Assignment

Chimene Tchokoko Diboma

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

**Information Technology System Architecture:**

Information technology plays the role of utility in modern business. Concept Analysis Corporation is a company providing data analysis services to other organizations. The company specializes in delivering big data analysis and trend development using streaming data analysis. The company utilizes an internal network of computing resources to provide efficient data analysis to its clients. As the most crucial asset of the organization is the data that it collected from its clients, the protection of the critical data against digital darks is the objective of the organization. Data is considered to be the oil in the modern world as cybercriminals are always inventing sophisticated attacks to compromise large corporate networks. Following Network Security and Vulnerability threat table provides an overview of the threats to the information technology infrastructure of the organization.

|  |  |  |  |
| --- | --- | --- | --- |
| Component | Vulnerabilities  | Threats | Likelihood |
| LAN Security | * Outdated router configuration
* Software security holes
* Lack of access policies
* Remote code execution
 | * Computer viruses
* Trojan Horses
* Key loggers
* Rootkits
* Hacking
* Eavesdropping
* Man in the middle attacks
* Ransomware
* Packet sniffing
 | Very High |
| Identity Management | * Authentication protocol spoofing.
* Authorization weakness
 | * Insider threats
* Host intrusions
 | High  |
| Physical Security | Lack of physical restrictions | Physical tempering in the system | High |
| Personal Security | Weakness in identity management protocols | Personal information of the employees or clients can be compromised by targeted attacks | Very High |
| Availability  | Weakness in the physical infrastructure of the network. | Data may not be available to concerned departments when needed due to cyber attacks | Very High |
| Privacy | Lack of intrusion detection systems and cryptography for message protection | Data interception by key loggers and hackers infiltrating the network | Very High |

 Cyber-attacks on information systems are increasing at an exponential rate. Hackers and malicious actors are continuously developing sophisticated attacks to gain more and more monetary benefits. Financial perks are the major motivation of most of the cyber-attacks. Criminals can be sponsored by the states as well to digitally harm the opponents of the state government. Cybercrimes are developing as an industry. Criminals focus on organizational networks because they can harvest more data from a single organizational attack as compared to the attack on millions of individual computer users (Rid & Buchanan, 2015). Common attack methods used by criminals include penetration into the organizational network. There can be several ways of penetration into the network of any organization. Most of the time successful penetrations into the network are accompanied by the existing vulnerabilities in installed software on the networked machines in the organization.

 Vulnerabilities serve as the open window in a locked home. The home will be at risk of being compromised in a theft attempt despite the fact that the main door was perfectly locked. All of the logical measures of securing and protecting the organizations serve the same functionality as locking down the main door. On the other hand software vulnerabilities serve as the open window in the locked home allowing an attacker to infiltrate the system. Hackers can also inject code into legitimate applications installed on the system creating and maintaining backdoor access to the system. When a system is compromised, then attackers can have full control over the network or the information being shared on the network. One such example is the man in the middle attacks in which the attacker can sniff the network packets and change their content before they reach the final destination without the knowledge of the participating parties in the network communication. Privacy of the message can be severely compromised in such attacks. Several measures, including patch management systems, vulnerability management, threat detection and response system, intrusion detection system, physical security measures, and encryption techniques will be added to the security portfolio of the organization to protect the most valuable asset of the organization.

**Plan of Protection:**

As per the described threats to the information systems and for information assurance to provide confidentiality, integrity, availability, and non-repudiation of the data following measures will be taken gradually. To protect the privacy of the data various encryption algorithms and technologies will be deployed. Encryption will help to maintain the confidentiality of the data either being shared on the network or stored in the databases. Public key cryptographic infrastructure will be utilized to provide authentication and non-repudiation of the data. As encryption algorithms include symmetric and asymmetric encryption capabilities, public key cryptographic systems are associated with asymmetric encryption. Asymmetric encryption provides with different keys for coding and decoding the data making it very hard for criminals to break the code.

 All the logical measures of protecting the data and critical information technology infrastructure of the organization may go in vain if there are no provisions of physical security. Physical security involves restricting physical access to the systems. It involves effective user authentication methods such as the use of smart cards for accessing certain physical systems of the organization. Physical restrictions will be applied to the system including a mechanism of access control using smart card approach. It will help the protection of critical assets against physical tampering.

