Option #1: XYZ Corporation Portfolio Project

Liam Bergerson

CSU - Global

ITS350-1

L. Schneider

1/16/22

Option #1: XYZ Corporation Portfolio Project

XYZ Corporation is currently a twenty to thirty employee organization that has made a substantial investment due to a successful widget development. As a result, the company is expected to be around one hundred employees and has moved into a new building. Because of this move, the local area network (LAN) structure is default. Everyone has access to everything and there are no security measures in place. XYZ's network will be secured with the highest level of security that will prevent attacks internally or externally. A plan will be implemented to provide secure access control for all users. A strong password policy will be implemented to ensure that strong passwords are enforced. Data will be encrypted with a detailed cryptography method. A remote access plan will be implemented to ensure that remote users are working using the network in a safe and secure manner. Finally, a plan to protect against malware and other attacks will be implemented.

Secure access control methods

Access control is defined as authenticating a person based on their identification and only giving that person what they need to access and nothing more (Gentry, 2021). Access control ensures that only the minimum access is given to an employee for their working needs; it is also to prevent an employee from damaging a piece of equipment from a lack of knowledge. There are four access control models that could be used for this organization: mandatory access control (MAC), role-based access control (RBAC), discretionary access control (DAC), and rule-based access control (RB-RBAC).

Mandatory access control gives only the owner and custodian management of the access controls (Gentry, 2021). In other words, the end user has no control over any

settings that provide any privileges to anyone (Gentry, 2021). There are typically two submodels to the MAC model: the Biba model and the Bell-LaPadula model. The Biba model focuses on the integrity of information whereas the Bell-LaPadula model focuses on the confidentiality of information. The Biba model utilizes a “read up” clearance, which means that employees with a lower level of clearance can only read documents with a higher level of information. Employees with a higher level of clearance can “write down” documents for lower level clearance information (Gentry, 2021). The Bell LaPadula model states that employees with a higher level of clearance can only write at that level and no lower, but can still read at lower levels. This model was originally developed in government or military facilities when information was kept within the same clearance level and no one else could read that information.

The second access control model is role-based access control (RBAC). This model provides access based on the role itself and not the employee (Gentry, 2021). So instead of a specific employee receiving the minimum amount of access, the position he or she fills will gain that minimum access. One benefit of RBAC is that it makes the system administrators job easier since they only have to configure access for the roles and not the individual employees. The trade-off of RBAC is that it would be difficult for employees to gain access to files not of his or her role (Gentry, 2021).

The third access control model is discretionary access control (DAC). This model allows an employee complete control over any objects they have along with software associated with those objects (Gentry, 2021). This is the least restrictive model of the four, however there are two weaknesses with DAC. The first is that it gives the end user complete control over security settings, meaning that other employees could have

authorized access to things they aren't supposed to have access to. The second weakness is end user permissions are inherited into other programs they execute. This means that the end user could execute malware without their knowledge (Gentry, 2021).

The final access control model is rule-based access control (RB-RBAC). RB-RBAC is similar to RBAC but it assigns access to employees based on rules set by system administrators (Gentry, 2021). For example, if employees are only allowed access to files during certain hours of the day, that is a rule set by the system administrator (Gentry, 2021).

The access control model I would choose for the highest amount of security for the XYZ Corporation is role-based access control. RBAC is a perfect balance between restrictive and lenient. MAC is too restrictive because only the owner can give access to other employees. DAC is too lenient because it allows an individual complete control over anything they own. RBAC gives the minimum access based on specific roles that an employee fills. RB-RBAC seems unpredictable because it's up to the system administrator to set the rules for access to employees. There could be a lack of rules for the maximum amount of security or there could be too many rules so nothing can be done.

