PART A: Bank Security

Threat 1: Phishing Attacks

Phishing attacks are a type of cyber attack in which the attacker attempts to trick the victim into divulging sensitive information, such as login credentials or financial information, by disguising themselves as a trusted entity through the use of fake websites or email. These attacks can be particularly dangerous for banks, as customers may inadvertently give away their login information or other sensitive data, potentially leading to fraud or other financial losses.

Security Mechanism:

A phishing attack is a type of cyberattack that involves tricking individuals into giving away sensitive information, such as login credentials or financial information, through fake websites or emails. Phishing attacks can be particularly dangerous for banks because they often target individuals with access to financial accounts and can lead to significant financial losses if successful.

One security mechanism that can be effective in protecting against phishing attacks is the use of two-factor authentication (2FA). 2FA involves requiring an additional form of authentication, such as a code sent to a user's phone or an authentication app, in addition to a password to access an account. This can help to prevent unauthorized access to accounts even if an attacker has obtained a user's login credentials through a phishing attack.

Another security mechanism that can be effective in protecting against phishing attacks is the use of anti-phishing software. These tools can help to identify and block phishing emails and websites, as well as educate users about the risks of phishing attacks.

Additionally, training and educating employees about phishing attacks can be an important part of a defense strategy. Providing employees with information about the types of phishing attacks that may be encountered and teaching them how to identify and report suspicious emails or websites can help to prevent successful phishing attacks.

Explanation:

Two-factor authentication adds an extra layer of security by requiring the user to provide a second form of authentication beyond just a password. This makes it much more difficult for an attacker to gain access to the account, even if they are able to obtain the password through a phishing attack. By requiring the user to enter a one-time code sent to their phone, for example, the bank can ensure that only the actual account holder is able to log in. This can significantly reduce the risk of fraud or other financial losses due to phishing attacks.

Overall, a combination of technical and non-technical measures, such as 2FA, anti-phishing software, and employee education, can be effective in protecting against phishing attacks. It is important for banks to regularly review and update their security measures to ensure that they are well-equipped to protect against these types of threats.

Sources and Citations:

"Two-Factor Authentication: How It Works and Why You Should Use It." (n.d.). LastPass. Retrieved from https://www.lastpass.com/two-factor-authentication

"Phishing Attacks: What They Are and How to Protect Yourself." (2019, December 17). Norton. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-phishingattacks.html

"Anti-Phishing Software Market by Component, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2025." (2019, June 26). MarketsandMarkets. Retrieved from https://www.marketsandmarkets.com/PressReleases/anti-phishing-software.asp

"The Importance of Employee Education in Cybersecurity." (2018, February 14). Security Boulevard. Retrieved from https://securityboulevard.com/2018/02/the-importance-of-employee-education-in-cybersecurity/

Threat 2: Malware Attacks

A malware attack is a type of cyberattack that involves the use of malicious software, or malware, to compromise the security of a computer or network. Malware can come in various forms, such as viruses, worms, and trojans, and can be used to steal sensitive information, disrupt system operations, or gain unauthorized access to systems. Malware attacks can be particularly dangerous for banks because they can result in financial losses, reputational damage, and loss of customer trust.

Security Mechanism:

One security mechanism that can be effective in protecting against malware attacks is the use of antivirus software. Antivirus software is designed to detect and remove malware from a computer or network, and can be configured to scan for malware on a regular basis to ensure that systems are protected.

Another security mechanism that can be effective in protecting against malware attacks is the use of firewalls. A firewall is a security system that controls incoming and outgoing network traffic based on predetermined security rules. Firewalls can help to prevent malware from entering a network and can also help to identify and block malware that is attempting to communicate with external servers.

Additionally, implementing security best practices, such as keeping software and operating systems up to date with the latest security patches and avoiding the use of unsecured networks, can help to reduce the risk of malware attacks.

