to information privacy. Tentatively, change is proactive. In this respect, the introduction of a newer system will bring in new developments within the organization and some quarters may feel violated or compromised. When the architecture of the payroll program is outsourced, while in the previous time, the system was developed internally it brings in the question of job loss and if the corporate is doing enough to foster employee development through initiation of training programs to acquire appropriate skills.

Potential Logical Threats

Considering the probable high number of consumers seeking services and access to the banking premises and in reference to the computer systems there are preferential security vulnerabilities. For the banking to deliver to the consumers need there is huge dependence on the computer system to retrieve patient’s information and get advice on certain health conditions. To achieve the effectiveness in delivering services it requires the logical access of the systems in providing guidelines and technical control of information needed to utilize, running programs and modifying patient and the premise information. However they are prevalent challenges logical threats that include Trojan, spyware, denial of service attack, phishing, and worms.

Trojan

It refers to malicious activities subjected to the computer software and significantly affects system files. Trojan causes disruption of the business operations which exposes a computer system as it takes the form of legit software that could cause impressive but gradual harm. According to Cappelli et al. (2012), the Trojan facilitates the capturing of crucial log in details such as the password and username; thus sending malicious URLs to other computers. The infection is the directed to other computers within reach and could result to harm of extensive files and eventually leading to congestion in the systems connection. Further, it can lead to financial treats as the banking will depend on the internet to facilitate payment and access business emails.

Cybercrime Policies

In the apparent evolution of information age guided by technological advancement extensive research is now focused on developing ways and policies to deal with a real problem threatening the information management sector. The emergence of new interaction platforms and the institution of technological systems to control most of our process in order to bring effectiveness and efficiency (Wilson, 2003). However, that endeavor has continued to expose the codes of information technology due to increased cases of cyber-attacks targeting large corporations and institutions with a malicious intent of accessing the systems using unauthorized means. Subjectively, the world is faced with a new challenge especially to law enforcers and policy makers to develop effective measures to deal with cyber terrorism and cybercrime.

Current research has established that cybercrime laws with its transnational nature offer the world a real and sound response to deal with the prevalent threat. However, international cooperation is recognized as key steps to squarely address the issue. Our information systems are susceptible to cybercrimes due to the numerous vulnerabilities that are increasingly emerging due top much reliance on technology. In addition, the evolution of technology is rapid which takes the advantage of the complexities involved in laws ad policy making it easier for malicious characters to exploit the existing vulnerabilities (Edwards, 2001). The real obstacle to dealing with cybercrime prevalence is the lack of definite laws and lack of cooperation among world nations to effectively respond to the emerging technological threats. In sum, the failure to initiate global consensus to address cyber related crimes and cyber terrorism is the real issue preventing effective responses. It is for that reason that we are slowly giving the power to the malicious characters (Terrorists and cyber criminals) a convenient platform to exploit the vulnerabilities as there are no definite instituted laws providing technical, legal, political, or cultural guidance in dealing with this vast growing monster. In the attempt to evaluate the probable interventions, development of a matrix comes hand in hand to offer a path towards enhancing international cooperation and responding to the vulnerabilities (Tricker, 2015).

In the formation of the matrix, credible points will be considered towards the journey of eliminating the existing vulnerabilities. These interventions include the call to establish a National Cyberspace Security Response System, development of a Global Cyberspace Security Threat and Vulnerability Reduction Program, initiation of Cyberspace Security Awareness and Training Program at a global level, and formulation of international cybercrime law and policies (The National Strategy to Secure Cyberspace, 2003, p. 28).

Cybercrime security; cybercrime is highly related to most of the greatest crimes that occur in the banks and financial institutions. Individual, website wizards, hacks on bank systems accessing banks most valuable information. The access to the banks data facilitates the transfer of huge amount of money to unknown accounts where the criminals can access the cash. The problem of cybercrime can be solved by installation of robust software that are complicated to crack, frequent change of the systems and software and also educating the bank personnel on the importance of using complicated passwords on their computers and accounts too (Comizio, Dayanim & Bain, 2016).

Vandalism of Hardware or Infrastructure

To address the risks of vandalism it requires the banking to establish a central point to facilitate maintenance of the computer hardware. Security can be enhanced through deployment of security systems and infrastructure. The strategy will certainly help the banking to monitor the hardware in one place (Kouns and Minoli, 2011).

Unstable Power Supply

Installation of alternative power supply is a good intervention to be performed to avoid disruption of storage data processes that could lead to loss of information. It is an intervention for the banking to mitigate risks of losing crucial data. In addition, the act is cost effective and reduces risk prevalence.

The banking to act in harnessing the technology of cloud computing as it helps in crowd gathering, validating, and leveraging data from numerous external sources globally. It further helps in enhancing a shielding platform to counter the prevalent threats targeting business enterprises.

Conclusion

Developing comprehensive infrastructure for a secure information system is not a simple task since technological skills are rapidly dynamic. However, to keep threats at minimal risk assessment performance is critical. It helps to identify potential threats in advance. In the selection of the appropriate infrastructure that matches the organizations requirement and specifications, as the architecture and program developer, the essential thing is to keep a balance of the divergent options with the competing priorities. This will help develop an ideal system as expected to serve the clients need in relation to what is on offer in the market.

References

Bradford, M. (2015). *Modern ERP: select, implement, and use today's advanced business systems*. Lulu. com.

Kavanagh, M. J., & Johnson, R. D. (Eds.). (2017). *Human resource information systems: Basics, applications, and future directions*. Sage Publications.

Lokuge, S., Sedera, D., & Grover, V. (2016, June). Thinking inside the box: Five Organizational strategies enabled through Information Systems. In *Pacific Asia Conference on Information Systems (PACIS 2016)*.

Cappelli, D. M., Moore, A., & Trzeciak, R. (2012). The certification and guide to insider threats: how to prevent, detect, and respond to information technology crimes. USA: Addison-Wesley Professional.

Comizio, V. G., Dayanim, B., & Bain, L. (2016). Cybersecurity as a Global Concern in Need of Global Solutions: An Overview of Financial Regulatory Developments in 2015. Journal of Investment Compliance, 17(1).

Durcekova, V., Schwartz, L., & Shahmehri, N. (2012). Sophisticated denial of service attacks aimed at application layer. In ELEKTRO, 20(12)55-60.

James A. Lewis (Eds), Security: Turning national solutions into international cooperation (pp. 1- 12). Washington D.C.: The CSIS Press:

Kenney, A. (2016). Third-party risk: How to trust your partners. Journal of Accountancy, 221(5), 56.

Kouns, J., & Minoli, D. (2011). Information technology risk management in enterprise environments: a review of industry practices and a practical guide to risk management teams. John Wiley & Sons.

Lord, S., Miller, L., & McLaughlin, E. (2015). GAO issues framework for managing fraud risks in federal programs. International Journal of Government Auditing, 42(4), 12.

Okeke, R., & Shah, M. (2016). Information Theft Prevention: Theory and Practice (Vol. 41). Routledge.

Rajput, R., Mishra, A., & Kumar, S. (2014). Optimize intrusion prevention and minimization of threats for stream data classification. The Communication Systems and Network Technologies (CSNT), 2014