**PORTFOLIO PROJECT**

Security Solutions at ZXY Corporation

Ismail Elmaliki

ITS 350 – Information Systems and Security

Colorado State University – Global Campus

Professor Lawrence Awuah

April 08, 2018

Introduction

Every person we know today has a lock at the entrance door to prevent unwanted intruders from entering their home. As with a home, a corporate environment and its network infrastructure must also be protected externally from unwanted intruders that enter company territory and from cyber criminals that attempt to intrude the corporate network; the company must also be protected internally to prevent its own employees from accidentally and intentionally putting the company’s security at risk. In order to fully protect ZXY Corporation’s network from external and internal threats we’ll be tackling these topics at a deep level:

* Securing access control methods for all user accounts
* Password policy
* A cryptology method to ensure data is encrypted
* A remote access plan to ensure users accessing the network remotely do so in a secure manner
* Protecting the network from malware and other malicious attacks

**Access Control Methods**

As defined from an article titled Access Control Facts (2018) via TestOut, access control is the ability to permit or deny privileges that users have when accessing resources within a network or computer. Access control can be broken down into three parts: *objects*, which include data, apps, systems, networks and physical spaces; *subjects*, which include users and processes that need access to objects; *access control system*, which includes policies and procedures. Another important aspect of access control that should be understood are the following essentials: Identification, Authentication, Authorization, and Auditing. Identification is a means of identifying an employee through a username or ID number; authentication is validating the employee’s identity like with a password and additional authentication methods that supplement a password like 2 factor authentication; authorization is either granting or denying that employee access to an object based on the level of permissions; auditing is maintaining a record trail of subject activities within the system. Now that we’ve covered access control methods at a high-level, we’ll dive into the steps that can be taken to control access from the top-down.

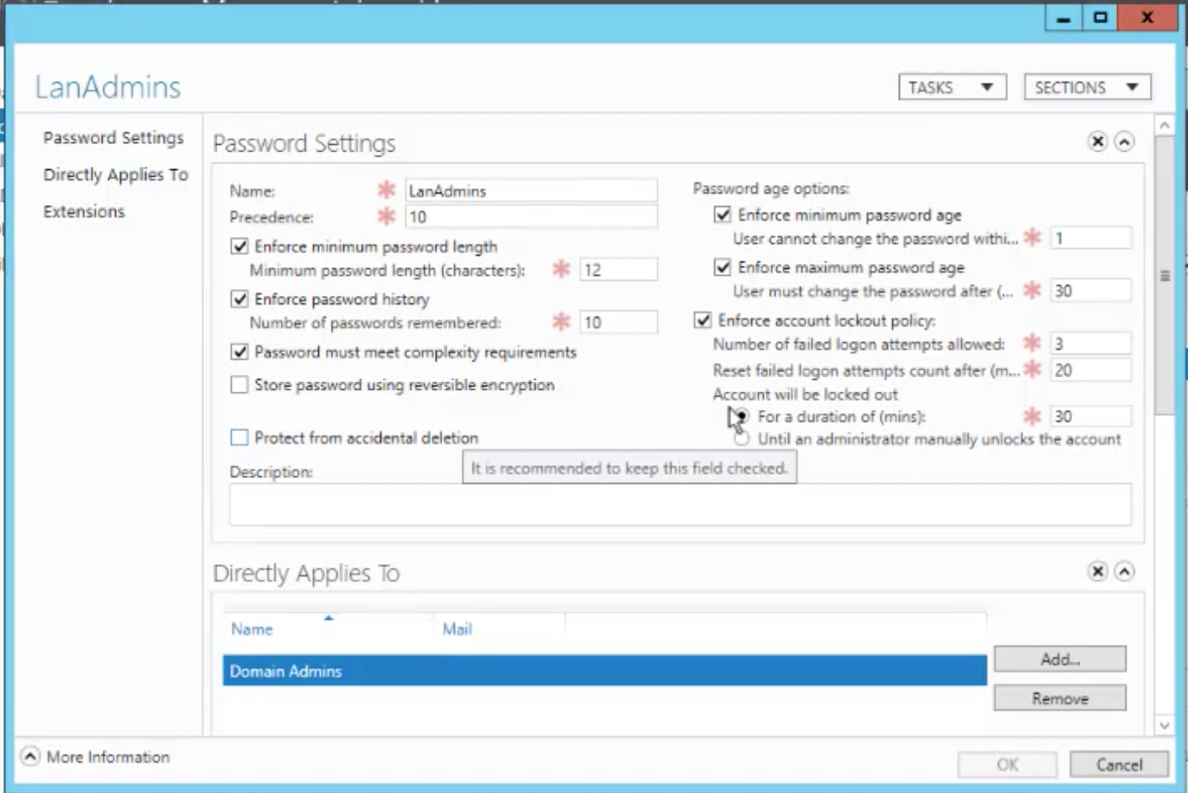
To cover the access control essentials of identification, authentication, authorization, and auditing, ZXY Corporation must use a directory service system like Active Directory for Windows sytems or Novell’s eDirectory for Linux and Windows systems. In order to use a directory service, the company must consider purchasing several servers to establish a server-client system within the company. From then on, when corporate computers are setup they’ll be a setup in a way that must follow the directory service standards and users will not be able to access anything but the essentials that are necessary for their role. As highlighted in the Access Control Best Practices Facts (2018) article via TestOut, following the principle of least privilege will ensure that users are granted minimal access to what they need best on their role; if more permissions are required, they can escalate to system administrators who’ll grant access based on the need of the employee. Going back to directory services, it’s important to highlight some of their key functions:

