Intrusion Detection System for Citi Bank

Abhinav Khemani

School or Institution Name (University at Place or Town, State)

**Executive Summary**

Internet penetration into banking and financial sectors have changed the way people do banking. Information technology plays the role of utility in modern banks. Most of the banking is now powered by the internet. Increased use of the internet has also increased the security challenges for banks such as intrusions. Following measures are proposed for Citi bank to protect its systems.

1. Network intrusion detection system
2. Host-based intrusion detection system
3. Anomaly-based intrusion detection system

The paper describes the threats to existing systems and the benefits of implementing intrusion detection systems.

**Introduction:**

Modern financial systems heavily rely on the internet and related technologies. Most of the financial transactions are now powered by Internet-based banking systems. Citi bank has also adopted the latest information technologies to ensure business continuity. With the increased penetration of the internet into the financial sector, the security risks for these systems are also increased at an exponential rate. Banking systems are prone to intrusions from third parties such as cybercriminals and hackers (Zheng, Zhou, Sheng, Xue, & Chen, 2018). Hackers cost billions of dollars to financial sectors every year. As the security researchers are improving the defenses, the criminals are also developing more sophisticated attacks to compromise these systems. The most critical asset of a bank is the internal network of the bank. Citi bank has deployed firewall to protect the network, but it is not enough to protect the system from the latest attacks. The paper describes the threat types and their preventing solutions to the Citi bank. Implementation of these systems will help the Citi bank to save millions of dollars annually spent on the troubleshooting and system restoration efforts.

**Literature Review:**

There is no business that can be imagined without the implementation and reliance on information technology solutions. The fundamental purpose of an information technology system is to process the data. As every business includes some data processing, there are some businesses that deal with critical information such as personally identifiable information. Banking is one of the businesses that use information technology solutions to process personally identifiable information of the clients to provide them with customized service as per their requirements (Kiwia, Dehghantanha, Choo, & Slaughter, 2018). Where every organization dealing with personally identifiable information of the clients claims to be the best in protecting the information as well the headlines are filled with the successful news of targeted data breaches of such organizations.

Cybercrimes cost billions of Dollars to many organizations annually. It is due to the reliance of the modern service on the internet. Banking is now based on the internet because the internet itself was not designed with much security in mind; therefore any service offered on the underlying internet will be inherently insecure. Banks deploy virtual private networks and many other security solutions to protect their network from hackers. Banking systems are prone to many types of attacks such as the man in the middle attacks, man in the browser attacks, and keylogger attacks (Cepheli, Büyükçorak, & Karabulut Kurt, 2016). All these risks are categorized by the intrusions into the network. In a man in the middle attack, the data transmitted over an insecure channel such as a communication wire can be intercepted by the intruder in transit. It is the external intrusion into the system. Although it is not common nowadays, but a decade ago it was a significant concern for banks all across the world.

Man in the browser and keylogger attacks are considered to be the intrusions arising from within the network. They have the same dangerous effects on the overall security of the data being transmitted as the previous attacks. Modern attacks are more sophisticated in their design than their old counterparts. Banks have implemented various security measures to render these attacks useless. But no defense in the digital world can be considered as hundred percent effective because threat landscape is ever changing. Information assurance is known as the strategies implemented by the organizations to ensure the confidentiality, integrity, availability, and non-repudiation of critical data (Hamed, Ernst, & Kremer, 2018). To minimize the expenditure on system restoration, the information assurance must be a part of the business plan, especially for the banks. Banks are now implementing various intrusion detections systems to prevent attacks before they even execute on the network.

**Empirical Analysis:**

Citi bank has deployed a network level firewall to protect its internal network from threats such as spyware and hackers. However, the problem with a firewall solution at the network level is that it considers the incoming traffic as an intrusion but ignores the traffic that generates from within the network. Therefore, insiders attack such as man in the browser attack can be successfully executed despite the fact the network is secured by the firewall. Firewall will not be able to block attacks initiated within the network (Hodo, Bellekens, Hamilton, Tachtatzis, & Atkinson, 2017). The risk of such attacks is significantly increased with the implementation of bring your own device policies. An employee of the bank may bring an already infected device and connect it to the sensitive network of the bank compromising the whole network.

To protect against such type of attacks intrusion detection systems are to be implemented in the Citi bank. One system is the network intrusion detection system that will monitor the internal network of Citi bank for any intrusion attempt. It will protect against any violation of local security policies while the firewall will be protecting against outside of the network attacks. As an industry practice, to complement the network intrusion detection system, a host-based intrusion detection system will also be implemented. Host-based intrusion detection system will pinpoint the device that is being used to initiate the attack on the network (Zhang, Jones, Song, Kang, & Brown, 2017). Therefore, any malicious attempt will be intercepted and responded before the payload execution. Anomaly-based intrusion detection system will be added as the fourth line o defense against digital darks. It will detect all of the information technology related processes of the Citi bank and if any anomaly between routine tasks is detected that will be intercepted accordingly. Implementation of these systems will help the Citi bank to save expenditures on the troubleshooting and restoration of the network systems after a successful attack on the network.

Targeted attacks on the network of the bank will also be prevented because information assurance is not about responding to the attacks, but it deals with the prevention of the attacks as well. Without the implementation of these systems, the protection of personally identifiable information of the clients cannot be ensured. Targeted attacks on financial organizations are increasing at an exponential rate. If an attack compromising the personal information of customers is successful, then along with the financial losses the organization suffers from severe reputation loss as well.

**Conclusion:**

Protection of critical information is inevitable for all of the financial institutions. The banks must implement effective intrusion detection systems to protect critical information assets of the bank. It is the customer’s trust in the bank that is required to ensure business continuity. Successful breaches of data can be fatal to customers trust in the banking system. Protection of personally identifiable information is the obligation of the organization processing the information such as the banks. Intrusion detection systems ensure the protection of valuable data stored in banking networks.

References

Cepheli, Ö., Büyükçorak, S., & Karabulut Kurt, G. (2016). Hybrid intrusion detection system for ddos attacks. *Journal of Electrical and Computer Engineering*, *2016*.

Hamed, T., Ernst, J. B., & Kremer, S. C. (2018). A survey and taxonomy of classifiers of intrusion detection systems. In *Computer and network security essentials* (pp. 21–39). Springer.

Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., & Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. *ArXiv Preprint ArXiv:1701.02145*.

Kiwia, D., Dehghantanha, A., Choo, K.-K. R., & Slaughter, J. (2018). A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence. *Journal of Computational Science*, *27*, 394–409.

Zhang, J., Jones, K., Song, T., Kang, H., & Brown, D. E. (2017). Comparing unsupervised learning approaches to detect network intrusion using NetFlow data. In *2017 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 122–127). IEEE.

Zheng, Y.-J., Zhou, X.-H., Sheng, W.-G., Xue, Y., & Chen, S.-Y. (2018). Generative adversarial network based telecom fraud detection at the receiving bank. *Neural Networks*, *102*, 78–86.