Password policy

The password policy that will be used for the XYZ Corporation will be robust enough to prevent any systems from falling to a brute force attack. A business with no password policy will have dramatically increased chances of information being lost or stolen because easily crackable passwords are used. A robust password policy will require an employee to make a complex password, the duration they are allowed to use

that password before they are required to change it, and the history of passwords to ensure that the same password isn't used too frequently. WCM (2021) is an example of a robust password policy. WCM (2021) defines a complex password to be at least 16 characters, including upper and lowercase letters, numbers, and special characters. It is recommended that a phrase be used and include numbers and special characters in it (WCM, 2021). For example, a common phrase WCM (2021) uses is "When I was five, I learned how to ride a bike." Convert that into a password and it would look like this, "WhenIwa$5,Ilh0wt0rab1k3." WCM (2021) also states that a password must be changed every 90 days and the same password must not be reused for at least six generations.

Cryptography method

There are two methods of cryptography to consider for proper data encryption. The first method is symmetric encryption. Symmetric encryption utilizes one shared key that is used to both encrypt and decrypt messages and files. The main advantage of symmetric encryption is the speed. Since the keys are shorter, the encryption process is quick (Mukherjee, 2020). The disadvantage, however, is that only one key is used for encrypting and decrypting. Symmetric encryption can be used to encrypt data for storage such as USBs that are stored in one place. There are three common standards for symmetric encryption: DES, 3DES, and AES. DES has a block size of 64 bits and a key size of 56 bits. 3DES still has a 64-bit block size but the key size is tripled from 56 bits to 168 bits. AES has a block size of 128 bits but the key size comes in 128, 192, and 256 bit versions (uCertify, n.d.).

The second method is asymmetric encryption. Asymmetric encryption utilizes two keys, a private and a public. Public keys are used for encrypting and are shared online; private keys are used for decrypting and are kept secret (Mukherjee, 2020). Asymmetric encryption is more secure than its counterpart, symmetric encryption. The trade off is that the encryption process is slower because the keys are longer and more complex (Mukherjee, 2020). Asymmetric encryption can be used for digital signatures to authenticate identities of employees. There are three standards for asymmetric encryption: RSA, Diffie-Helman, and Elliptic curve. The RSA standard can use keys ranging from 512 bits, to 2048 bits (uCertify, n.d.). The Diffie-Helman standard relies on a secure key exchange before data can be encrypted (uCertify, n.d.). The Elliptic Curve standard generates keys based on values of an elliptic curve (uCertify, n.d.).

The method of encryption that will be used for the XYZ Corporation will be a mix of symmetric and asymmetric and will utilize the AES and RSA standards. Symmetric encryption will be used to encrypt storage media to ensure that the data on the drive is protected against unauthorized individuals. AES will be used because it offers the highest block cipher size and key size compared to DES and 3DES. Asymmetric encryption will be used for digital signatures to ensure that identities are authenticated properly. The RSA standard will be used because it boasts a massive 2048-bit key size which makes it very hard to decrypt without the key.

Remote access plan

Remote access is ever-growing in this technology filled age. That means that employees can now work from home with their laptops, tablets, and smartphones. That also means that employees are more vulnerable to attacks since they are now outside

of the physical walls of the building and the firewall protections. A remote access plan will provide remote employees with appropriate access in order to maximize productivity yet still protect information from accidental or malicious loss or damage (Simon, 2021). A remote access plan informs remote employees of their responsibilities in the security protocols highlighted to keep their systems and the data on their systems secure. A remote access plan also maintains confidentiality and keeps intellectual property secure. Proper consequences should be outlined in the remote access plan for employees that do not follow all of the protocols outlined in the plan. There are a few challenges which could prevent the use of a remote access plan. Some of those considerations are organizations with strict government access restrictions, retail and food-service workers, workers who lack discipline outside of the office, organizations that lack the infrastructure to provide security appliances, assembly line production process, and medical record staff will all inhibit the use of a remote access plan (Simon, 2021).