* Being able to create a user account for each employee
* Fulfilling the identification aspect of access control by providing a valid user account name
* Fulfilling the authentication aspect of access control by providing a password along with other requirements necessary to verify user identity
* Fulfilling the authorization aspect of access control by providing access to certain resources like files, printers, computers and other sources that are controlled by permissions
* Fulfilling the auditing aspect of access control by utilizing auditing within the operating system to keep track of actions performed by the user

The beauty of a directory service is its ability to fulfill all aspects of aspect controls when employees are using corporate computers. With that in mind, it’s also a must to consider physical access when employees are entering the premise. Referring to another TestOut article titled Physical Security Facts (2018), physical access controls should be considered like badges to gain entrance into the company building then have an area in which security guards are present to verify employee identity and granting access to enter the company premises. The badge card readers can rely on system that can be easily controlled by security guards, which can include an audit trail of who’s swiping to enter a room or facility. It would also be important to consider a physical log of visitors that access the building and to verify identity via federal/state issued identification. Finally, having door locks in sensitive areas like network and server rooms along with surveillance to ensure only authorized individuals are entering into those areas.

**Password Policy**

With an access control system in place like Active Directory, it’s important to apply security features like password policies – this will ensure a minimum-security standard is enforced on all user accounts, along with applying even stricter password policies for different user groups. Here’s a picture below from the video Using Fine-Grained Password Policies (2018) via TestOut.



* **Minimum password length**: aiming for a minimum password length that’s 8 to 12 characters long is reasonable, but if it starts at 12 it will definitely prevent possible brute-force attacks from ever being successful.
* **Enforce password history**: this feature will remember a particular number of passwords entered by the user to prevent re-use of a particular password. For example, if 10 is the value entered, then the user cannot use the last 10 passwords. By the time it reaches that point however, the user will most likely forget the password he/she would like to re-use.
* **Complexity requirements**: according to the TestOut article Hardening Authentication Facts (2018), Microsoft’s password complexity requirement must: be over 7 characters or more, include a minimum of 3 of the 4 special characters (e.g., lower case letters, upper case letters, numbers, or !, @, #, $, %, ^, &, \*), and cannot use dictionary words or any part of the user login identification.
* **Enforce minimum password age**: once the user changes his/her password, that password cannot be changed within a minimum number of days before the user decides to change the password again.
* **Enforce maximum password age**: this indicates the number of days a password will be valid for before the user is prompted to change his/her password; ideally some days may include 30, 60, 90, or 120 days.
* **Enforce account lockout policy**: This includes the number of failed login attempts allowed, after how many minutes failed login attempts should be reset, and a course of action to take once the account is locked out (locking the account for a particular number of minutes or requiring an administrator to unlock the account). This is an amazing security feature because it prevents unwanted intruders from guessing the password an unlimited number of times.

With regard to password policies, it’s important to balance both security and the overall user experience. For example, if the maximum password age is 30 days, then this may frustrate users and lead many to forget their password since it changes so frequently. Another thing to keep in mind is the lockout policy – depending on the preferred security method for the company, making that decision between locking the account only or requiring an administrator to unlock the user account. Although an administrator unlocking the account is the best way to go security wise, this will lead to workload on an IT administrator’s end. When it all comes down to it, balancing security, the user experience, and how security features may affect a colleague’s workload are all important things consider. Finally, understand that users should have more than one way of authenticating their accounts. For example, including 2-factor authentication, a SMART card, biometric reader, or a combination of all three are all important things to consider. Adding another layer will make it that much more difficult for any cyber intruder authenticate into employee accounts.

**Cryptology Methods**

With implementing a strong password policy, it’ll be difficult for any individual to crack that password. However, a somewhat tech savvy individual can download an app that’s easily accessible on the internet and change a user account’s password. At this point, does this mean our password policies are for nothing? Not at all! The reinforce password policies and to prevent anyone from logging into user accounts, we need to make sure we have encryption features turned on. Some common encryption methods to implement are full-volume encryptions like BitLocker for Windows and FileVault for Mac OS X operating systems. With encryption enabled, this will prevent anyone from changing the password using open source apps because the entire drive will be encrypted! Full-volume encryption is a logical lock that prevents anyone from grabbing the content or changing the password of that drive.