**Data Hiding Technologies:**

Cryptography is a practice of coding the ordinary message with special techniques known as ciphers so that only the intended recipients can read the message. After applying cipher on the plain text message, the resulting message is known as the ciphertext. A simple example is of shift ciphers or Caesar ciphers. In Caesar cipher, each letter of the English alphabets is rotated three places. The resulting message is known as ciphertext. To retrieve the original message the receiver must perform the exact opposite of the operation at the sender end (Patil, Narayankar, Narayan, & Meena, 2016). In Caesar cipher, the key to encrypting the message is three. In such encryption techniques, the data will be secure even if the attacker knows exactly the underlying algorithm of the encryption as well provided that the key is kept secret. Polyalphabetic ciphers are based on the substitution of the alphabets with multiple characters. These are also symmetric cryptographic methods because the keys for encryption and decryption remains the same.

 Block ciphers are also symmetric in nature, but they do not replace single characters with the ciphers. Instead, block ciphers capture a block of input data and apply the cipher on the block of data resulting in a block of encrypted data. Block ciphers are widely used in network communications due to the simplicity of their implementation and higher speeds of their operation. It is relatively easy for criminals to break symmetric encryption due to the same keys used for encryption and decryption (Gupta & Kaushik, 2017). However, the sophistication of such symmetric ciphers can be increased by passing the plaintext message through the encryption algorithm multiple times. A popular example of this technique is known as a triple data encryption standard also known as DES. In triple DES, the cipher is applied on the plaintext three times creating three folds of encryption. RSA, on the other hand, is an encryption algorithm utilizing asymmetric cryptography also known as public key cryptography. The problem with the symmetric cryptography was to share the secret key with intended parties using some secure channel. The problem created a bottleneck in the development of symmetric cryptography systems. Solution to the problem is asymmetric cryptographic systems such as RSA.

 In the RSA algorithm, different keys are used for encrypting and decrypting the message. Before starting the communication, a public key is decided and broadcasted to everyone including the attacker. The encryption is a result of encrypting the data with a combination of shared public key and a secret private key. The strength of the system is governed by the fact that even if both the private and public keys are based on prime number factorization, none can be extracted from the other. Simply a public key cannot be used in any way to retrieve the private key of any party because there is no correlation between the two. Advance encryption standard also known as AES is asymmetric cryptographic standard (Rihan, Khalid, & Osman, 2015). The reason behind the invention of the AES is that DES use smaller key lengths. It is not feasible in modern world communications to use DES because a DES-encrypted message can be cracked in 52 hours and it has been proved ineffective as well. AES uses key lengths of 128 bit or 256 bits. Computational resources required to break these keys are not feasible even in the modern world. Therefore, it is the most secure encryption standard up until now.

 Instead of encrypting the messages using sophisticated encryption techniques the information can also be protected against malicious use by hiding the information. A technique in which the actual message is hidden in an ordinary image is known as steganography. Only the intended person will be able to find the message in such a picture. Digital watermarks can also be used to ensure non-repudiation and authenticity of the message. In digital watermarking, a small portion of authentication data is embedded within the message not visible to humans except the intended parties.

**Network Security Vulnerability and Threat Table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Vulnerabilities  | Threats | Likelihood | Defense  |
| LAN Security | * Outdated router configuration
* Software security holes
* Lack of access policies
* Remote code execution
 | * Computer viruses
* Trojan Horses
* Key loggers
* Rootkits
* Hacking
* Eavesdropping
* Man in the middle attacks
* Ransomware
* Packet sniffing
 | Very High | Use of updated security software along with security policies ensuring the data security. |
| Identity Management | * Authentication protocol spoofing.
* Authorization weakness
 | * Insider threats
* Host intrusions
 | High  | Use of smart cards and access controls. |
| Physical Security | Lack of physical restrictions | Physical tempering in the system | High | Physical access restrictions and authentication using smart cards. |
| Personal Security | Weakness in identity management protocols | Personal information of the employees or clients can be compromised by targeted attacks | Very High | Host based intrusion prevention systems. |
| Availability  | Weakness in the physical infrastructure of the network. | Data may not be available to concerned departments when needed due to cyber attacks | Very High | Monitoring and compliance of the physical network. |
| Privacy | Lack of intrusion detection systems and cryptography for message protection | Data interception by key loggers and hackers infiltrating the network | Very High | Public key cryptographic systems based on AES.  |

**Access Control Based on Smart Card Strategies:**

As it has been described earlier that all of the logical security steps can be bypassed if there are no adequate physical security measures. Various physical security measures can be deployed to control access to the physical infrastructure of the organization. Smart card approach will be used to protect physical breaches of critical infrastructure. Smart cards have electronic chips integrated with them to provide encryption capabilities to the data stored on such cards. Personally identifiable information of the employees will be stored in the chips and will be encrypted using a public key cryptographic system. The information will be digitally signed by the digital certificate of the organization as part of the identity management program.