The remote access plan for the XYZ Corporation will provide the maximum amount of productivity, yet still protect sensitive information from loss or theft. Simon (2021) highlights guidelines for the remote access plan. Hardware and software configurations will include firewalls, anti-malware, and anti-virus programs. Proper encryption policies will ensure that vital data is encrypted. Email policies will ensure that information is secure and kept confidential with authorized individuals. Proper access privileges, authentication, and access hierarchy will ensure that employees access information that is only for them. Connectivity guidelines will tell employees what to connect to and what not to connect to. Password protocols will ensure that only complex

passwords are used, changed often, and the same password isn't used over changes. Acceptable use policies will ensure that remote employees are using information appropriately. Only trusted third-party protections and standards will be used to protect data. Finally, all remote employees will follow these guidelines otherwise consequences will be distributed.

Protection from malware and other attacks

Proper protection from malware and other attacks is especially important to protect data. Data lost or stolen from malware can cost millions and render information systems unavailable for hours, days, or even weeks. The network security for the XYZ Corporation will consist of a properly configured firewall, anti-virus, and anti-malware software. The organization will have an incident response plan that will mitigate the damage caused should malware infiltrate the information system. User training and awareness will be required as well to teach employees how to recognize malicious attacks such as phishing and malicious websites.

The purpose of an incident response plan is to have a detailed plan for responding to security incidents at your company (Cerrigione, 2020). Cerrigione (2020) highlights the phases of an incident response plan as: preparation, detection, containment, investigation, remediation, and recovery. The preparation phase consists of the creation of policies and procedures that aid in the response to the security incident. The detection phase is identification of the security incident. The containment phase is isolating the cause of the security incident. The investigation phase determines the scope, priority, and risk of the security incident. The remediation phase eradicates

the security incident from the system and repairs any systems affected. The final phase, recovery, analyzes the incident so it doesn't happen again in the future.

The purpose of user training and awareness is to help train employees in an organization to recognize, avoid, and report potential risks or vulnerabilities that can affect sensitive data. These risks include malware, phishing, ransomware, and spyware. User training and awareness is important because it protects data that will cost the business money, a tarnished reputation, etc. It also helps convert employees from attack victims to an extra layer of defense for the organization.

Conclusion

The elements highlighted will ensure that the XYZ Corporation has the maximum amount of security for safe and secure operations. The secure access control method will be role-based access. That will ensure that access is given to the role of the employee rather than the employee itself. The password policy highlighted will ensure that only complex passwords are used, the passwords are changed often, and the same password cannot be used until a number of password changes occur. Vital data will be encrypted with AES symmetric encryption for data at rest and RSA asymmetric encryption for data transfer. The remote access plan will ensure that remote employees are working in a safe and secure manner. Finally, firewalls, anti-virus, and anti-malware software will be implemented. A proper incident response plan and user training and awareness will be implemented as well.

References

Cerrigione, C. (2020, October 15). *Incident Response Plan*. IT Security. Retrieved January 13, 2022, from https://security.uconn.edu/incident-response-plan/

Gentry, S. (2021, May 27). *Access control: Models and methods [updated 2021]*. Infosec Resources. Retrieved January 12, 2022, from https://resources.infosecinstitute.com/certification/access-control-models-and-methods/

Mukherjee, L. (2020, June 18). *5 Differences Between Symmetric vs Asymmetric Encryption*. InfoSec Insights. Retrieved January 4, 2022, from https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/

Simon, B. (2021, August 3). *Increase Productivity While Maintaining Organizational Security with an Effective Remote Access Policy*. Smartsheet. Retrieved January 13, 2022, from https://www.smartsheet.com/effective-remote-access-policy

WCM. (2021, April 28). *11.15 - Password Policy and Guidelines | Information Technologies & Services*. Weill Cornell Medicine. Retrieved January 12, 2022, from https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines

uCertify. (n.d.). *Comprehensive Computer Technician.* *https://www.ucertify.com/?func=ebook&chapter_no=15#03V76*