Going a step further, enabling firmware or BIOS passwords on all workstations is an even better step to take. By enabling a firmware password, it’ll prevent any tech-savvy user from entering into the BIOS and attempting to change to boot order or run a program that may pose a threat to the computer. By having both encryption and a firmware password enabled, any malicious user that steals a laptop will not be able to do anything with it. The computer will be practically useless and because of encryption data will be inaccessible.

**Remote Access**

In this section we’ll be touching a little bit of networking and discussing a secure method in which employees can remotely access the network. Referencing the its definition from the TestOut VPN Facts (2018) article, a Virtual Private Network is a remote access connection that encrypts data securely that’s sent over an untrusted network. For example, if an employee is using the company laptop and needs to connect to a company resource remotely, he/she can connect to a public Wi-Fi while using a VPN to access that company internal website safely and securely. The way to setup a VPN is to make sure the enterprise network router has built-in VPN functionality – from there, it can be easily configured through the router portal. When configuring the VPN, it’s important to:

* Select a protocol that’s supported by all devices to encrypt and encapsulate packets
* Open appropriate ports to allow VPN traffic through a firewall

Expanding with regard to opening the appropriate network ports, the best approach to take is to close all ports by default then figuring out which network port protocols to enable. For example, if there’s an incoming request to access the server remotely it, the appropriate and most secure port to open is SSH. Also allowing only HTTPS because it uses SSL encryption whereas HTTP doesn’t consider an encryption method.

**Network Security**

When it comes to network security, it’s important to identify the various network devices that are used by an organization. Referencing an article from TestOut titled Switch Security Facts (2018), these are strongly recommended security practices for switches: VLAN, MAC filtering, and Port authentication (802.1x).

* **Virtual LAN**: a logical grouping of computers based on a switch port which helps organize and better control the flow of traffic.
* **MAC filtering**: prevents unidentified computers from connecting directly to company switches and to any open Ethernet port in the office.
* **Port authentication**: if a device is connected to a switch, it must authenticate with credentials like a username and password, smart card, or another authentication device. Can be used in conjunction with MAC filtering for greater security.

Another common networking device in corporate environments are access points and Wireless LAN Controllers. Referencing Wireless Security Facts (2018) via TestOut, here are strong security practices:

* **SSID obfuscation**: changing the default SSID to something that doesn’t obviously identify the company and turning SSID broadcasting off.
* **Encryption**: enabling wireless encryption using AES with WPA2.
* **Authentication**: ensures that devices connecting to the wireless network authenticate – those authentication credentials can match a directory service or may require other means of authentication. Using authentication in conjunction with MAC filtering as previously mentioned in the switches section can also be applied to wireless networking security!
* **Separating internal and external network**: it’s important to create an external guest network and enforce a security policy to mandate that BYODs (bring your own device) must connect to the external guest network; all other internal corporate devices can connect to the internal network.
* **Utilizing VPN**: if the network has both internal and external networks, using a VPN would be ideal while using the internal network.

Of course, enabling both network-based (applies to routers and wireless access points) and host-based (applies to workstations) firewalls are a must when it comes to network security. With a network-based firewall, it can be enabled via the wireless access web portal and router web portal; it’ll be able to constantly monitor incoming and outgoing traffic on the network and prevents suspicious traffic from entering the network by dropping its network packets. With a host-based firewall, it’ll act as an extra layer to protect suspicious traffic from entering into the workstation.

Finally, it’s important to point out these final security practices with all network devices and workstations:

* **Default usernames and passwords**: many manufacturers have default username and passwords when it comes to switch, router, and wireless access portals. ***Because those default usernames and passwords are easily accessible to anyone on the web, change both the username and password!***
* **Stay up-to-date**: if any tech equipment is outdated hardware wise, it may pose a security risk and require an upgrade; while maintaining existing hardware, it’s important to apply patches, updates, and firmware updates to continually stay protected from the latest security exposures.

**Conclusion**

Bringing everything together, we were able to discuss securing access control methods for all user accounts, password policies, a cryptology method to ensure data is encrypted and inaccessible, a remote access plan to ensure users accessing the network remotely do so in a secure manner and protecting the network from malware and other malicious attacks. By following these security measures, while continually creating a security conscious environment via employee new hire training sessions and annual training sessions, ZXY Corporation will be able to continually protect itself from the latest security threats.

References

Access Control Best Practices Facts. Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Access Control Facts. Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Physical Security Facts. Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Switch Security Facts. (2018). Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Using Fine-Grained Password Policies. (2018). Retrieved from TestOut website:

https://cdn.testout.com/client-v5-1-10-501/startlabsim.html

VPN Facts. (2018). Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html

Wireless Security Facts. (2018). Retrieved from TestOut website: https://cdn.testout.com/

client-v5-1-10-501/startlabsim.html