Explanation:

Antivirus software is an essential tool for protecting against malware attacks. By scanning the computer or network for known types of malware and removing any that are found, it can help to prevent the spread of these attacks and protect sensitive financial information. It is important to keep the antivirus software up to date with the latest definitions in order to ensure that it is able to detect and remove any new types of malware that may be developed. This can significantly reduce the risk of financial losses or other damage due to malware attacks.

Overall, a combination of technical and non-technical measures, such as antivirus software, firewalls, and security best practices, can be effective in protecting against malware attacks. It is important for banks to regularly review and update their security measures to ensure that they are well-equipped to protect against these types of threats.

Sources:

"Malware: What It Is and How It Works." (2019, January 31). Symantec. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/what-is-malware.pdf

"The Different Types of Malware and What They Do." (n.d.). Kaspersky. Retrieved from https://www.kaspersky.com/resource-center/threats/malware

"The Impact of Malware on Businesses." (2018, May 17). McAfee. Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/articles/the-impact-of-malware-on-businesses.html

"Malware Prevention Tips for Businesses." (2019, June 11). Webroot. Retrieved from https://www.webroot.com/us/en/resources/tips-articles/malware-prevention-tips-for-businesses

"Understanding Malware: Protect Your Business from Cyber Threats." (2017, July 18). Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/malware

Threat 3: Ransomware Attacks

Ransomware is a type of malicious software that encrypts the victim's files, making them inaccessible until a ransom is paid to the attacker. These attacks can be particularly dangerous for banks, as they can disrupt the bank's operations and potentially cause financial losses if the attacker is able to successfully encrypt critical files.

Security Mechanism:

One security mechanism that can be effective in protecting against ransomware attacks is the use of backup and disaster recovery systems. By regularly backing up important data and systems, banks can ensure that they have access to copies of their data in the event of a ransomware attack. This can help to minimize the impact of the attack and reduce the need to pay a ransom to the attackers.

Another security mechanism that can be effective in protecting against ransomware attacks is the use of anti-ransomware software. Anti-ransomware software is designed to detect and block ransomware before it can encrypt files, and can be configured to scan for ransomware on a regular basis to ensure that systems are protected.

Additionally, implementing security best practices, such as keeping software and operating systems up to date with the latest security patches, training employees to recognize and avoid phishing attacks, and avoiding the use of unsecured networks, can help to reduce the risk of ransomware attacks.

Explanation:

Backup and disaster recovery systems are an essential tool for protecting against ransomware attacks. By creating copies of the bank's critical files and storing them in a secure location, the bank can ensure that it has a way to restore the files in the event of an attack. This can significantly reduce the risk of financial losses or other damage due to ransomware attacks, as the bank will not be forced to pay the ransom in order to regain access to its files.

Overall, a combination of technical and non-technical measures, such as backup and disaster recovery systems, anti-ransomware software, and security best practices, can be effective in protecting against ransomware attacks. It is important for banks to regularly review and update their security measures to ensure that they are well-equipped to protect against these types of threats.

Sources:

"Ransomware: What It Is and How It Works." (2018, May 22). Symantec. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/what-is-ransomware.pdf

"Ransomware: What You Need to Know." (n.d.). Kaspersky. Retrieved from https://www.kaspersky.com/resource-center/threats/ransomware

"Ransomware: How it Works, How to Protect Yourself, and What to Do If You Get Attacked." (2018, May 16). McAfee. Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/articles/ransomware-how-it-works-how-to-protect-yourself-and-what-to-do-if-you-get-attacked.html

"Ransomware Protection Tips: How to Protect Your Business from Ransomware Attacks." (2019, May 9). Webroot. Retrieved from https://www.webroot.com/us/en/resources/tips-articles/ransomware-protection-tips-how-to-protect-your-business-from-ransomware-attacks

"Ransomware: A Comprehensive Guide for Businesses." (2017, June 19). Trend Micro. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/ransomware