 In this way trusted third parties would also participate in authentication of the users before granting access to the critical infrastructure. Card scanners will be available along with all of the doors of the departments (Batalla, Mastorakis, Mavromoustakis, & Zurek, 2016). Whenever an employee tries to open the door, the card will be scanned. The solution will also provide extended monitoring of daily attendance of the employees as well. Common access cards are actively being used by the department of defense for personnel identification and identity management due to the extended security features of these cards. Similar mechanisms will be implemented in the organizations for physical security and identity management of employees and workers.

**The Email Security Strategy:**

The main source of communication between the employees and clients is using email. As phishing campaigns are increasing both in numbers and in complexity, it is inevitable to secure email communications. Pretty good privacy is a public key cryptography system to secure email communications. It provides authentication and identification capabilities. A message is signed with the digital signature of the individual using the PGP encryption mechanism (Anugurala & Chopra, 2016). The recipient of the message will be able to verify the identity of the message by looking at the digital signature that is accompanied by the message. PGP encryption mechanism will be implemented in the organization, and it will be mandatory for employees to digitally sign all of the email messages. Digital signatures provide encryption capabilities and are managed by certification authorities. Certification authorities and verification mechanism of digital signatures are part of the public key infrastructure.

 Public key infrastructure is a network of certification authorities that issue digital signatures to the public. Digital signatures bind public keys with the corresponding private keys of the users. In an organization, a digital signature can be used to identify and manage the identity of the employee. When a message is to be sent by the sender, will encrypt the message with the private key along with the public key of the intended recipient of the message (White & Yeh, 2017). The receiver will decrypt the original message from the email using a private key and corresponding public key. In this case, the public key is designated as the digital signature used to sign the message. Certification authorities regulate the use of digital certificates. There are expiration dates as well for digital signatures or certificates to ensure that the ownership details are up to date. It is inevitable to stop misuse of public keys as well.

 Mobile devices are used by the employees to send and receive emails. Most of the time critical documents related to the business operations are also stored in handheld devices of the employees. Therefore, securing mobile devices using encryption algorithms is inevitable. Some of the mobile manufacturers provide encryption capabilities by default such as Apple and Blackberry. Encryption provides added layers of security for mobile devices because if the mobile devices are lost no third party will be able to retrieve the data stored in the device (Callaghan et al., 2016). Other device manufacturers and software developer’s applications can be configured to support encryption capabilities. Devices support external memory cards, or memory enhancement add-ons must be encrypted as well. If the memory enhancements are not encrypted, then attackers can use the memory devices to retrieve the data from the devices. All of the recommended security measures along with intrusion detection systems will be implemented in the organization to ensure confidentiality, integrity, availability, and non-repudiation of the data.

References

Anugurala, A., & Chopra, A. (2016). Securing and preventing man in middle attack in grid using open pretty good privacy (PGP). In *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 517–521). IEEE.

Batalla, J. M., Mastorakis, G., Mavromoustakis, C. X., & Zurek, J. (2016). On cohabitating networking technologies with common wireless access for home automation system purposes. *IEEE Wireless Communications*, *23*(5), 76–83.

Callaghan, D., Pudipeddi, R., Olsen, G., Patel, S., Zhou, J., & D’silva, D. (2016). *Content item encryption on mobile devices*. Google Patents.

Gupta, A., & Kaushik, S. (2017). A Review: RSA and AES Algorithm. *IITM Journal of Management and IT*, *8*(1), 82–85.

Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617–624.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Rihan, S. D., Khalid, A., & Osman, S. E. F. (2015). A performance comparison of encryption algorithms AES and DES. *International Journal of Engineering Research & Technology (IJERT)*, *4*(12), 151–154.

White, K. D., & Yeh, J. (2017). Developing Accessible P2P Email Encryption Based on CLOW-GKA.